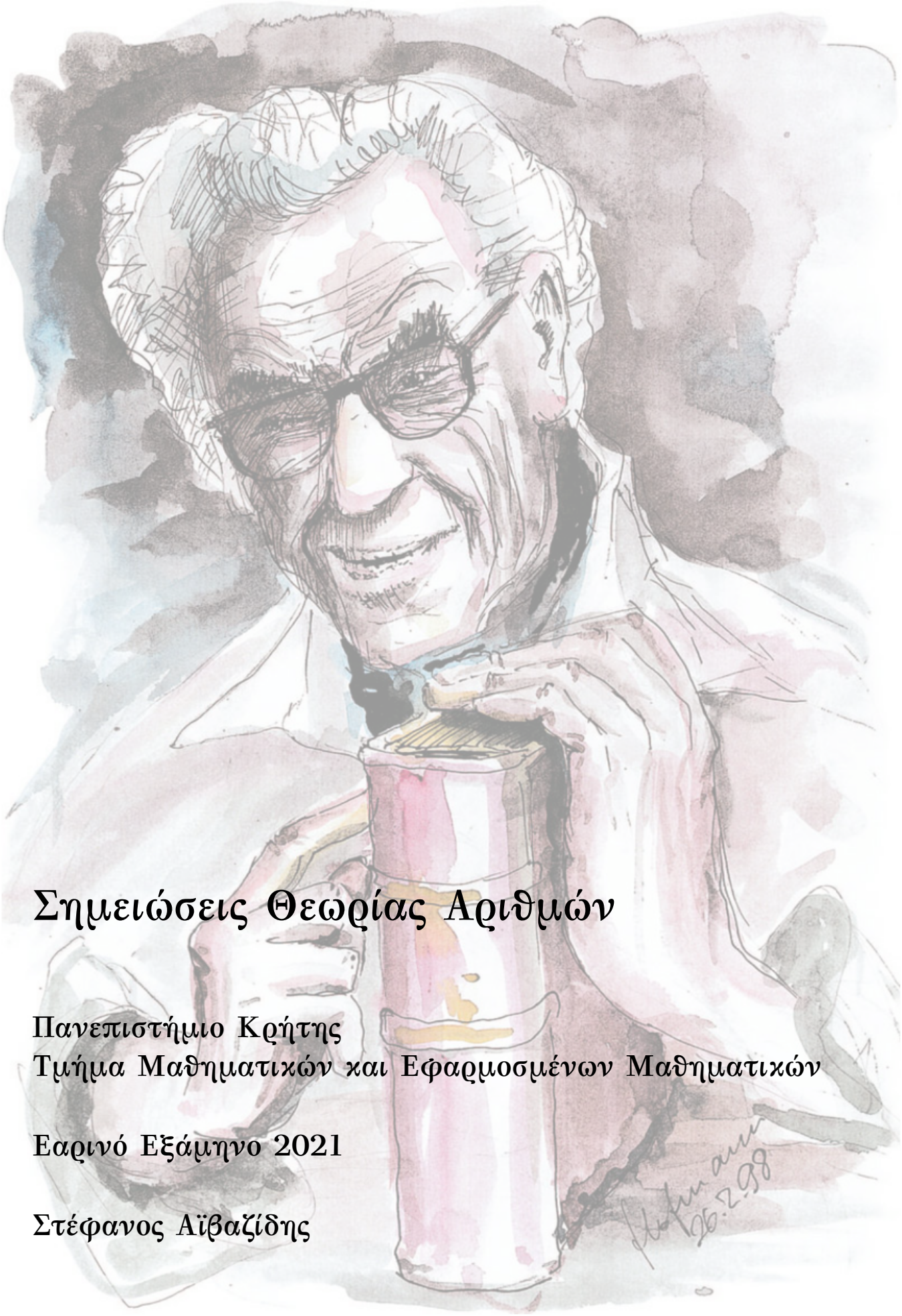


Σημειώσεις Θεωρίας Αριθμών

Πανεπιστήμιο Κρήτης
Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών

Εαρινό Εξάμηνο 2021

Στέφανος Αϊβαζίδης

Προλεγόμενα

Η Θεωρία Αριθμών είναι από τα πιο ενδιαφέροντα και συναρπαστικά μαθήματα ενός προπτυχιακού προγράμματος σπουδών στα Μαθηματικά και ελπίζω ότι με το πέρας των διαλέξεων αυτού του εξαμήνου, αλλά και αργότερα όταν θα ολοκληρώνετε πια τις σπουδές σας, θα μοιράζεστε κι εσείς την ίδια άποψη.

Στο μάθημα αυτό θα συναντήσουμε μερικές από τις πιο βασικές έννοιες της «Στοιχειώδους Θεωρίας Αριθμών», το πεδίο εκείνο δηλαδή που δεν στηρίζεται σε βαθύτερη Αλγεβρική ή Αναλυτική Θεωρία. Ελπίδα μου είναι να ενδιαφερθείτε αρκετά για την περιοχή αυτή ώστε αργότερα να πάρετε πιο προχωρημένα μαθήματα, όπως η Αλγεβρική Θεωρία Αριθμών που προσφέρει το Τμήμα σε μεταπτυχιακό επίπεδο.

Στην πραγματικότητα, τα προαπαιτούμενα για να παρακολουθήσει κανείς αυτό το μάθημα είναι ελάχιστα έως μηδαμινά. Θα δούμε έννοιες όπως η διαιρετότητα, ο μέγιστος κοινός διαιρέτης και το ελάχιστο κοινό πολλαπλάσιο, οι πρώτοι αριθμοί και το Θεμελιώδες Θεώρημα της Αριθμητικής, η αριθμητική των ισοτιμιών, η βασική θεωρία των αριθμητικών συναρτήσεων και τα επώνυμα Θεωρήματα των Fermat, Wilson και Euler. Θα μιλήσουμε ακόμα για την βασική θεωρία τετραγωνικών υπολοίπων και τον Νόμο Τετραγωνικής Αντιστροφής. Εφ' όσον μας το επιτρέψει ο χρόνος, ίσως καταφέρουμε να δούμε ακόμα ένα ή δύο εμβόλιμα θέματα.

Κάθε εβδομάδα θα έχετε στην διάθεσή σας βίντεο-διαλέξεις αναρτημένες στο Youtube οι οποίες θα είναι βασισμένες στις σημειώσεις που ετοιμάζω για το μάθημα. Τις σημειώσεις αυτές, οι οποίες θα ανανεώνονται διαρκώς ώστε να είναι κάθε φορά επίκαιρες, θα έχετε επίσης στην διάθεσή σας για την μελέτη σας. Θα παρατηρήσετε ότι στο τέλος κάθε μαθήματος υπάρχουν μερικές ασκήσεις προς λύση. Τις ασκήσεις αυτές (με μία εξαίρεση στην οποία θα αναφερθώ παρακάτω), θα πρέπει να τις θεωρείτε *υποχρεωτικές*. Για τον ίδιο λόγο που κανείς δεν μπορεί να μάθει να μαγειρεύει ξεφυλλίζοντας απλά ένα βιβλίο συνταγών, καμία καινούργια μαθηματική γνώση δεν μπορεί να κατακτηθεί χωρίς την προσπάθεια που χρειάζεται για την επίλυση προβλημάτων.

Στο τέλος κάθε διδακτικής εβδομάδας θα σας παρέχονται φυλλάδια με λυμένες όλες τις ασκήσεις που τέθηκαν στις δύο προηγούμενες παραδόσεις. Ενίοτε, ίσως συναντήσετε ασκήσεις με ένα αστεράκι ($*$). Οι ασκήσεις αυτές είναι αυξημένης δυσκολίας και μπορείτε να τις δοκιμάσετε ή όχι, όπως κρίνετε εσείς. Η πρότασή μου, σε όσους και όσες αποφασίσουν να ασχοληθούν με κάποιες από αυτές τις ασκήσεις, είναι να θέσετε στον εαυτό σας ένα χρονικό όριο για την προσπάθεια επίλυσης. Ο χρόνος που έχετε ως φοιτητές για να αντεπεξέλθετε στις απαιτήσεις του προγράμματος σπουδών του Τμήματός σας είναι περιορισμένος, επομένως θα πρέπει να τον διαχειρίζεστε με σύνεση.

Παραμένω, καθ' όλη την διάρκεια του μαθήματος, στην διάθεσή σας για να απαντήσω σε απορίες και να βοηθήσω σε όποιες μαθηματικές δυσκολίες συναντήσετε. Όπως αναφέρω και στην γενική περιγραφή του μαθήματος στο σύστημα Moodle, είναι προτιμητέο να χρησιμοποιείτε

το forum του μαθήματος για τις ερωτήσεις σας, το οποίο θα ελέγχω τακτικά. Ο λόγος είναι να αποφεύγεται κατά το δυνατόν η επανάληψη αλλά και να ωφελούνται και άλλοι από τις απαντήσεις.

Καλή πρόοδο!

Στέφανος Αϊβαζίδης
Φεβρουάριος 2021

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

1η Παράδοση

1.1 Τι είναι η Θεωρία Αριθμών; Μια μικρή εισαγωγή

Η Θεωρία Αριθμών είναι η περιοχή εκείνη των Μαθηματικών που ασχολείται με γενικές ιδιότητες κυρίως των φυσικών αριθμών $\mathbb{N} = \{1, 2, 3, \ldots\}$, ενίοτε όμως και των ακεραίων ή των ρητών. Ένα κανονικό παράδειγμα αριθμοθεωρητικής πρότασης είναι ότι κάθε φυσικός γράφεται ως άθροισμα το πολύ 4 τετραγώνων. Φερ' ειπείν,

$$496 = 20^2 + 8^2 + 4^2 + 4^2.$$

Ακολουθούν μερικά παραδείγματα ερωτημάτων που έχουν απασχολήσει τον κλάδο της Θεωρίας Αριθμών:

- Δοθέντος φυσικού αριθμού n, πώς αποφασίζουμε αν ο n είναι πρώτος ή σύνθετος; Αν είναι σύνθετος, πώς τον παραγοντοποιούμε;
- Πόσες λύσεις έχουν εξισώσεις όπως η $x^2 + y^2 = n$ ή η $x^3 + y^3 = z^3$ για σταθερό n, όπου οι μεταβλητές είναι φυσικοί αριθμοί;
- Πόσο καλά μπορούμε να προσεγγίσουμε έναν δοσμένο άρρητο από ρητούς «χαμηλής πολυπλοκότητας»;
- Πόσοι πρώτοι περίπου υπάρχουν μικρότεροι ή ίσοι του $10^{10^{10}}$;
- Είναι περισσότεροι οι πρώτοι της μορφής $4k + 1$ ή της μορφής $4k - 1$;

Ερωτήματα αυτού του είδους συναρπάζουν τον μαθηματικά κλίνοντα άνθρωπο εδώ και χιλιάδες χρόνια. Αρκεί να σκεφτούμε ότι ο Ευκλείδης έγραψε τα περίφημα «Στοιχεία» του, όπου μεταξύ άλλων αποδεικνύει αυστηρά ότι υπάρχουν άπειροι πρώτοι αριθμοί, πριν από περίπου 2300 χρόνια. Από την άλλη, υπάρχουν περιοχές της Θεωρίας Αριθμών, όπως για παράδειγμα ο έλεγχος αν ένας αριθμός είναι πρώτος και η παραγοντοποίηση, που έχουν μεγάλη πρακτική χρησιμότητα, αφού κώδικες και πρωτόκολλα ασφαλούς επικοινωνίας βασίζονται σε ιδιότητες των φυσικών και σε έννοιες της Θεωρίας Αριθμών όπως η αριθμητική ισοτιμιών.

1.2 Η Αρχή της Επαγωγής

Σε αυτό το μάθημα δεν θα κάνουμε καμία προσπάθεια να ορίσουμε αξιωματικά τους φυσικούς αριθμούς. Υποθέτουμε, αντιθέτως, ότι μας δίνονται και ότι ο αναγνώστης είναι εξοικειωμένος

με τις βασικές ιδιότητές τους. Υπενθυμίζουμε την εξής βασική αρχή, η οποία αποτελεί το σημείο εκκίνησης για εμάς και την οποία δεχόμαστε ως αξίωμα.

Αξίωμα 1.2.1 (Αρχή του Ελαχίστου). *Κάθε μη κενό υποσύνολο των φυσικών αριθμών έχει ελάχιστο στοιχείο.*

Η Αρχή του Ελαχίστου, επομένως, η οποία είναι γνωστή και ως Αρχή της Καλής Διάταξης, διατείνεται ότι αν έχουμε ένα $S \subseteq \mathbb{N}$ το οποίο είναι μη κενό, τότε υπάρχει στοιχείο $a \in S$ τέτοιο που $a \leqslant b$ για κάθε στοιχείο $b \in S$. Ας δούμε τώρα πώς με την αρχή του ελαχίστου μπορούμε να αποδείξουμε ότι οι φυσικοί αριθμοί έχουν την λεγόμενη Αρχιμήδεια Ιδιότητα.

Θεώρημα 1.2.2 (Αρχιμήδεια Ιδιότητα). *Έστω a, b φυσικοί. Τότε υπάρχει φυσικός n τέτοιος που $na \geqslant b$.*

Απόδειξη. Ας υποθέσουμε ότι αυτό που καλούμαστε να δείξουμε δεν ισχύει. Έπεται τότε ότι για κάποιους a, b έχουμε ότι $na < b$ για κάθε φυσικό n. Επομένως, το σύνολο

$$S = \{b - na : n \in \mathbb{N}\}$$

αποτελείται εξ ολοκλήρου από φυσικούς αριθμούς. Από την Αρχή του Ελαχίστου τώρα, το S έχει ελάχιστο στοιχείο, έστω το $b - ma$. Παρατηρούμε εδώ ότι το $b - (m+1)a \in S$, αφού το S περιλαμβάνει όλους τους φυσικούς αυτής της μορφής. Επιπλέον, έχουμε ότι

$$b - (m+1)a = (b - ma) - a < b - ma$$

κάτι που αντιβαίνει στην επιλογή του $b - ma$ ως ελαχίστου στοιχείου του S. Η αντίφαση αυτή προέκυψε από την αρχική μας παραδοχή ότι η Αρχιμήδεια Ιδιότητα δεν ισχύει. Επομένως το θεώρημα ισχύει πράγματι και η απόδειξή μας είναι πλήρης. ■

Έχοντας τώρα στη διάθεσή μας την Αρχή του Ελαχίστου, μπορούμε να διατυπώσουμε και να αποδείξουμε την Αρχή της Επαγωγής ή, ακριβέστερα, την 1η Μορφή της Αρχής της Επαγωγής.

Θεώρημα 1.2.3 (1η Μορφή της Αρχής της Επαγωγής). *Έστω S σύνολο φυσικών αριθμών με τις ακόλουθες ιδιότητες:*

(i) *Ο φυσικός $1 \in S$.*

(ii) *Όποτε $k \in S$, τότε και $k + 1 \in S$.*

Τότε το S είναι το σύνολο των φυσικών $\mathbb{N}$.

Απόδειξη. Έστω T το σύνολο των φυσικών που δεν ανήκουν στο S. Ας υποθέσουμε ακόμα ότι το T είναι μη κενό σύνολο. Από την Αρχή του Ελαχίστου παίρνουμε ότι το T έχει ελάχιστο στοιχείο, το οποίο καλούμε a. Εφ' όσον $1 \in S$ εξ υποθέσεως, ισχύει σίγουρα ότι $a > 1$, και έτσι $0 < a - 1 < a$. Η επιλογή του a ως ελαχίστου στοιχείου του T συνεπάγεται ότι το $a - 1$ δεν ανήκει στο T ή ισοδύναμα ότι το $a - 1 \in S$. Από την υπόθεσή μας όμως και πάλι έχουμε ότι το $a = (a - 1) + 1$ ανήκει στο S, κάτι που αντιβαίνει στο γεγονός ότι $a \in T$. Καταλήγουμε λοιπόν ότι η αρχική μας υπόθεση ήταν εσφαλμένη και άρα το T είναι το κενό σύνολο από το οποίο προκύπτει ότι $S = \mathbb{N}$, όπως ακριβώς θέλαμε να δείξουμε. ■

Να σημειώσουμε εδώ ότι θα μπορούσαμε να δεχτούμε την Αρχή της Επαγωγής ως Αξίωμα αντί της Αρχής του Ελαχίστου και σε αυτήν την περίπτωση η Αρχή του Ελαχίστου θα προέκυπτε

ως Θεώρημα. Οι δύο αυτές Αρχές είναι, λοιπόν, ισοδύναμες μεταξύ τους και το ποια από τις δύο θα ληφθεί ως Αξίωμα και ποια θα προκύψει αποδεικτικά είναι κυρίως θέμα προτίμησης.

Ας δούμε τώρα ένα παράδειγμα πώς το Θεώρημα 1.2.3 μπορεί να χρησιμοποιηθεί για να αποδειχθεί ένας αρκετά γνωστός τύπος.

Παράδειγμα 1.2.4. Για κάθε φυσικό n έχουμε ότι

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1.2.1}$$

Απόδειξη. Έστω S το σύνολο των φυσικών που ικανοποιούν την εξίσωση (1.2.1). Παρατηρούμε αρχικά ότι

$$1^2 = \frac{1(1+1)(2+1)}{6} = 1.$$

Επομένως, έχουμε ότι $1 \in S$. Έστω τώρα ότι ο φυσικός k ανήκει στο σύνολο S, έτσι ώστε

$$1^2 + 2^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}. \tag{1.2.2}$$

Για να λάβουμε το άθροισμα των πρώτων $k+1$ τετραγώνων αρκεί να προσθέσουμε το $(k+1)^2$ και στα δύο μέλη της (1.2.2) παίρνοντας

$$1^2 + 2^2 + \ldots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2.$$

Αλγεβρικοί χειρισμοί στο δεξί μέλος μάς δίνουν ότι

$$(k+1)\left[\frac{k(2k+1)+6(k+1)}{6}\right] = (k+1)\left[\frac{2k^2+7k+6}{6}\right] = \frac{(k+1)(k+2)(2k+3)}{6}$$

και αυτή η έκφραση είναι ακριβώς το δεξί μέλος τής (1.2.1) για $n = k+1$. Δείξαμε λοιπόν ότι αν $k \in S$ τότε και $k+1 \in S$. Από το Θεώρημα 1.2.3 προκύπτει τώρα ότι $S = \mathbb{N}$, που ήταν και το ζητούμενο. ■

Σχόλιο 1.2.5. Χάριν συντομίας, δεν θα κάνουμε στο εξής αναφορά σε ένα σύνολο S για το οποίο θα καλούμαστε να δείξουμε ότι $1 \in S$ και αν $k \in S$ για κάποιον φυσικό k, τότε και $k+1 \in S$. Αντίθετα, θα επιχειρηματολογούμε άμεσα ως εξής: εφ' όσον η πρόταση που καλούμαστε να δείξουμε είναι αληθής για τον φυσικό 1 και αν είναι αληθής για τον φυσικό k, τότε είναι αληθής και για τον $k+1$, προκύπτει ότι η πρόταση είναι αληθής για κάθε φυσικό αριθμό.

Η πρώτη συνθήκη του Θεωρήματος 1.2.3 συνήθως καλείται η *βάση* της επαγωγής, ενώ η δεύτερη το *επαγωγικό βήμα*. Χρειάζεται προσοχή από μέρους μας σε αυτό το σημείο. Κανένα συμπέρασμα δεν μπορεί να εξαχθεί αν δεν επαληθευθούν και οι δύο συνθήκες του Θεωρήματος 1.2.3! Καλείστε να εξετάσετε τον αναληθή ισχυρισμό

$$1 + 3 + 5 + \ldots + (2n-1) = n^2 + 3. \tag{1.2.3}$$

Βλέπουμε εύκολα ότι το επαγωγικό βήμα δουλεύει άριστα στον παραπάνω τύπο με την έννοια ότι αν η (1.2.3) ισχύει για $n = k$ τότε ισχύει και για $n = k+1$. Όμως η (1.2.3) δεν αληθεύει για καμία τιμή του n.

Σε πολλές περιπτώσεις το Θεώρημα 1.2.3 είναι ανεπαρκές για να λειτουργήσει ένα επαγωγικό επιχείρημα. Αυτό συμβαίνει σε περίπτωση που χρειάζεται να λάβουμε ως δεδομένη την αλήθεια ενός ισχυρισμού για ένα σύνολο φυσικών το πολύ k, όπου $k \in \mathbb{N}$, και όχι μόνο για έναν τέτοιον k. Αυτό ακριβώς το κενό καλύπτει η 2η μορφή της Αρχής της Επαγωγής (γνωστή και ως Ισχυρή Επαγωγή) όπως θα δούμε παρακάτω.

Θεώρημα 1.2.6 (2η Μορφή της Αρχής της Επαγωγής). *Έστω S σύνολο φυσικών αριθμών με τις ακόλουθες ιδιότητες:*

(i) *Ο φυσικός $1 \in S$.*

(ii) *Όποτε k φυσικός τέτοιος που $1, 2, \ldots, k \in S$, τότε και $k + 1 \in S$.*

Τότε το S είναι το σύνολο των φυσικών $\mathbb{N}$.

Απόδειξη. Η απόδειξη είναι παρόμοια με αυτήν του Θεωρήματος 1.2.3. Έστω πάλι T το σύνολο των φυσικών που δεν ανήκουν στο S. Αν το T είναι μη κενό σύνολο, έστω n το ελάχιστο στοιχείο του T. Τότε $n > 1$ από την πρώτη υπόθεση, ενώ από το γεγονός ότι το n είναι ελάχιστο συμπεραίνουμε ότι κανένας από τους φυσικούς $1, 2, \ldots, n-1$ δεν ανήκει στο T ή ισοδύναμα ότι οι $1, 2, \ldots, n-1$ όλοι ανήκουν στο S. Από την δεύτερη υπόθεση έπεται τώρα ότι ο $n = (n-1) + 1 \in S$, που είναι άτοπο. Επομένως $T = \emptyset$ και άρα $S = \mathbb{N}$. ■

Ας δούμε τώρα ένα παράδειγμα όπου η χρήση της 2ης μορφής, και όχι της 1ης, είναι απαραίτητη για να λειτουργήσει το επαγωγικό επιχείρημα.

Παράδειγμα 1.2.7. Η ακολουθία του Lucas

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$$

ορίζεται από τον κανόνα $a_1 = 1$, $a_2 = 3$ και $a_n = a_{n-1} + a_{n-2}$ για $n \geqslant 3$. Να δειχθεί ότι $a_n < (7/4)^n$ για κάθε $n \in \mathbb{N}$.

Απόδειξη. Παρατηρούμε αρχικά ότι $a_1 = 1 < 7/4$ και $a_2 = 3 < (7/4)^2 = 49/16$, επομένως η ζητούμενη ανισότητα ισχύει σε αυτές τις δύο αρχικές περιπτώσεις. Έχουμε λοιπόν τη βάση της επαγωγής. Ας υποθέσουμε τώρα ότι η ζητούμενη ανισότητα ισχύει για όλους τους φυσικούς που είναι μικρότεροι δοθέντος $k \in \mathbb{N}$, όπου $k \geqslant 3$. Επομένως $a_{k-1} < (7/4)^{k-1}$ και $a_{k-2} < (7/4)^{k-2}$. Έχουμε τώρα

$$\begin{aligned} a_k = a_{k-1} + a_{k-2} &< (7/4)^{k-1} + (7/4)^{k-2} \\ &= (7/4)^{k-2}(7/4 + 1) \\ &= (7/4)^{k-2}(11/4) \\ &< (7/4)^{k-2}(7/4)^2 \\ &= (7/4)^k, \end{aligned}$$

όπου στην πρώτη ανισότητα χρησιμοποιήσαμε την επαγωγική υπόθεση. Οι συνθήκες του Θεωρήματος 1.2.6 καλύπτονται κι έτσι συμπεραίνουμε ότι η ζητούμενη ανισότητα ισχύει για κάθε $k \in \mathbb{N}$. ■

1.3 Ασκήσεις

Άσκηση 1.3.1. Να αποδείξετε ότι

$$1+3+5+\ldots+(2n-1)=n^2, \tag{1.3.1}$$

για κάθε φυσικό n.

Απόδειξη. Για $n=1$ έχουμε το προφανές $1=1^2$, που ισχύει. Έστω τώρα ότι το ζητούμενο ισχύει για τον φυσικό n, όπου $n \geqslant 1$. Έχουμε ότι

$$1+3+5+\ldots+(2n-1)+(2n+1)=n^2+2n+1=(n+1)^2\,, \tag{1.3.2}$$

όπου στην πρώτη ισότητα αντικαταστήσαμε το $1+3+5+\ldots+(2n-1)$ με το n^2 από την επαγωγική υπόθεση. Η ισότητα στην (1.3.2) δείχνει ότι η (1.3.1) ισχύει για τον φυσικό $n+1$. Χρησιμοποιώντας την 1η Μορφή της Αρχής της Επαγωγής, καταλήγουμε ότι το ζητούμενο ισχύει για κάθε φυσικό αριθμό. ■

Άσκηση 1.3.2. Για κάθε φυσικό n, να δειχθεί ότι

$$\frac{1}{1^2}+\frac{1}{2^2}+\ldots+\frac{1}{n^2} \leqslant 2-\frac{1}{n}\,.$$

Απόδειξη. Για $n=1$ έχουμε

$$1=\frac{1}{1^2}=2-\frac{1}{1},$$

οπότε και ισχύει η ισότητα στην ζητούμενη ανισότητα. Δεχόμαστε τώρα την ισχύ της ανισότητας για τον φυσικό n, όπερ

$$\frac{1}{1^2}+\frac{1}{2^2}+\ldots+\frac{1}{n^2} \leqslant 2-\frac{1}{n} \tag{1.3.3}$$

και προσθέτουμε τον όρο $\frac{1}{(n+1)^2}$ και στα δύο μέλη της (1.3.3), παίρνοντας

$$\frac{1}{1^2}+\frac{1}{2^2}+\ldots+\frac{1}{n^2}+\frac{1}{(n+1)^2} \leqslant 2-\frac{1}{n}+\frac{1}{(n+1)^2}\,.$$

Βλέπουμε λοιπόν ότι, για να δείξουμε την ισχύ της (1.3.3) για $n+1$, αρκεί να δείξουμε ότι

$$2-\frac{1}{n}+\frac{1}{(n+1)^2} \leqslant 2-\frac{1}{n+1}$$

ή ισοδύναμα ότι

$$\frac{1}{n+1}+\frac{1}{(n+1)^2} \leqslant \frac{1}{n}\,.$$

Πολλαπλασιάζουμε και τα δύο μέλη της παραπάνω ανισότητας (την οποία θυμόμαστε ότι καλούμαστε να δείξουμε) με τον όρο $n(n+1)^2$ για να την απλοποιήσουμε και παίρνουμε την

$$n(n+1)+n=n^2+2n \leqslant (n+1)^2\,,$$

η οποία προφανώς ισχύει. Η επαγωγή μας είναι πλήρης επομένως, άρα η ζητούμενη ανισότητα ισχύει για κάθε φυσικό n. ■

Άσκηση 1.3.3. Να αποδείξετε ότι

$$1^3 + 2^3 + \ldots + n^3 = \left[\frac{n(n+1)}{2}\right]^2 \tag{1.3.4}$$

για κάθε φυσικό n. Ακολούθως, να συμπεράνετε ότι κάθε κύβος φυσικού γράφεται ως διαφορά τετραγώνων.

Απόδειξη. Για $n = 1$ η ισότητα είναι προφανής. Έστω ότι η (1.3.4) ισχύει για τον n. Τότε

$$\begin{aligned} 1^3 + 2^3 + \ldots + n^3 + (n+1)^3 &= \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 \\ &= (n+1)^2\left(\frac{n^2}{4} + n + 1\right) \\ &= (n+1)^2\frac{(n+2)^2}{4} \\ &= \left[\frac{(n+1)(n+2)}{2}\right]^2, \end{aligned}$$

που είναι η (1.3.4) για $n+1$. Το επαγωγικό επιχείρημα είναι πλήρες.

Μας μένει τώρα να δείξουμε ότι αν n φυσικός, τότε ο n^3 είναι διαφορά τετραγώνων φυσικών. Παρατηρούμε όμως ότι

$$\begin{aligned} n^3 &= (1^3 + 2^3 + \ldots + n^3) - \left[1^3 + 2^3 + \ldots + (n-1)^3\right] \\ &= \left[\frac{n(n+1)}{2}\right]^2 - \left[\frac{n(n-1)}{2}\right]^2, \end{aligned}$$

όπου η δεύτερη ισότητα προκύπτει από το πρώτο μέρος. ■

Άσκηση 1.3.4. Να αποδείξετε επαγωγικά την ανισότητα του Bernoulli σύμφωνα με την οποία αν x είναι πραγματικός τέτοιος που $1 + x > 0$, τότε $(1+x)^n \geqslant 1 + nx$ για κάθε φυσικό n.

Απόδειξη. Έστω x τυχαίος πραγματικός ώστε $1 + x > 0$. Η ζητούμενη ανισότητα είναι ισότητα στην περίπτωση $n = 1$, οπότε η βάση της επαγωγής δουλεύει. Υποθέτοντας ότι η $(1+x)^n \geqslant 1 + nx$ ισχύει για τον n, έχουμε

$$(1+x)^{n+1} = (1+x)^n(1+x) \geqslant (1+nx)(1+x) = [1 + (n+1)x] + nx^2 \geqslant 1 + (n+1)x\,.$$

Η πρώτη ανισότητα ισχύει από το επαγωγικό βήμα, ενώ η τελευταία επειδή για κάθε πραγματικό x και για κάθε φυσικό n έχουμε ότι $nx^2 \geqslant 0$. Η επαγωγή μας δουλεύει συνολικά, επομένως η ανισότητα Bernoulli ισχύει για κάθε φυσικό n. ■

Άσκηση 1.3.5. Να δειχθεί η ακόλουθη παραλλαγή του Θεωρήματος 1.2.3.

Θεώρημα. Έστω $n_0 \in \mathbb{N}$ και S υποσύνολο του $\mathbb{N}_{\geqslant n_0} = \{n \in \mathbb{N} : n \geqslant n_0\}$ με τις ακόλουθες ιδιότητες:

(i) Ο φυσικός $n_0 \in S$.

(ii) Όποτε $k \in S$, τότε και $k+1 \in S$.

Τότε το S είναι το σύνολο των φυσικών $n \geqslant n_0$.

Απόδειξη. Η απόδειξη είναι παρόμοια με αυτήν των σημειώσεων.

Έστω T το σύνολο των φυσικών $\geqslant n_0$ που δεν ανήκουν στο S. Ας υποθέσουμε ακόμα ότι $T \neq \emptyset$. Από την Αρχή του Ελαχίστου παίρνουμε ότι το T έχει ελάχιστο στοιχείο, το οποίο καλούμε a. Εφ΄ όσον $n_0 \in S$ εξ υποθέσεως, ισχύει ότι $a > n_0$, και έτσι $a-1 \geqslant n_0$. Η επιλογή του a ως ελαχίστου στοιχείου του T συνεπάγεται ότι το $a-1 \notin T$ ή ισοδύναμα ότι $a-1 \in S$ αφού $a-1 \geqslant n_0$. Από την υπόθεσή μας όμως και πάλι, έχουμε ότι το $a = (a-1)+1$ ανήκει στο S, κάτι που αντιβαίνει στο γεγονός ότι $a \in T$. Καταλήγουμε λοιπόν ότι η αρχική μας υπόθεση ήταν εσφαλμένη και άρα το T είναι το κενό σύνολο από το οποίο προκύπτει ότι $S = \mathbb{N}_{\geqslant n_0}$, όπως ακριβώς θέλαμε να δείξουμε. ■

Κεφάλαιο 2

2η Παράδοση

Συνεχίζουμε στο σημερινό μάθημα με λίγο-πολύ γνωστές έννοιες. Θα μιλήσουμε για τον Αλγόριθμο της Διαίρεσης με τον οποίο είμαστε όλοι εξοικειωμένοι και θα δούμε αργότερα τον μέγιστο κοινό διαιρέτη δύο ακεραίων και κάποιες από τις βασικές ιδιότητές του.

2.1 Ο Αλγόριθμος της Διαίρεσης

Ξεκινούμε με το ακόλουθο γνωστό αποτέλεσμα.

Θεώρημα 2.1.1 (Αλγόριθμος της Διαίρεσης). *Έστω a ακέραιος και b φυσικός. Τότε υπάρχουν μοναδικοί ακέραιοι q και r που ικανοποιούν την σχέση*

$$a = qb + r \qquad 0 \leqslant r < b.$$

Οι ακέραιοι q και r καλούνται αντίστοιχα το **πηλίκο** *και το* **υπόλοιπο** *της διαίρεσης του a με τον b.*

Απόδειξη. Δείχνουμε αρχικά ότι το σύνολο

$$S = \{a - xb : x \in \mathbb{Z},\, a - xb \geqslant 0\}$$

είναι μη κενό. Για να το πετύχουμε αυτό, αρκεί να βρούμε μία τιμή του x για την οποία $a - xb \geqslant 0$. Εφ' όσον $b \geqslant 1$, έχουμε $|a|b \geqslant |a|$ και έτσι

$$a - (-|a|)b = a + |a|b \geqslant a + |a| \geqslant 0.$$

Επομένως, η επιλογή $x = -|a|$ μας δίνει $a - xb \in S$. Από την Αρχή του Ελαχίστου τώρα, συμπεραίνουμε ότι το σύνολο S διαθέτει ελάχιστο στοιχείο, έστω το r. Από τον ορισμό του συνόλου S, υπάρχει ακέραιος q που ικανοποιεί

$$r = a - qb \qquad r \geqslant 0.$$

Ισχυριζόμαστε τώρα ότι $r < b$. Διαφορετικά, $r \geqslant b$ και

$$a - (q+1)b = (a - qb) - b = r - b \geqslant 0.$$

Έπεται λοιπόν ότι ο ακέραιος $a - (q+1)b$ ανήκει στο S. Όμως $a - (q+1)b = r - b < r$, που αντιβαίνει στον ορισμό του r ως ελαχίστου στοιχείου του S. Επομένως $r < b$, όπως ισχυριστήκαμε.

Απομένει τώρα να δείξουμε την μοναδικότητα των q και r. Ας υποθέσουμε αντιθέτως ότι ο a έχει δύο αναπαραστάσεις της επιθυμητής μορφής. Δηλαδή

$$a = qb + r = q'b + r',$$

όπου $0 \leqslant r < b$, $0 \leqslant r' < b$. Τότε $r' - r = b(q - q')$ και από αυτή τη σχέση έπεται ότι $|r' - r| = b|q - q'|$. Προσθέτοντας τις ανισότητες $-b < -r \leqslant 0$ και $0 \leqslant r' < b$, παίρνουμε $-b < r' - r < b$ ή ισοδύναμα $|r' - r| < b$. Επομένως, $b|q - q'| < b$, το οποίο μας δίνει

$$0 \leqslant |q - q'| < 1.$$

Αφού ο $|q - q'|$ είναι ακέραιος, συμπεραίνουμε από την παραπάνω σχέση ότι $|q - q'| = 0$ και άρα $q = q'$. Προκύπτει τώρα άμεσα ότι και $r = r'$, όπως θέλαμε να δείξουμε. ■

Θα δούμε τώρα ότι η γενική περίπτωση του Αλγορίθμου της Διαίρεσης, όπου απαιτούμε μόνο $b \neq 0$ αλλά ο b μπορεί να είναι και αρνητικός ακέραιος, είναι απλό πόρισμα του Θεωρήματος 2.1.1.

Πόρισμα 2.1.2 (Γενική Μορφή του Αλγορίθμου της Διαίρεσης). *Έστω a και b ακέραιοι με $b \neq 0$. Τότε υπάρχουν μοναδικοί ακέραιοι q και r που ικανοποιούν την σχέση*

$$a = qb + r \qquad 0 \leqslant r < |b|.$$

Απόδειξη. Αρκεί να εξετάσουμε την περίπτωση όπου $b < 0$. Τότε έχουμε $|b| > 0$ και το Θεώρημα 2.1.1 μας δίνει μοναδικούς ακεραίους q' και r τέτοιους που

$$a = q'|b| + r \qquad 0 \leqslant r < |b|.$$

Εφ' όσον $|b| = -b$, παίρνουμε $q = -q'$ και έτσι $a = qb + r$ με $0 \leqslant r < |b|$. ■

Ας δούμε τώρα μερικά παραδείγματα και εφαρμογές. Αρχικά, αν $b = 2$ τότε τα δυνατά υπόλοιπα είναι $r = 0$ και $r = 1$. Όταν $r = 0$, ο ακέραιος a έχει την μορφή $a = 2q$ και καλείται **άρτιος**, ενώ όταν $r = 1$, ο ακέραιος a έχει την μορφή $a = 2q + 1$ και καλείται **περιττός**. Επίσης, το a^2 έχει είτε την μορφή $(2q)^2 = 4k$ ή την $(2q + 1)^2 = 4(q^2 + q) + 1 = 4\ell + 1$. Έπεται δηλαδή ότι, αν το τετράγωνο ενός ακεραίου διαιρεθεί με το 4, αφήνει υπόλοιπο 0 ή 1.

Παράδειγμα 2.1.3. Το τετράγωνο ενός περιττού ακεραίου είναι της μορφής $8k + 1$.

Απόδειξη. Από τον Αλγόριθμο της Διαίρεσης, κάθε ακέραιος γράφεται σε μία από τις ακόλουθες τέσσερις μορφές: $4q$, $4q + 1$, $4q + 2$, $4q + 3$. Αν ο a είναι περιττός, τότε $a = 4q + 1$ ή $a = 4q + 3$. Στην πρώτη περίπτωση έχουμε

$$(4q + 1)^2 = 8(2q^2 + q) + 1 = 8k + 1,$$

ενώ στην δεύτερη έχουμε

$$(4q + 3)^2 = 8(2q^2 + 3q + 1) + 1 = 8\ell + 1.$$

Η απόδειξη είναι πλήρης. ■

2.2 Διαιρετότητα και ο Μέγιστος Κοινός Διαιρέτης

Η περίπτωση όπου ο Αλγόριθμος της Διαίρεσης δίνει υπόλοιπο 0, χρήζει ιδιαίτερης μνείας και με αυτήν ακριβώς την περίπτωση θα ασχοληθούμε σε αυτήν την παράγραφο. Οι έννοιες στις οποίες θα αναφερθούμε παραμένουν ως επί το πλείστον οικείες.

Ορισμός 2.2.1. Ένας ακέραιος b **διαιρείται** από έναν ακέραιο $a \neq 0$, το οποίο συμβολίζουμε ως $a \mid b$, αν υπάρχει ακέραιος c τέτοιος ώστε $b = ac$. Επίσης, γράφουμε $a \nmid b$ για να δηλώσουμε ότι ο b δεν διαιρείται από τον a.

Επομένως, ο -15 διαιρείται από το 5 αφού $-15 = 5(-3)$, ενώ ο 10 δεν διαιρείται από το 3 αφού η ισότητα $10 = 3c$ δεν αληθεύει για κανέναν ακέραιο c. Ακόμα, ένας αριθμός a είναι άρτιος αν $2 \mid a$ και περιττός αν $2 \nmid a$.

Να επισημάνουμε σε αυτό το σημείο ότι η σχέση της διαιρετότητας $a \mid b$ εκφράζεται και με άλλους ισοδύναμους τρόπους. Λέμε, για παράδειγμα, ότι ο a είναι **διαιρέτης** του b ή ότι ο a είναι **παράγοντας** του b ή ακόμα ότι ο b είναι **πολλαπλάσιο** του a.

Αν τώρα ο a διαιρεί τον b, τότε ο b διαιρείται επίσης και από τον $-a$, αφού η $b = ac$ συνεπάγεται την $b = (-a)(-c)$. Βλέπουμε δηλαδή ότι οι διαιρέτες ενός ακεραίου εμφανίζονται πάντα σε ζεύγη. Για να βρούμε, επομένως, τους διαιρέτες ενός ακεραίου, αρκεί να βρούμε τους θετικούς διαιρέτες του ακεραίου αυτού και να επισυνάψουμε στη λίστα τους αντίστοιχους αρνητικούς ακεραίους. Για τον λόγο αυτό, συνήθως εστιάζουμε στους *θετικούς διαιρέτες* μόνο ενός ακεραίου.

Στο επόμενο θεώρημα συγκεντρώνουμε μερικές βασικές ιδιότητες της σχέσης της διαιρετότητας οι οποίες προκύπτουν άμεσα από τον Ορισμό 2.2.1 και οι οποίες αποδεικνύονται εύκολα.

Θεώρημα 2.2.2. *Δοθέντων ακεραίων a, b, c, ισχύουν τα ακόλουθα.*

(i) $a \mid 0$, $1 \mid a$, $a \mid a$.

(ii) $a \mid 1$, *αν και μόνο αν* $a = \pm 1$.

(iii) *Αν* $a \mid b$ *και* $c \mid d$, *τότε* $ac \mid bd$.

(iv) *Αν* $a \mid b$ *και* $b \mid c$, *τότε* $a \mid c$.

(v) $a \mid b$ *και* $b \mid a$, *αν και μόνο αν* $a = \pm b$.

(vi) *Αν* $a \mid b$ *και* $b \neq 0$, *τότε* $|a| \leqslant |b|$.

(vii) *Αν* $a \mid b$ *και* $a \mid c$, *τότε* $a \mid (bx + cy)$ *για οποιουσδήποτε ακεραίους* x, y.

Απόδειξη. (i) Έχουμε $0 = 0 \cdot a$, $a = a \cdot 1$, και $a = 1 \cdot a$.

(ii) Οι μοναδικοί διαιρέτες του 1 είναι προφανώς οι 1 και -1.

(iii) Αν $b = ka$ και $d = \ell c$ για κάποιους ακεραίους k, ℓ, τότε $bd = k\ell(ac)$. Επομένως, $ac \mid bd$.

(iv) Αν $b = ka$ και $c = \ell b$ για τους ακεραίους k, ℓ, τότε $c = \ell k(a)$. Έπεται ότι $a \mid c$.

(v) Από τις σχέσεις $b = ka$ και $a = \ell b$ παίρνουμε ότι $b = k\ell b$, δηλαδή $1 = k\ell$. Χρησιμοποιώντας το (ii) τώρα, βλέπουμε ότι οι μόνες δυνατές περιπτώσεις είναι $k = \ell = 1$ ή $k = \ell = -1$ κι έτσι προκύπτει το ζητούμενο.

(vi) Αν $a \mid b$, υπάρχει ακέραιος k τέτοιος ώστε $b = ka$ και μάλιστα $k \neq 0$, αφού υποθέτουμε ότι $b \neq 0$. Έπεται λοιπόν ότι $|b| = |k||a| \geqslant |a|$, όπου η ανισότητα προκύπτει από το γεγονός ότι ο k είναι ακέραιος διάφορος του 0 και άρα $|k| \geqslant 1$.

(vii) Έστω ακέραιοι x, y. Από την σχέση $a \mid b$, υπάρχει ακέραιος k τέτοιος ώστε $b = ka$ και παρόμοια παίρνουμε $c = \ell a$ για κάποιον ακέραιο ℓ από την δεύτερη σχέση. Έπεται τώρα ότι

$$bx + cy = kax + \ell ay = (kx + \ell y)a.$$

Συμπεραίνουμε ότι $a \mid (bx+cy)$, όπως ακριβώς θέλαμε να δείξουμε, και μ' αυτό ολοκληρώνεται η απόδειξη. ■

Σημειώνουμε εδώ ότι η ιδιότητα (vii) στο παραπάνω θεώρημα επεκτείνεται εύκολα σε αθροίσματα με περισσότερους από δύο όρους. Δηλαδή, αν $a \mid b_k$ για $k = 1, 2, \ldots, n$, τότε

$$a \mid (b_1x_1 + b_2x_2 + \ldots b_nx_n)$$

για οποιουσδήποτε ακεραίους $x_1, x_2, \ldots, x_n$. Η απόδειξη (με επαγωγή στο πλήθος των όρων) αφήνεται ως άσκηση.

Αν οι a, b είναι ακέραιοι, τότε ο ακέραιος d λέγεται **κοινός διαιρέτης** των a, b, αν ισχύει $d \mid a$ και $d \mid b$. Επειδή ο 1 είναι κοινός διαιρέτης κάθε ακεραίου, ο 1 είναι κοινός διαιρέτης των a, b, Επομένως, το σύνολο των θετικών κοινών διαιρετών τους είναι μη κενό. Όμως κάθε ακέραιος διαιρεί τον 0 και έτσι αν $a = b = 0$, τότε κάθε ακέραιος είναι κοινός διαιρέτης των a, b. Σε αυτήν την περίπτωση, το σύνολο των κοινών διαιρετών των a, b είναι άπειρο. Αν όμως τουλάχιστον ένας εκ των a, b δεν είναι 0, τότε ο αριθμός των θετικών κοινών διαιρετών τους είναι πεπερασμένος. Μεταξύ αυτών υπάρχει ένας μέγιστος, ο οποίος καλείται ο μέγιστος κοινός διαιρέτης των a, b.

Ορισμός 2.2.3. Έστω a, b ακέραιοι τουλάχιστον ένας εκ των οποίων δεν είναι 0. Ο **μέγιστος κοινός διαιρέτης** των a, b, τον οποίο συμβολίζουμε με $\gcd(a, b)$, είναι ο φυσικός d που ικανοποιεί τα ακόλουθα.

(i) $d \mid a$ και $d \mid b$.

(ii) Αν $c \mid a$ και $c \mid b$, τότε $c \leqslant d$.

Παράδειγμα 2.2.4. Οι θετικοί διαιρέτες του -12 είναι οι 1, 2, 3, 4, 6, 12, ενώ εκείνοι του 30 είναι οι 1, 2, 3, 5, 6, 10, 15, 30. Επομένως οι θετικοί κοινοί διαιρέτες των -12 και 30 είναι οι 1, 2, 3, 6. Εφ' όσον ο 6 είναι ο μεγαλύτερος εξ αυτών, έπεται ότι $\gcd(-12, 30) = 6$. Με τον ίδιο τρόπο δείχνουμε ότι

$$\gcd(-5, 5) = 5 \qquad \gcd(8, 17) = 1 \qquad \gcd(-8, -36) = 4.$$

Στο επόμενο θεώρημα θα δούμε ότι ο μέγιστος κοινός διαιρέτης των a, b αναπαρίσταται ως γραμμικός συνδυασμός τους.

Θεώρημα 2.2.5. *Δοθέντων ακεραίων a, b που δεν είναι και οι δύο 0, υπάρχουν ακέραιοι x, y τέτοιοι ώστε*

$$\gcd(a, b) = ax + by.$$

Απόδειξη. Θεωρούμε το σύνολο S των θετικών γραμμικών συνδυασμών των a, b:

$$S = \{au + bv : au + bv > 0, \quad u, v \in \mathbb{Z}\}$$

και παρατηρούμε ότι το S είναι μη κενό αφού ο $|a| = au + b \cdot 0 \in S$, όπου $u = 1$ ή $u = -1$ ανάλογα με το αν ο a είναι θετικός ή αρνητικός. Από την Αρχή του Ελαχίστου, το S έχει ελάχιστο στοιχείο που καλούμε d, ενώ από τον ορισμό του S υπάρχουν ακέραιοι x, y τέτοιοι ώστε $d = ax + by$. Ισχυριζόμαστε τώρα ότι $d = \gcd(a, b)$.

Από τον Αλγόριθμο της Διαίρεσης, λαμβάνουμε ακεραίους q και r τέτοιους που $a = qd + r$, όπου $0 \leqslant r < d$. Τότε ο r γράφεται στην μορφή

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$$

Αν $r > 0$, τότε προκύπτει από την παραπάνω σχέση ότι $r \in S$, κάτι που αντιφάσκει με το γεγονός ότι ο d είναι το ελάχιστο στοιχείο του S. Επομένως, $r = 0$ και έτσι $a = qd$ ή ισοδύναμα $d \mid a$. Με παρόμοιο επιχείρημα έχουμε $d \mid b$, οπότε ο d είναι κοινός διαιρέτης των a, b.

Αν τώρα ο c είναι θετικός κοινός διαιρέτης των a, b, τότε από το (vii) του Θεωρήματος 2.2.2 συμπεραίνουμε ότι $c \mid (ax + by)$, δηλαδή $c \mid d$. Από το (vi) του Θεωρήματος 2.2.2 και πάλι, έχουμε $c = |c| \leqslant |d| = d$, έτσι ώστε ο d είναι ο μέγιστος κοινός διαιρέτης των a, b, όπως ακριβώς θέλαμε να δείξουμε. ■

Η παραπάνω απόδειξη είναι «υπαρξιακή» και δεν μας δίνει καμία πρακτική μέθοδο να βρίσκουμε τους ακεραίους x, y. Αυτό είναι κάτι που θα δούμε λίγο αργότερα. Η μορφή των ακεραίων του συνόλου S υποδεικνύει ένα ακόμα αποτέλεσμα, το οποίο καταγράφουμε ακολούθως.

Πόρισμα 2.2.6. *Δοθέντων ακεραίων a, b που δεν είναι και οι δύο 0, το σύνολο*

$$T = \{ax + by : x, y \in \mathbb{Z}\}$$

είναι ακριβώς το σύνολο των πολλαπλασίων του $d = \gcd(a, b)$.

Απόδειξη. Εφ' όσον $d \mid a$ και $d \mid b$, γνωρίζουμε ότι $d \mid (ax + by)$ για όλους τους ακεραίους x, y. Επομένως, κάθε στοιχείο του T είναι πολλαπλάσιο του d. Από την άλλη, ο d γράφεται ως $d = ax_0 + by_0$ για κατάλληλους ακεραίους x_0, y_0, έτσι που κάθε πολλαπλάσιο nd του d είναι της μορφής

$$nd = n(ax_0 + by_0) = a(nx_0) + b(ny_0).$$

Έπεται ότι ο nd είναι γραμμικός συνδυασμός των a, b, οπότε ανήκει στο T εξ ορισμού. ■

Αν τύχει οι 1, -1 να είναι οι μόνοι κοινοί διαιρέτες ενός ζεύγους ακεραίων a, b, τότε προφανώς $\gcd(a, b) = 1$. Για παράδειγμα,

$$\gcd(2, 5) = \gcd(-9, 16) = \gcd(-27, -35) = 1.$$

Αυτό είναι κάτι που συμβαίνει αρκετά συχνά και έχει ξεχωριστή σημασία.

Ορισμός 2.2.7. Δύο ακέραιοι a, b, που δεν είναι και οι δύο 0, καλούνται **σχετικά πρώτοι**, όταν $\gcd(a, b) = 1$.

Το επόμενο αποτέλεσμα χαρακτηρίζει τους σχετικά πρώτους ακεραίους συναρτήσει γραμμικών συνδυασμών.

Θεώρημα 2.2.8. *Έστω a, b ακέραιοι όχι και οι δύο 0. Τότε οι a, b είναι σχετικά πρώτοι αν και μόνο αν υπάρχουν ακέραιοι x, y τέτοιοι ώστε $ax + by = 1$.*

Απόδειξη. Αν οι a, b είναι σχετικά πρώτοι, έτσι ώστε $\gcd(a, b) = 1$, το ζητούμενο είναι απόρροια του Θεωρήματος 2.2.5. Αντίστροφα, έστω ότι $ax + by = 1$ και $d = \gcd(a, b)$. Αφού $d \mid a$ και $d \mid b$, παίρνουμε από το Θεώρημα 2.2.2 (vii) ότι ο d διαιρεί τον $ax + by = 1$ και εφ' όσον $d > 0$, καταλήγουμε ότι $d = 1$. ■

Πόρισμα 2.2.9. *Αν $\gcd(a, b) = d$, τότε $\gcd(a/d, b/d) = 1$.*

Απόδειξη. Από το Θεώρημα 2.2.5, υπάρχουν ακέραιοι x, y έτσι ώστε $d = ax + by$. Διαιρώντας με d και τα δύο μέλη αυτής της ισότητας, παίρνουμε

$$1 = \left(\frac{a}{d}\right) x + \left(\frac{b}{d}\right) y$$

και το ζητούμενο προκύπτει από το Θεώρημα 2.2.8. ■

Σημειώνουμε εδώ ότι δεν ισχύει γενικά πως αν $a \mid c$ και $b \mid c$, τότε $ab \mid c$. Παραδείγματος χάριν, $6 \mid 24$ και $8 \mid 24$, αλλά $6 \cdot 8 \nmid 24$. Έχουμε όμως το ακόλουθο.

Πόρισμα 2.2.10. *Αν $a \mid c$ και $b \mid c$ με $\gcd(a, b) = 1$, τότε $ab \mid c$.*

Απόδειξη. Οι σχέσεις $a \mid c$ και $b \mid c$ εξασφαλίζουν την ύπαρξη ακεραίων r, s αντίστοιχα έτσι ώστε $c = ar = bs$, ενώ το δεδομένο $\gcd(a, b) = 1$ μας επιτρέπει να γράψουμε $1 = ax + by$ για κάποια επιλογή ακεραίων x, y. Έχουμε λοιπόν ότι

$$c = c \cdot 1 = c(ax + by) = acx + bcy = a(bs)x + b(ar)x = ab(sx + ry)$$

ή ισοδύναμα $ab \mid c$, που ήταν και το ζητούμενο. ■

Το επόμενο αποτέλεσμα, αν και φαίνεται σχετικά «αθώο», είναι θεμελιώδους σημασίας.

Θεώρημα 2.2.11 (Λήμμα του Ευκλείδη). *Αν $a \mid bc$ με $\gcd(a, b) = 1$, τότε $a \mid c$.*

Απόδειξη. Το Θεώρημα 2.2.5 μας εξασφαλίζει την ύπαρξη ακεραίων x, y τέτοιων που $1 = ax + by$. Πολλαπλασιάζοντας με c και τα δύο μέλη, παίρνουμε

$$c = 1 \cdot c = (ax + by)c = acx + bcy.$$

Αφού όμως $a \mid ac$ και $a \mid bc$ εξ υποθέσεως, βλέπουμε ότι $a \mid (acx + bcy)$, δηλαδή $a \mid c$. ■

Η συνθήκη $\gcd(a, b) = 1$ στο Λήμμα του Ευκλείδη είναι προφανώς απαραίτητη. Για παράδειγμα, $12 \mid 9 \cdot 8$, αλλά $12 \nmid 9$ και $12 \nmid 8$.

Κλείνουμε αυτήν την παράγραφο με το ακόλουθο θεώρημα, το οποίο αξίζει να επισημάνουμε ότι συχνά χρησιμοποιείται ως *ορισμός* του μέγιστου κοινού διαιρέτη δύο ακεραίων. (Όταν συμβαίνει αυτό, χρειάζεται φυσικά να επανεξετάσουμε τι χρειάζεται να αποδείξουμε και τι όχι.)

Θεώρημα 2.2.12. *Έστω a, b ακέραιοι που δεν είναι και οι δύο 0. Για έναν φυσικό d ισχύει ότι $d = \gcd(a, b)$, αν και μόνο αν*

(i) $d \mid a$ *και* $d \mid b$.

(ii) *Αν* $c \mid a$ *και* $c \mid b$, *τότε* $c \mid d$.

Απόδειξη. Έστω πρώτα ότι $d = \gcd(a, b)$. Έπεται τώρα ότι $d \mid a$ και $d \mid b$, οπότε η συνθήκη (i) ικανοποιείται. Επίσης, από το Θεώρημα 2.2.5 ο d γράφεται ως $d = ax + by$ για κάποιους ακεραίους x, y. Επομένως, αν $c \mid a$ και $c \mid b$, τότε $c \mid (ax + by)$ ή ισοδύναμα $c \mid d$. Βλέπουμε λοιπόν ότι και η συνθήκη (ii) ικανοποιείται.

Ας υποθέσουμε τώρα αντιστρόφως ότι ο φυσικός d ικανοποιεί τις δοθείσες συνθήκες. Αν c είναι κοινός διαιρέτης των a και b, τότε $c \mid d$ από την (ii). Επομένως, $d \geqslant c$ και από αυτήν την ανισότητα έπεται ότι ο d είναι ο μέγιστος κοινός διαιρέτης των a και b. ■

2.3 Ασκήσεις

Άσκηση 2.3.1. Να αποδείξετε ότι αν a, b ακέραιοι με $b > 0$, τότε υπάρχουν μοναδικοί ακέραιοι q, r τέτοιοι ώστε $a = qb + r$, όπου $2b \leqslant r < 3b$.

Απόδειξη. Από τον Αλγόριθμο της Διαίρεσης, έπεται ότι υπάρχουν μοναδικοί ακέραιοι q', r' τέτοιοι ώστε $a = q'b + r'$, όπου $0 \leqslant r' < b$. Παίρνοντας $q = q' - 2$ και $r = r' + 2b$, βλέπουμε ότι $2b \leqslant r < 3b$, ενώ παράλληλα

$$qb + r = (q' - 2)b + (r' + 2b) = q'b + r' = a\,.$$

Επομένως έχουμε δείξει το ζητούμενο. ■

Άσκηση 2.3.2. Να δειχθεί ότι ο $3a^2 - 1$ δεν είναι ποτέ τέλειο τετράγωνο.

Απόδειξη. Είδαμε στο μάθημα ότι αν το τετράγωνο ενός ακεραίου διαιρεθεί με το 4, αφήνει υπόλοιπο 0 ή 1. Άρα $a^2 = 4k$ ή $a^2 = 4k + 1$ για κάποιον φυσικό k. Στην πρώτη περίπτωση, έχουμε

$$3a^2 - 1 = 3 \cdot 4k - 1 = 4(3k - 1) + 3\,,$$

που αφήνει υπόλοιπο 3 αν διαιρεθεί με το 4. Στην δεύτερη περίπτωση, έχουμε

$$3a^2 - 1 = 3(4k + 1) - 1 = 4(3k) + 2\,,$$

που αφήνει υπόλοιπο 2. Επομένως, σε κάθε περίπτωση ο $3a^2 - 1$ δεν είναι τέλειο τετράγωνο.

Εναλλακτικά, το ζητούμενο μπορεί να δειχθεί αν πρώτα δείξουμε ότι όταν το τετράγωνο ενός ακεραίου διαιρεθεί με το 3 αφήνει υπόλοιπο 0 ή 1 (η απόδειξη αυτού είναι εντελώς παρόμοια με αυτή του 4) και μετά παρατηρήσουμε ότι $3a^2 - 1 = 3(a^2 - 1) + 2$. ■

Άσκηση 2.3.3. Να αποδείξετε ότι κανένας όρος της ακολουθίας

$$11, 111, 1111, 11111, \ldots$$

δεν είναι τέλειο τετράγωνο.

Απόδειξη. Αρχικά, ο 11 δεν είναι τέλειο τετράγωνο. Τώρα, ένας αριθμός της μορφής $111\ldots111$ μπορεί να γραφεί ως εξής:

$$111\ldots111 = 111\ldots108 + 3\,.$$

Όμως, ο αριθμός $111\ldots108$ είναι πολλαπλάσιο του 4 και άρα ο $111\ldots111$ είναι της μορφής $4k+3$. Επικαλούμαστε και πάλι το αποτέλεσμα που δείξαμε στο μάθημα ότι αν το τετράγωνο ενός ακεραίου διαιρεθεί με το 4, αφήνει υπόλοιπο 0 ή 1 για να καταλήξουμε ότι ισχύει το ζητούμενο. ■

Άσκηση 2.3.4. Να βρεθούν όλοι οι φυσικοί n για τους οποίους ο $n+1$ διαιρεί τον n^2+1.

Λύση. Μόνο ο $n=1$ έχει την ζητούμενη ιδιότητα. Αυτό συμβαίνει διότι

$$n^2+1 = n(n+1) - (n-1)\,.$$

Επομένως, αν ο $n+1$ διαιρεί τον n^2+1, τότε ο $n+1$ διαιρεί τον $n-1$ από βασική ιδιότητα της διαιρετότητας που δείξαμε στο μάθημα. Όμως $n+1 > n-1$, επομένως έχουμε αναγκαστικά $n-1=0$. ■

Άσκηση 2.3.5. Να αποδείξετε ότι για κάθε ακέραιο n ισχύει ότι $\gcd(2n+1, 9n+4) = 1$.

Απόδειξη. Το ζητούμενο έπεται άμεσα από την παρατήρηση

$$9\cdot(2n+1) - 2\cdot(9n+4) = 1\,,$$

όπου χρησιμοποιούμε το βασικό αποτέλεσμα που δείξαμε στο μάθημα ότι αν ένας γραμμικός συνδυασμός δύο ακεραίων ισούται με 1, τότε αυτοί οι ακέραιοι είναι σχετικά πρώτοι (Θεώρημα 2.2.8). ■

Άσκηση 2.3.6. Επαληθεύστε τις ακόλουθες ιδιότητες του μέγιστου κοινού διαιρέτη.

(i) Αν $\gcd(a,b) = 1$ και $\gcd(a,c) = 1$, τότε $\gcd(a,bc) = 1$.

(ii) Αν $\gcd(a,b) = 1$ και $c \mid a$, τότε $\gcd(b,c) = 1$.

(iii) Αν $\gcd(a,b) = 1$, τότε $\gcd(ac,b) = \gcd(c,b)$.

(iv) Αν $\gcd(a,b) = 1$ και $c \mid a+b$, τότε $\gcd(a,c) = \gcd(b,c) = 1$.

Υπόδειξη: Έστω $d = \gcd(a,c)$. Τότε $d \mid a$, $d \mid c$ συνεπάγεται ότι $d \mid (a+b) - a$ ή $d \mid b$.

(v) Αν $\gcd(a,b) = 1$, $d \mid ac$ και $d \mid bc$, τότε $d \mid c$.

(vi) Αν $\gcd(a,b) = 1$, τότε $\gcd(a^2,b^2) = 1$.

Υπόδειξη: Δείξτε πρώτα ότι $\gcd(a,b^2) = \gcd(a^2,b) = 1$.

Απόδειξη. (i) Για να δείξουμε ότι $\gcd(a,bc) = 1$, αρκεί να βρούμε ακεραίους x, y τέτοιους ώστε $xa + ybc = 1$. Από την σχέση $\gcd(a,b) = 1$, έπεται ότι υπάρχουν r, s ώστε $ra + sb = 1$, ενώ από την σχέση $\gcd(a,c) = 1$, έπεται ότι υπάρχουν t, u ώστε $ta + uc = 1$. Έχουμε λοιπόν ότι

$$1 = (ra+sb)(ta+uc) = (rta + ruc + stb)\cdot a + (su)\cdot bc\,,$$

οπότε παίρνοντας $x = rta + ruc + stb$ και $y = su$ προκύπτει το ζητούμενο.

(ii) Επιχειρηματολογούμε όπως παραπάνω. Από την σχέση $\gcd(a,b)=1$, έπεται ότι υπάρχουν r, s ώστε $ra+sb=1$. Αφού $c \mid a$, υπάρχει u ώστε $a=uc$. Άρα $sb+(ru)c=1$. Επομένως, $\gcd(b,c)=1$.

(iii) Έστω $d_1=\gcd(ac,b)$ και $d_2=\gcd(c,b)$. Θα δείξουμε ότι $d_1 \mid d_2$ και $d_2 \mid d_1$ και από αυτό θα προκύψει το ζητούμενο.

Αρχικά, $d_2 \mid c$ οπότε $d_2 \mid ac$. Επίσης, $d_2 \mid b$. Από το Θεώρημα 2.2.12 έπεται ότι $d_2 \mid d_1$.

Έχουμε τώρα ότι $d_1 \mid ac$ και $d_1 \mid b$. Έστω k θετικός κοινός διαιρέτης των d_1 και a. Από την μεταβατικότητα της διαιρετότητας, έχουμε ότι $k \mid b$ και $k \mid a$, οπότε ο k διαιρεί τον $\gcd(a,b)=1$ και άρα $k=1$. Δείξαμε λοιπόν ότι $\gcd(d_1,a)=1$. Αφού $d_1 \mid ac$, έπεται από το Λήμμα του Ευκλείδη ότι $d_1 \mid c$. Έχουμε επίσης ότι $d_1 \mid b$, οπότε ο d_1 διαιρεί τον $d_2=\gcd(c,b)$.

(iv) Ακολουθούμε την υπόδειξη. Έστω $d=\gcd(a,c)$. Τότε $d \mid a$, $d \mid c$ συνεπάγεται ότι $d \mid (a+b)-a$ ή $d \mid b$. Επομένως, $d \mid \gcd(b,c)$. Αρκεί τώρα να δείξουμε ότι $\gcd(b,c)=1$. Από την $\gcd(a,b)=1$ έπεται ότι υπάρχουν x, y ώστε $ax+by=1$. Ακόμα, υπάρχει z ώστε $a+b=zc$. Άρα $(zc-b)x+yb=1$ ή $(y-x)b+(zx)c=1$. Έπεται λοιπόν ότι $\gcd(b,c)=1$, όπως θέλαμε να δείξουμε.

(v) Από την $\gcd(a,b)=1$ έπεται ότι υπάρχουν x, y ώστε $ax+by=1$. Πολλαπλασιάζοντας με c και τα δύο μέλη, παίρνουμε $acx+bcy=c$. Μας δίνεται τώρα ότι $d \mid ac$ και $d \mid bc$. Άρα $d \mid acx+bcy$ ή $d \mid c$.

(vi) Από την $\gcd(a,b)=1$ έπεται ότι υπάρχουν x, y ώστε $ax+by=1$. Επομένως

$$1=(ax+by)^2=a^2x^2+b(2axy+by^2)=b^2y^2+a(2bxy+ax^2)\,.$$

Έπεται από την παραπάνω σχέση ότι $\gcd(a,b^2)=\gcd(a^2,b)=1$. Βάζοντας τώρα όπου a το a^2 και εφαρμόζοντας αυτό που έχουμε ήδη δείξει, παίρνουμε ότι η $\gcd(a^2,b)=1$ συνεπάγεται την $\gcd(a^4,b)=1$ και την $\gcd(a^2,b^2)=1$. ■

Άσκηση 2.3.7. $(*)$ Να βρεθούν όλες οι συναρτήσεις $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ οι οποίες ικανοποιούν τις ακόλουθες ιδιότητες

(i) $f(x,x)=x$,

(ii) $f(x,y)=f(y,x)$,

(iii) $f(x,y)=f(x,x+y)$,

για όλους τους φυσικούς x, y.

Υπόδειξη: Υπάρχει μόνο μία τέτοια συνάρτηση και (προφανώς) έχει σχέση με όσα είδαμε στο μάθημα. Εφ' όσον υποθέσετε σωστά ποια μπορεί είναι, εργαστείτε με Ισχυρή Επαγωγή στο $x+y$ για να δείξετε ότι μόνο αυτή ικανοποιεί τις δοθείσες συνθήκες.

Λύση. Δείχνουμε ότι $f(x,y)=\gcd(x,y)$ για όλους για όλους τους φυσικούς x, y και εργαζόμαστε με Ισχυρή Επαγωγή στο άθροισμα $x+y$ για να το πετύχουμε αυτό.

Η μικρότερη τιμή που μπορεί να πάρει ο $x+y$ είναι 2 το οποίο συμβαίνει μόνο όταν $x=y=1$. Έχουμε

$$f(1,1)=1=\gcd(1,1),$$

όπου η πρώτη ισότητα ισχύει από το (i), οπότε όντως η f είναι ο μέγιστος κοινός διαιρέτης σε αυτήν την περίπτωση. Έχουμε λοιπόν την βάση της επαγωγής. Έστω τώρα ότι οι x, y είναι

φυσικοί τέτοιοι ώστε $x+y = k > 2$ και ότι έχουμε δείξει τον ισχυρισμό μας για κάθε μικρότερο άθροισμα (η επαγωγική υπόθεση). Βλέπουμε από τις (i) και (ii) ότι δεν βλάπτεται η γενικότητα να θεωρήσουμε $x < y$, ενώ από την (iii) έχουμε ότι

$$f(x, y) = f(x, x + (y - x)) = f(x, y - x).$$

Από την επαγωγική υπόθεση (την οποία μπορούμε να εφαρμόσουμε γιατί $x + (y - x) = y < x + y$), έχουμε ότι

$$f(x, y - x) = \gcd(x, y - x)\,,$$

επομένως αρκεί να δείξουμε ότι $\gcd(x, y - x) = \gcd(x, y)$. Αν $c \mid x$ και $c \mid y$, τότε $c \mid x$ και $c \mid (y - x)$. Προκύπτει λοιπόν ότι

$$\gcd(x, y) \leqslant \gcd(x, y - x).$$

Παρόμοια, αν $c \mid x$ και $c \mid (y - x)$, τότε $c \mid x$ και $c \mid y$ και άρα

$$\gcd(x, y) \geqslant \gcd(x, y - x).$$

Συνδυάζοντας τις δύο ανισότητες, παίρνουμε ότι $\gcd(x, y-x) = \gcd(x, y)$, που είναι αυτό που θέλαμε να δείξουμε. ■

Κεφάλαιο 3

3η Παράδοση

Στο σημερινό μάθημα θα αναφερθούμε στον Ευκλείδειο Αλγόριθμο και στην έννοια του ελάχιστου κοινού πολλαπλασίου.

3.1 Ο Ευκλείδειος Αλγόριθμος

Στο προηγούμενο μάθημα μιλήσαμε για τον μέγιστο κοινό διαιρέτη δύο ακεραίων. Ας υποθέσουμε τώρα ότι μας δίνονται δύο ακέραιοι a, b καθένας εκ των οποίων έχει δεκάδες ψηφία και μας ζητούν να υπολογίσουμε τον μέγιστο κοινό διαιρέτη τους. Ένα απλοϊκό σχέδιο θα ήταν να βρούμε (με όποια εργαλεία διαθέτουμε στο οπλοστάσιό μας) όλους τους διαιρέτες καθενός εκ των a, b και μετά να συγκρίνουμε αυτές τις δύο λίστες. Ο μεγαλύτερος αριθμός που είναι κοινός και στις δύο λίστες είναι ο αριθμός που ψάχνουμε.

Στην πράξη όμως το να βρει κανείς τους διαιρέτες ενός (πιθανώς αρκετά μεγάλου) αριθμού είναι δύσκολο πρόβλημα. Ο Ευκλείδειος Αλγόριθμος, ο οποίος βασίζεται πρακτικά στον Αλγόριθμο της Διαίρεσης και σε μία απλή παρατήρηση, είναι η γρηγορότερη μέθοδος για να βρίσκουμε τον μέγιστο κοινό διαιρέτη δύο αριθμών.

Ξεκινούμε λοιπόν ως εξής: αν a, b ακέραιοι, βλέπουμε εύκολα ότι $\gcd(|a|, |b|) = \gcd(a, b)$, οπότε αρκούμαστε στο να υποθέσουμε ότι οι a, b είναι φυσικοί. Έπειτα, εφαρμόζουμε τον Αλγόριθμο της Διαίρεσης και παίρνουμε

$$a = q_1 b + r_1 \qquad 0 \leqslant r_1 < b\,.$$

Αν $r_1 = 0$, τότε $b \mid a$ και $\gcd(a, b) = b$. Αν $r_1 \neq 0$, διαιρούμε τον b με τον r_1 και παίρνουμε ακεραίους q_2 και r_2 που ικανοποιούν την

$$b = q_2 r_1 + r_2 \qquad 0 \leqslant r_2 < r_1\,.$$

Αν $r_2 = 0$ σταματούμε. Διαφορετικά, συνεχίζουμε όπως πριν και παίρνουμε

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leqslant r_3 < r_2\,.$$

Η διαδικασία αυτή συνεχίζεται έως ότου βρούμε μηδενικό υπόλοιπο, έστω στην $n+1$ επανάληψη, όπου διαιρούμε τον r_{n-1} με τον r_n. Το ότι κάποια στιγμή θα εμφανιστεί μηδενικό υπόλοιπο είναι συνέπεια της παρατήρησης ότι η ακολουθία

$$b > r_1 > r_2 > \ldots \geqslant 0$$

περιέχει το πολύ b αριθμούς. Έχουμε λοιπόν το ακόλουθο σύστημα εξισώσεων.

$$\begin{aligned} a &= q_1 b + r_1 & 0 < r_1 < b \\ b &= q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ &\vdots & \vdots \\ r_{n-2} &= q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Αυτό που ισχυριζόμαστε τώρα είναι ότι ο r_n, το τελευταίο μη μηδενικό υπόλοιπο, είναι ίσος με $\gcd(a, b)$. Για την απόδειξη βασιζόμαστε στο παρακάτω λήμμα.

Λήμμα 3.1.1. *Αν $a = qb + r$, τότε $\gcd(a, b) = \gcd(b, r)$.*

Απόδειξη. Έστω $d = \gcd(a, b)$. Οι σχέσεις $d \mid a$ και $d \mid b$ συνεπάγονται ότι $d \mid (a - qb)$ ή $d \mid r$. Επομένως ο d είναι κοινός διαιρέτης των b, r. Από την άλλη, αν ο c είναι ένας κοινός διαιρέτης των b και r, τότε $c \mid (qb + r)$, οπότε $c \mid a$. Άρα ο c είναι κοινός διαιρέτης των a και b και έτσι $c \leqslant d$. Προκύπτει τώρα από τον ορισμό του $\gcd(b, r)$ ότι $d = \gcd(b, r)$. ■

Χρησιμοποιώντας τώρα το παραπάνω λήμμα (επαγωγικά), έχουμε τις διαδοχικές ισότητες

$$\gcd(a, b) = \gcd(b, r_1) = \ldots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n \,,$$

όπως ισχυριστήκαμε.

Είδαμε στο Θεώρημα 2.2.6 του προηγούμενου μαθήματος ότι ο $\gcd(a, b)$ μπορεί να εκφραστεί ως $ax+by$, αλλά η απόδειξη του θεωρήματος δεν μας καθοδηγεί πώς να βρούμε τους ακεραίους x, y. Ας δούμε τώρα πώς μπορούμε να το πετύχουμε αυτό με τον Ευκλείδειο Αλγόριθμο.

Ξεκινώντας με την προτελευταία ισότητα, γράφουμε

$$r_n = r_{n-2} - q_n r_{n-1} \,.$$

Λύνουμε τώρα την προηγούμενή της ισότητα ως προς r_{n-1} και αντικαθιστούμε παίρνοντας

$$r_n = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = (1 + q_n q_{n-1}) r_{n-2} + (-q_n) r_{n-3} \,.$$

Αυτό αναπαριστά τον r_n ως γραμμικό συνδυασμό των r_{n-2} και r_{n-3}. Συνεχίζοντας προς τα πίσω στο σύστημα εξισώσεων που προκύπτει από τον Αλγόριθμο, απαλείφουμε διαδοχικά τα υπόλοιπα $r_{n-1}, r_{n-2}, \ldots r_2, r_1$ έως ότου φτάσουμε στο στάδιο όπου ο $r_n = \gcd(a, b)$ έχει εκφραστεί ως γραμμικός συνδυασμός των a και b.

Παράδειγμα 3.1.2. Θα υπολογίσουμε τον μέγιστο κοινό διαιρέτη των 12378 και 3054. Διαδοχικές εφαρμογές του Αλγορίθμου της Διαίρεσης μας δίνουν

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162 \\ 3054 &= 18 \cdot 162 + 138 \\ 162 &= 1 \cdot 138 + 24 \\ 138 &= 5 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 + 0 \,. \end{aligned}$$

Από την συζήτηση που προηγήθηκε, προκύπτει ότι ο 6, το τελευταίο μη μηδενικό υπόλοιπο, είναι ο μέγιστος κοινός διαιρέτης των 12378 και 3054. Για να αναπαραστήσουμε τώρα τον 6 ως γραμμικό συνδυασμό των φυσικών 12378 και 3054, ξεκινούμε με την προτελευταία ισότητα και απαλείφουμε διαδοχικά τα υπόλοιπα $18, 24, 138, 162$ ως εξής:

$$\begin{aligned}
6 &= 24 - 18 \\
&= 24 - (138 - 5 \cdot 24) \\
&= 6 \cdot 24 - 138 \\
&= 6(162 - 138) - 138 \\
&= 6 \cdot 162 - 7 \cdot 138 \\
&= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\
&= 132 \cdot 162 - 7 \cdot 3054 \\
&= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\
&= 132 \cdot 12378 + (-535)3054\,.
\end{aligned}$$

Έχουμε λοιπόν ότι

$$6 = \gcd(12378, 3054) = 12378x + 3054y\,,$$

όπου $x = 132$ και $y = -535$.

Σχόλιο 3.1.3. Ο Γάλλος μαθηματικός Gabriel Lamé (1795-1870) απέδειξε ότι ο αριθμός των βημάτων που χρειάζεται ο Ευκλείδειος Αλγόριθμος για να τερματίσει, είναι το πολύ 5 φορές ο αριθμός των ψηφίων του μικρότερου από τους δύο ακεραίους, ενώ ο μέγιστος αριθμός βημάτων που χρειάζεται ο Αλγόριθμος, είναι όταν οι ακέραιοι είναι διαδοχικοί αριθμοί Fibonacci. Μία ακόμα ενδιαφέρουσα παρατήρηση είναι ότι για κάθε $n > 0$, μπορούμε να βρούμε ακεραίους a_n, b_n ώστε ο Ευκλείδειος Αλγόριθμος να περατώνεται σε ακριβώς n βήματα.

Συνέπεια του Ευκλείδειου Αλγορίθμου είναι το παρακάτω αποτέλεσμα.

Θεώρημα 3.1.4. *Αν $k > 0$, τότε $\gcd(ka, kb) = k \gcd(a, b)$.*

Απόδειξη. Αν πολλαπλασιάσουμε τις εξισώσεις που εμφανίζονται στον Αλγόριθμο του Ευκλείδη για τους ακεραίους a, b με τον k, παίρνουμε

$$\begin{aligned}
ak &= q_1(bk) + r_1k & 0 < r_1k < bk \\
bk &= q_2(r_1k) + r_2k & 0 < r_2k < r_1k \\
&\vdots & \vdots \\
r_{n-2}k &= q_n(r_{n-1}k) + r_nk & 0 < r_nk < r_{n-1}k \\
r_{n-1}k &= q_{n+1}(r_nk) + 0
\end{aligned}$$

Αυτός όμως είναι απλά ο Ευκλείδειος Αλγόριθμος εφαρμοσμένος στους ακεραίους ak, bk και έτσι ο μέγιστος κοινός διαιρέτης τους είναι το τελευταίο μη μηδενικό υπόλοιπο r_nk. Δηλαδή

$$\gcd(ka, kb) = r_nk = k \gcd(a, b)\,,$$

που είναι ακριβώς ο ισχυρισμός του θεωρήματος. ■

Έχουμε ακόμα το επόμενο.

Πόρισμα 3.1.5. *Για κάθε ακέραιο $k \neq 0$, έχουμε* $\gcd(ka, kb) = |k| \gcd(a, b)$.

Απόδειξη. Αρκεί να θεωρήσουμε την περίπτωση $k < 0$. Τότε $-k = |k| > 0$ και από το Θεώρημα 3.1.4 προκύπτει ότι

$$\begin{aligned} \gcd(ak, bk) &= \gcd(-ak, -bk) \\ &= \gcd(a|k|, b|k|) \\ &= |k| \gcd(a, b)\,, \end{aligned}$$

όπως θέλαμε να δείξουμε. ■

Χρησιμοποιώντας για παράδειγμα το Θεώρημα 3.1.4, βλέπουμε ότι

$$\gcd(12, 30) = 3 \gcd(4, 10) = 3 \cdot 2 \gcd(2, 5) = 6 \cdot 1 = 6\,.$$

3.2 Το Ελάχιστο Κοινό Πολλαπλάσιο

Μία έννοια στην οποία δεν έχουμε αναφερθεί ακόμα και η οποία είναι εφάμιλλη αυτής του μέγιστου κοινού διαιρέτη, είναι η έννοια του *ελάχιστου κοινού πολλαπλασίου*. Ένας ακέραιος c λέγεται κοινό πολλαπλάσιο δύο μη μηδενικών ακεραίων a και b όταν $a \mid c$ και $b \mid c$. Ο ακέραιος 0 είναι προφανώς κοινό πολλαπλάσιο των a και b, ενώ οι ab και $-(ab)$ είναι μη τετριμμένα παραδείγματα κοινών πολλαπλασίων. Από την Αρχή του Ελαχίστου, το σύνολο των θετικών κοινών πολλαπλασίων των a, b περιέχει έναν ελάχιστο ακέραιο τον οποίο καλούμε το ελάχιστο κοινό πολλαπλάσιο των a και b. Ο «επίσημος» ορισμός έχει ως εξής.

Ορισμός 3.2.1. Το **ελάχιστο κοινό πολλαπλάσιο** δύο μη μηδενικών ακεραίων a και b, που συμβολίζεται με $\operatorname{lcm}(a, b)$, είναι ο θετικός ακέραιος m που ικανοποιεί τα εξής:

(i) $a \mid m$ και $b \mid m$.

(ii) Αν $a \mid c$ και $b \mid c$, όπου $c > 0$, τότε $m \leqslant c$.

Έχουμε, φερ' ειπείν, ότι τα θετικά κοινά πολλαπλάσια των ακεραίων -12 και 30 είναι τα $60, 120, 180, \ldots$. Επομένως, $\operatorname{lcm}(-12, 30) = 60$. Από όσα έχουμε αναφέρει μέχρι τώρα, προκύπτει άμεσα ότι για μη μηδενικούς ακέραιους a, b, το $\operatorname{lcm}(a, b)$ πάντα υπάρχει και ικανοποιεί την $\operatorname{lcm}(a, b) \leqslant |ab|$. Στο επόμενο θεώρημα θα δούμε πώς συνδέονται οι έννοιες του ελάχιστου κοινού πολλαπλασίου και του μέγιστου κοινού διαιρέτη.

Θεώρημα 3.2.2. *Αν a, b φυσικοί, τότε*

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab\,.$$

Απόδειξη. Θέτουμε $d = \gcd(a, b)$ και γράφουμε $a = dr$, $b = ds$ για φυσικούς r, s. Αν τώρα $m = ab/d$, τότε $m = as = rb$, επομένως ο m είναι (θετικό) κοινό πολλαπλάσιο των a, b.

Έστω τώρα c φυσικός που είναι κοινό πολλαπλάσιο των a, b. Συγκεκριμένα, ας πούμε ότι $c = au = bv$. Γνωρίζουμε ότι υπάρχουν ακέραιοι x, y τέτοιοι ώστε $d = ax + by$. Επομένως,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \left(\frac{c}{b}\right) x + \left(\frac{c}{a}\right) y = vx + uy\,.$$

Έπεται από την παραπάνω εξίσωση ότι $m \mid c$ και άρα $m \leqslant c$. Σύμφωνα με τον Ορισμό 3.2.1, $m = \operatorname{lcm}(a, b)$, δηλαδή

$$\operatorname{lcm}(a, b) = \frac{ab}{d} = \frac{ab}{\gcd(a, b)},$$

που είναι αυτό που θέλαμε να δείξουμε. ■

Κάνουμε ξεχωριστή μνεία στην ακόλουθη απόρροια του Θεωρήματος 3.2.2.

Πόρισμα 3.2.3. *Για οποιαδήποτε επιλογή φυσικών a, b, έχουμε ότι $\operatorname{lcm}(a, b) = ab$, αν και μόνο αν $\gcd(a, b) = 1$.*

Η αξία του Θεωρήματος 3.2.2 έγκειται στο ότι ο υπολογισμός του ελάχιστου κοινού πολλαπλασίου δύο ακεραίων a, b ανάγεται στην εύρεση του μέγιστου κοινού διαιρέτη τους, ο οποίος με την σειρά του υπολογίζεται από τον Αλγόριθμο του Ευκλείδη. Είδαμε προηγουμένως, για παράδειγμα, ότι $\gcd(12378, 3054) = 6$, επομένως

$$\operatorname{lcm}(12378, 3054) = \frac{12378 \cdot 3054}{6} = 6300402.$$

Κλείνουμε το σημερινό μάθημα αναφέροντας ότι η έννοια του μέγιστου κοινού διαιρέτη μπορεί να γενικευθεί σε περισσότερους από δύο ακεραίους με τον προφανή τρόπο. Αν έχουμε, για παράδειγμα, τρεις ακεραίους a, b, c, οι οποίοι δεν είναι όλοι 0, τότε ο $\gcd(a, b, c)$ ορίζεται ως ο φυσικός d με τις ακόλουθες ιδιότητες:

(i) Ο d είναι διαιρέτης καθενός εκ των a, b, c.

(ii) Αν ο e διαιρεί τους a, b, c, τότε $e \leqslant d$.

Παραδείγματος χάριν, $\gcd(39, 42, 54) = 3$ και $\gcd(49, 210, 350) = 7$. Χρειάζεται προσοχή όμως. Ενδέχεται να έχουμε $\gcd(a, b, c) = 1$ χωρίς οι a, b, c να είναι σχετικά πρώτοι ανά δύο. Αυτό φαίνεται π.χ. στην τριάδα των φυσικών 6, 10 και 15.

3.3 Ασκήσεις

Άσκηση 3.3.1. Να δειχθεί ότι αν a, b, c είναι ακέραιοι και οι a, b διαιρούν και οι δύο τον c, τότε και ο $\operatorname{lcm}(a, b)$ διαιρεί τον c.

Απόδειξη. Αρκεί να δείξουμε ότι $\operatorname{lcm}(a, b) \mid |c|$, οπότε μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι $c > 0$. Εφ' όσον ο c είναι κοινό πολλαπλάσιο των a, b, έχουμε ότι $\operatorname{lcm}(a, b) \leqslant c$. Από τον Αλγόριθμο της Διαίρεσης προκύπτει ότι υπάρχουν q, r τέτοιοι ώστε

$$c = q \cdot \operatorname{lcm}(a, b) + r,$$

όπου $0 \leqslant r < \operatorname{lcm}(a, b)$. Έχουμε τώρα ότι ο $r = c - q \cdot \operatorname{lcm}(a, b)$ είναι κοινό πολλαπλάσιο των a, b, αφού και ο c και ο $\operatorname{lcm}(a, b)$ είναι κοινά πολλαπλάσια των a, b. Όμως $r < \operatorname{lcm}(a, b)$ και εφ' όσον ο $\operatorname{lcm}(a, b)$ είναι το ελάχιστο κοινό πολλαπλάσιο των a, b, προκύπτει ότι $r = 0$. Επομένως $\operatorname{lcm}(a, b) \mid c$, όπως θέλαμε να δείξουμε. ■

Άσκηση 3.3.2. Να βρεθούν όλοι οι φυσικοί a, b τέτοιοι ώστε $\operatorname{lcm}(a, b) - \gcd(a, b) = 143$.

Λύση. Θέτουμε $d = \gcd(a, b)$. Αρχικά, εφ' όσον $d \mid a \mid \operatorname{lcm}(a, b)$, βλέπουμε ότι ο d διαιρεί τον $143 = \operatorname{lcm}(a, b) - \gcd(a, b)$. Έχουμε λοιπόν να εξετάσουμε τις περιπτώσεις $d = 1$, $d = 11$, $d = 13$ και $d = 143$. Γράφουμε τώρα $a = md$ και $b = nd$, οπότε έχουμε $\gcd(m, n) = 1$.

(i) Αν $d = 1$, τότε η σχέση $\operatorname{lcm}(a, b) - \gcd(a, b) = 143$ γίνεται $mn = 144$ και αφού $\gcd(m, n) = 1$, έχουμε τις περιπτώσεις $a = m = 16$ και $b = n = 9$ όπως και $a = m = 1$ και $b = n = 144$.

(ii) Αν $d = 11$, τότε $mn = 14$ και άρα $m = 2$ και $n = 7$ (που δίνουν $a = 22$ και $b = 77$), όπως και $m = 1$ και $n = 14$ (που δίνουν $a = 11$ και $b = 154$).

(iii) Αν $d = 13$, παίρνουμε $a = 39$ και $b = 52$ καθώς και $a = 13$ και $b = 156$.

(iv) Αν $d = 143$, παίρνουμε $a = 143$ και $b = 286$.

Άρα οι λύσεις είναι οι $\{\{1, 144\}, \{9, 16\}, \{11, 154\}, \{13, 156\}, \{22, 77\}, \{39, 52\}, \{143, 286\}\}$. ■

Άσκηση 3.3.3. Έστω a, b, c φυσικοί. Δείξτε ότι

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c)\,.$$

Χρησιμοποιήστε ό,τι δείξατε για να υπολογίσετε τον $\gcd(132, 102, 36)$ και να βρείτε $x, y, z \in \mathbb{Z}$ τέτοιους ώστε

$$\gcd(132, 102, 36) = 132x + 102y + 36z\,.$$

Απόδειξη. Έστω $d_1 = \gcd(a, b, c)$ και $d_2 = \gcd(\gcd(a, b), c)$. Έχουμε ότι $d_1 \mid a$ και $d_1 \mid b$, οπότε $d_1 \mid \gcd(a, b)$. Ακόμα, $d_1 \mid c$, οπότε $d_1 \mid d_2$. Από την άλλη, έχουμε $d_2 \mid \gcd(a, b)$, οπότε προκύπτει ότι $d_2 \mid a$ και $d_2 \mid b$. Εφ' όσον $d_2 \mid c$, παίρνουμε $d_2 \mid d_1$. Από τις δύο σχέσεις $d_1 \mid d_2$ και $d_2 \mid d_1$ προκύπτει ότι $d_1 = d_2$.

Από τον Ευκλείδειο Αλγόριθμο έχουμε

$$\begin{aligned} 132 &= 102 \cdot 1 + 30 \\ 102 &= 30 \cdot 3 + 12 \\ 30 &= 12 \cdot 2 + 6 \\ 12 &= 6 \cdot 2 + 0 \end{aligned}$$

Έπεται λοιπόν ότι $\gcd(132, 102) = 6$ και άρα

$$\gcd(132, 102, 36) = \gcd(\gcd(132, 102), 36) = \gcd(36, 6) = 6\,,$$

όπου η πρώτη ισότητα προκύπτει από αυτό που δείξαμε στο πρώτο μέρος της άσκησης. Από την σειρά εξισώσεων που προέκυψε από τον Αλγόριθμο του Ευκλείδη, έχουμε διαδοχικά ότι

$$\begin{aligned} 6 &= 30 - 12 \cdot 2 = 30 - (102 - 3 \cdot 30) \cdot 2 = 7 \cdot 30 - 2 \cdot 102 \\ &= 7 \cdot (132 - 102) - 102 \cdot 2 = 7 \cdot 132 - 9 \cdot 102 \end{aligned}$$

Από την άλλη, έχουμε $7 \cdot 6 + (-1) \cdot 36 = 6$, οπότε

$$7 \cdot (7 \cdot 132 - 9 \cdot 102) - 36 = 6\,,$$

από την οποία έπεται ότι

$$49 \cdot 132 + (-63) \cdot 102 + (-1) \cdot 36 = 6\,.$$

Επομένως μπορούμε να διαλέξουμε $x = 49$, $y = -63$ και $z = -1$. ■

Άσκηση 3.3.4. Αληθεύει ότι αν οι φυσικοί a, b είναι σχετικά πρώτοι, τότε ισχύει ότι $\gcd(a^2, ab, b^2) = 1$;

Λύση. Ναι. Αν $\gcd(a, b) = 1$, τότε $\gcd(a^2, b^2) = 1$. Αυτό είναι κάτι που δείξαμε στην Άσκηση 2.3.6. Επομένως,

$$\gcd(a^2, b^2, ab) = \gcd(\gcd(a^2, b^2), ab) = \gcd(1, ab) = 1\,,$$

όπου η πρώτη ισότητα στην παραπάνω εξίσωση προκύπτει από αυτό που δείξαμε στην προηγούμενη άσκηση. ■

Άσκηση 3.3.5. $(*)$ Έστω $v_1, v_2, \ldots$ μία γνήσια αύξουσα ακολουθία φυσικών αριθμών. Να δείξετε ότι η σειρά

$$\sum_{n=1}^{\infty} \frac{1}{\operatorname{lcm}(v_n, v_{n+1})}$$

συγκλίνει.

Υπόδειξη: Βρείτε κατάλληλη ακολουθία (w_n) τέτοια ώστε $1/\operatorname{lcm}(v_n, v_{n+1}) \leqslant w_n$ για κάθε φυσικό n και η σειρά $\sum_{n=1}^{\infty} w_n$ να συγκλίνει. Συγκεκριμένα, προσπαθήστε να δημιουργήσετε ένα τηλεσκοπικό άθροισμα.

Απόδειξη. Αν $a > b$, τότε $a - b \geqslant \gcd(a, b)$, αφού ο $a - b$ είναι φυσικός που διαιρείται με τον $\gcd(a, b)$. Γνωρίζουμε επίσης από το Θεώρημα 3.2.2 ότι $\operatorname{lcm}(a, b)\gcd(a, b) = ab$. Επομένως,

$$(v_{n+1} - v_n)\operatorname{lcm}(v_{n+1}, v_n) \geqslant \gcd(v_{n+1}, v_n)\operatorname{lcm}(v_{n+1}, v_n) = v_{n+1} \cdot v_n$$

και από αυτήν την ανισότητα προκύπτει ότι

$$\frac{1}{\operatorname{lcm}(v_{n+1}, v_n)} \leqslant \frac{v_{n+1} - v_n}{v_{n+1} \cdot v_n} = \frac{1}{v_n} - \frac{1}{v_{n+1}}\,.$$

Παρατηρούμε τώρα ότι για κάθε φυσικό N έχουμε

$$\sum_{n=1}^{N} \left(\frac{1}{v_n} - \frac{1}{v_{n+1}}\right) = \left(\frac{1}{v_1} - \frac{1}{v_2}\right) + \left(\frac{1}{v_2} - \frac{1}{v_3}\right) + \ldots + \left(\frac{1}{v_N} - \frac{1}{v_{N+1}}\right) = \frac{1}{v_1} - \frac{1}{v_{N+1}}$$

και εφ' όσον $\lim_{n\to\infty} v_n = \infty$, έχουμε ότι

$$\sum_{n=1}^{\infty} \left(\frac{1}{v_n} - \frac{1}{v_{n+1}}\right) = \lim_{N\to\infty} \left(\frac{1}{v_1} - \frac{1}{v_{N+1}}\right) = \frac{1}{v_1}.$$

Από το Κριτήριο Σύγκρισης έπεται ότι η σειρά στην εκφώνηση της άσκησης συγκλίνει, αφού φράσσεται εκ των άνω από συγκλίνουσα σειρά. ■

Κεφάλαιο 4

4η Παράδοση

Σε αυτό το μάθημα θα εισαγάγουμε και θα μελετήσουμε την κεντρικότερη έννοια της Θεωρίας Αριθμών, αυτή των *πρώτων αριθμών*, και θα δούμε το σημαντικότερο ίσως θεώρημά της, το Θεμελιώδες Θεώρημα της Αριθμητικής.

4.1 Οι Πρώτοι Αριθμοί

Ορισμός 4.1.1. Ένας φυσικός $p > 1$ καλείται **πρώτος αριθμός** ή απλά **πρώτος**, αν οι μόνοι θετικοί διαιρέτες του είναι οι 1 και p. Αν ένας φυσικός μεγαλύτερος του 1 δεν είναι πρώτος, τότε καλείται **σύνθετος**.

Μεταξύ των πρώτων 10 φυσικών οι $2, 3, 5, 7$ είναι πρώτοι, ενώ οι $4, 6, 8, 9, 10$ είναι σύνθετοι. Προσέξτε ότι ο 2 είναι ο μοναδικός άρτιος πρώτος, ενώ ο 1, σύμφωνα με τον ορισμό μας, δεν θεωρείται ούτε πρώτος ούτε σύνθετος. Στο εξής τα γράμματα p, q θα συμβολίζουν, ως επί το πλείστον, πρώτους αριθμούς.

Η Πρόταση 14 του Βιβλίου IX των Στοιχείων του Ευκλείδη περιέχει (τουλάχιστον μερικώς) το αποτέλεσμα που αργότερα έγινε γνωστό ως το *Θεμελιώδες Θεώρημα της Αριθμητικής*[1] κατά το οποίο κάθε φυσικός διάφορος του 1 αναλύεται με μοναδικό τρόπο σε γινόμενο πρώτων. Βλέπουμε λοιπόν ότι ένας φυσικός $a > 1$ είναι είτε πρώτος ή, χάριν του Θεμελιώδους Θεωρήματος, γράφεται ως γινόμενο πρώτων μοναδικά. Υπ' αυτήν την έννοια, οι πρώτοι είναι τα δομικά συστατικά των φυσικών και κατ' επέκτασιν και όλων των ακεραίων.

Δεν είναι επομένως παράξενο που οι πρώτοι συναρπάζουν τους μαθηματικούς εδώ και χιλιάδες χρόνια, ενώ είναι αξιοπρόσεκτο τι έχουμε καταφέρει να αποδείξουμε για τους πρώτους. (Εξίσου αξιοπρόσεκτο πάντως είναι και το τι *δεν* έχουμε καταφέρει να αποδείξουμε γι' αυτούς!)

Ξεκινούμε με την απλή παρατήρηση ότι ο 3 διαιρεί τον 36, ενώ ο 36 μπορεί να γραφεί ως γινόμενο με τους εξής τρόπους:

$$6 \cdot 6 = 9 \cdot 4 = 12 \cdot 3 = 18 \cdot 2\,.$$

Σε κάθε περίπτωση, ο 3 διαιρεί τουλάχιστον έναν από τους όρους που εμφανίζονται στα γινόμενα. Αυτό είναι χαρακτηριστικό του επόμενου γενικότερου αποτελέσματος.

[1] Στην πραγματικότητα η πρώτη διατύπωση και απόδειξη του Θ.Θ.Α. όπως θα το παρουσιάσουμε εμφανίζεται για πρώτη φορά στο βιβλίο του Gauss Disquisitiones Arithmeticae. Θα συναντήσουμε λίγο αργότερα ξανά αυτό το όνομα αλλά και το βιβλίο.

Θεώρημα 4.1.2. *Αν p πρώτος και $p \mid ab$, τότε $p \mid a$ ή $p \mid b$.*

Απόδειξη. Αν $p \mid a$, το ζητούμενο ισχύει και δεν υπάρχει κάτι άλλο να δείξουμε. Ας υποθέσουμε λοιπόν ότι $p \nmid a$. Εφ' όσον οι μόνοι θετικοί διαιρέτες του p είναι οι 1 και p, βλέπουμε ότι $\gcd(p, a) = 1$. Από το Λήμμα του Ευκλείδη επομένως (Θεώρημα 2.2.11), παίρνουμε ότι $p \mid b$. ■

Είναι εύκολο να επεκτείνουμε το παραπάνω θεώρημα σε περισσότερους από δύο όρους.

Πόρισμα 4.1.3. *Αν p πρώτος και $p \mid a_1 a_2 \cdots a_n$, τότε $p \mid a_k$ για κάποιον k, όπου $1 \leqslant k \leqslant n$.*

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στο n. Όταν $n = 1$, είναι ξεκάθαρο ότι το ζητούμενο ισχύει, ενώ όταν $n = 2$, το ζητούμενο προκύπτει από το Θεώρημα 4.1.2. Για την επαγωγική μας υπόθεση τώρα, ας υποθέσουμε ότι $n > 2$ και ότι όποτε ο p διαιρεί ένα γινόμενο με λιγότερους από n όρους, τότε ο p διαιρεί τουλάχιστον έναν από αυτούς. Έχουμε εξ υποθέσεως ότι $p \mid a_1 a_2 \cdots a_n$. Το Θεώρημα 4.1.2 μας δίνει ότι είτε $p \mid a_n$ είτε $p \mid a_1 a_2 \cdots a_{n-1}$. Αν $p \mid a_n$, έχουμε τελειώσει, ενώ αν $p \mid a_1 a_2 \cdots a_{n-1}$, η επαγωγική υπόθεση εξασφαλίζει ότι $p \mid a_k$ για κάποια επιλογή του δείκτη k, όπου $1 \leqslant k \leqslant n$. Άρα ο p διαιρεί τουλάχιστον έναν από τους ακεραίους $a_1, a_2, \ldots, a_n$ και έτσι η επαγωγή μας έχει ολοκληρωθεί. ■

Πόρισμα 4.1.4. *Αν οι $p, q_1, q_2, \ldots, q_n$ είναι πρώτοι και $p \mid q_1 q_2 \cdots q_n$, τότε $p = q_k$ για κάποιον k, όπου $1 \leqslant k \leqslant n$.*

Απόδειξη. Από το Πόρισμα 4.1.3 έχουμε ότι υπάρχει δείκτης k με $1 \leqslant k \leqslant n$ τέτοιος ώστε $p \mid q_k$. Ο q_k είναι πρώτος όμως και άρα διαιρείται μόνο από τους 1 και q_k. Αφού $p > 1$, έπεται ότι $p = q_k$. ■

Με αυτήν την προετοιμασία, είμαστε έτοιμοι να αποδείξουμε το επόμενο σημαντικό θεώρημα.

4.2 Το Θεμελιώδες Θεώρημα της Αριθμητικής

Όπως αναφέραμε πρωτύτερα, σύμφωνα με το Θεμελιώδες Θεώρημα κάθε φυσικός αναλύεται σε γινόμενο πρώτων με «ουσιαστικά» μοναδικό τρόπο. Η λέξη «ουσιαστικά» ενέχει μια γλωσσική αμφισημία την οποία πρέπει να ξεκαθαρίσουμε:

η παραγοντοποίηση $2 \cdot 2 \cdot 3$ του αριθμού 12 *δεν θεωρείται διαφορετική* από την $2 \cdot 3 \cdot 2$.

Θεώρημα 4.2.1 (Θεμελιώδες Θεώρημα της Αριθμητικής). *Κάθε φυσικός $n > 1$ είτε είναι πρώτος είτε γινόμενο πρώτων και η αναπαράσταση αυτή είναι μοναδική αν αγνοήσουμε την σειρά με την οποία εμφανίζονται οι όροι.*

Απόδειξη. Για το «υπαρξιακό» κομμάτι της απόδειξης θα χρησιμοποιήσουμε Ισχυρή Επαγωγή (Θεώρημα 1.2.6). Για $n = 2$ το ζητούμενο προφανώς ισχύει, οπότε υποθέτουμε ότι $n > 2$. Ο n τώρα είτε είναι πρώτος είτε σύνθετος. Αν είναι πρώτος, η απόδειξη έχει τελειώσει. Μπορούμε επομένως να υποθέσουμε ότι ο n είναι σύνθετος.

Έπεται τότε ότι υπάρχει φυσικός d, με $1 < d < n$, ώστε $d \mid n$. Μεταξύ όλων των d με αυτήν την ιδιότητα, έστω p_1 ο ελάχιστος. (Η επιλογή αυτή καθίσταται δυνατή από την Αρχή του Ελαχίστου.) Ισχυριζόμαστε τώρα ότι ο p_1 είναι πρώτος. Διαφορετικά, ο p_1 έχει διαιρέτη κάποιον q με $1 < q < p_1$, επομένως ο q διαιρεί τον p_1 και άρα και τον n. Αυτό όμως έρχεται σε αντίφαση με την επιλογή του p_1 ως ελαχίστου θετικού διαιρέτη του n μεγαλύτερου του 1.

Είμαστε σε θέση τώρα να γράψουμε $n = p_1 n_1$, όπου ο p_1 είναι πρώτος και $1 < n_1 < n$. Εφαρμόζοντας την επαγωγική υπόθεση στον φυσικό n_1, έχουμε ότι ο n_1 είναι γινόμενο πρώτων. Έπεται λοιπόν ότι και ο $n = p_1 n_1$ είναι γινόμενο πρώτων και η επαγωγή μας είναι πλήρης.

Μας μένει τώρα να αποδείξουμε ότι η γραφή του n σε γινόμενο πρώτων είναι «ουσιαστικά» μοναδική. Ας υποθέσουμε αντίθετα ότι υπάρχει φυσικός n που έχει δύο γραφές. Για παράδειγμα

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad r \leqslant s\,,$$

όπου οι p_i και q_j είναι όλοι πρώτοι σε αύξουσα σειρά

$$p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r \qquad q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s\,.$$

Έστω ακόμα ότι ο n είναι ο ελάχιστος φυσικός που έχει τουλάχιστον δύο τέτοιες αναλύσεις. Είναι προφανές ότι ο n δεν είναι πρώτος και άρα $2 \leqslant r \leqslant s$. Εφ' όσον $p_1 \mid q_1 q_2 \cdots q_s$, το Πόρισμα 4.1.4 μας δίνει ότι $p_1 = q_k$ για κάποιον δείκτη k. Άρα $p_1 \geqslant q_1$ και με ανάλογο επιχείρημα έχουμε $q_1 \geqslant p_1$. Καταλήγουμε λοιπόν ότι $p_1 = q_1$, οπότε μπορούμε να διαγράψουμε τον κοινό αυτό όρο και να πάρουμε

$$a = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s\,.$$

Ο αριθμός a είναι μικρότερος του n. Έπεται λοιπόν, από την επιλογή του n ως ελαχίστου φυσικού με τουλάχιστον δύο αναλύσεις σε γινόμενο πρώτων, ότι η ανάλυση του a είναι μοναδική και επομένως $r = s$ και $p_2 = q_2, p_3 = q_3, \ldots, p_r = q_s$. Εφ' όσον $p_1 = q_1$, βλέπουμε ότι η ανάλυση του n είναι μοναδική, κάτι που αντιφάσκει με την αρχική μας επιλογή. Καταλήγουμε λοιπόν ότι όλοι οι φυσικοί που είναι μεγαλύτεροι του 1 αναλύονται σε γινόμενο πρώτων με μοναδικό τρόπο και μ' αυτό ολοκληρώνεται η απόδειξη. ■

Είναι προφανές ότι κάποιοι από τους πρώτους που εμφανίζονται στην ανάλυση ενός φυσικού ενδεχομένως εμφανίζονται περισσότερες από μία φορές. Για παράδειγμα, $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. «Μαζεύοντας», επομένως, κοινούς όρους, μπορούμε να αναδιατυπώσουμε το Θεμελιώδες Θεώρημα της Αριθμητικής ως εξής:

Πόρισμα 4.2.2. *Κάθε φυσικός $n > 1$ δύναται να γραφεί μοναδικά σε* **κανονική μορφή**

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\,,$$

όπου κάθε k_i είναι φυσικός και κάθε p_i είναι πρώτος με $p_1 < p_2 < \ldots < p_r$ για $i = 1, 2, \ldots, r$.

Ενδεικτικά, η κανονική μορφή του φυσικού 360 είναι $360 = 2^3 \cdot 3^2 \cdot 5$. Έχουμε ακόμα

$$4725 = 3^3 \cdot 5^2 \cdot 7 \qquad \text{και} \qquad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2\,.$$

Εισάγουμε σε αυτό το σημείο έναν βολικό συμβολισμό που μας επιτρέπει να κάνουμε αναφορά στον εκθέτη ενός πρώτου που εμφανίζεται στην κανονική μορφή ενός φυσικού.

Ορισμός 4.2.3. Έστω n φυσικός και p πρώτος διαιρέτης του n. Με $v_p(n)$ θα συμβολίζουμε την μεγαλύτερη δύναμη του p που διαιρεί τον n. Τον φυσικό e δηλαδή για τον οποίο ισχύει $p^e \mid n$ και $p^{e+1} \nmid n$.

Η ανάλυση σε γινόμενο πρώτων μας παρέχει έναν ακόμη τρόπο να υπολογίζουμε τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο δύο φυσικών. Ας υποθέσουμε ότι οι

$p_1, p_2, \ldots, p_n$ είναι οι διακεκριμένοι πρώτοι που διαιρούν είτε τον a είτε τον b. Επιτρέποντας στους εκθέτες να πάρουν την τιμή 0, μπορούμε να γράψουμε

$$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \qquad b = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n}.$$

Τότε

$$\gcd(a,b) = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} \qquad \text{και} \qquad \operatorname{lcm}(a,b) = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n},$$

όπου $r_i = \min\{k_i, j_i\}$ και $s_i = \max\{k_i, j_i\}$ για $i = 1, 2, \ldots, n$. Δηλαδή ο r_i είναι ο μικρότερος και ο s_i ο μεγαλύτερος από τους εκθέτες που αντιστοιχούν στον πρώτο p_i. Στην περίπτωση των αριθμών 4725 και 17460 που είδαμε παραπάνω, έχουμε

$$4725 = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7, \qquad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

και έτσι

$$\gcd(4725, 17460) = 2^0 \cdot 3^2 \cdot 5 \cdot 7 = 315, \qquad \operatorname{lcm}(4725, 17460) = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 = 264600.$$

Ας δούμε τώρα ως εφαρμογή το επόμενο πασίγνωστο αποτέλεσμα, του οποίου η ανακάλυψη φημολογείται ότι οδήγησε σε φόνο.

Εφαρμογή 4.2.4. Θα δείξουμε ότι ο αριθμός $\sqrt{2}$ είναι άρρητος.

Έστω, αντιθέτως, ότι $\sqrt{2} = \frac{m}{n}$, όπου m, n φυσικοί. Μπορούμε να υποθέσουμε ότι οι m, n είναι σχετικά πρώτοι γιατί διαφορετικά απλοποιούμε το κλάσμα διαιρώντας αριθμητή και παρονομαστή με τον $\gcd(m,n)$ και το ζητούμενο προκύπτει από το Πόρισμα 2.2.9.

Έχουμε τώρα $m^2 = 2n^2$, από το οποίο έπεται ότι $n \mid m^2$. Αν $n > 1$, τότε το Θεμελιώδες Θεώρημα της Αριθμητικής εξασφαλίζει την ύπαρξη ενός πρώτου p τέτοιου ώστε $p \mid n$. Επομένως $p \mid m^2$ και από το Θεώρημα 4.1.2 έχουμε ότι $p \mid m$. Άρα $1 = \gcd(m,n) \geqslant p$, που είναι άτοπο. Καταλήγουμε ότι αναγκαστικά $n = 1$, που οδηγεί στην αντίφαση ότι ο φυσικός 2 είναι τέλειο τετράγωνο φυσικού. Η αρχική μας υπόθεση επομένως είναι εσφαλμένη και άρα ο $\sqrt{2}$ είναι άρρητος, όπως θέλαμε να δείξουμε. ■

Σημείωση 4.2.5. Υπάρχει, φυσικά, και πιο εύκολη απόδειξη του παραπάνω αποτελέσματος. Ο σκοπός μας στην λύση που δώσαμε ήταν να χρησιμοποιήσουμε τα βασικά αποτελέσματα στα οποία αναφερθήκαμε προηγουμένως.

Μία ακόμα αξιοσημείωτη απόδειξη δουλεύει ως εξής: έστω $\sqrt{2} = \frac{m}{n}$, όπου m, n σχετικά πρώτοι. Τότε υπάρχουν ακέραιοι r, s τέτοιοι ώστε $mr + ns = 1$. Επομένως,

$$\sqrt{2} = \sqrt{2}(mr + ns) = (\sqrt{2}m)r + (\sqrt{2}n)s = 2nr + ms.$$

Βλέπουμε λοιπόν ότι ο $\sqrt{2}$ είναι φυσικός, άτοπο.

Με παρόμοιο τρόπο μπορεί να αποδειχθεί ότι για κάθε φυσικό n που δεν είναι τετράγωνο ακεραίου ο αριθμός $\sqrt{n}$ είναι άρρητος. (Σας αφήνω να εικάσετε τι συμβαίνει ακόμα γενικότερα με τους αριθμούς $n^{\frac{1}{m}}$, όπου m φυσικός.)

4.3 Ασκήσεις

Άσκηση 4.3.1. Να αποδείξετε ότι κανένας από τους αριθμούς

$$12321, 1234321, 123454321, 12345654321, 1234567654321,$$
$$123456787654321, 12345678987654321$$

δεν είναι πρώτος.

Απόδειξη. Καθένας από τους αριθμούς αυτούς είναι τέλειο τετράγωνο. Συγκεκριμένα, έχουμε $12321 = 111^2$, $1234321 = 1111^2, \ldots,$ $12345678987654321 = 111111111^2$. ■

Άσκηση 4.3.2. Αν οι p, q είναι πρώτοι με $p \geqslant q \geqslant 5$, να δειχθεί ότι $24 \mid p^2 - q^2$.

Απόδειξη. Από το Πόρισμα 2.2.10, είναι αρκετό να δείξουμε ότι ο $p^2 - q^2$ διαιρείται και με το 8 και με το 3. Για να δείξουμε ότι $8 \mid p^2 - q^2$, παρατηρούμε ότι οι p, q είναι και οι δύο περιττοί, επομένως το Παράδειγμα 2.1.3 του δεύτερου μαθήματος μας δίνει $p^2 = 8k + 1$ και $q^2 = 8\ell + 1$ για κάποιους φυσικούς k, ℓ. Έπεται ότι ο

$$p^2 - q^2 = 8(k - \ell)$$

είναι πολλαπλάσιο του 8.

Θα δείξουμε τώρα κάτι ανάλογο και για το 3. Εφ' όσον ο $p > 3$ είναι πρώτος, έπεται ότι $p = 3m + 1$ ή $p = 3m + 2$. Στην πρώτη περίπτωση έχουμε

$$p^2 = 3(3m^2 + 2m) + 1\,,$$

ενώ στην δεύτερη

$$p^2 = 3(3m^2 + 4m + 1) + 1\,.$$

Και στις δύο περιπτώσεις λοιπόν έχουμε ότι $p^2 = 3k + 1$ για κάποιον φυσικό k και με το ίδιο επιχείρημα βρίσκουμε φυσικό ℓ ώστε $q^2 = 3\ell + 1$. Καταλήγουμε ότι

$$p^2 - q^2 = 3(k - \ell)$$

είναι πολλαπλάσιο του 3, όπως θέλαμε να δείξουμε. ■

Άσκηση 4.3.3. Αν οι p, q είναι διαδοχικοί περιττοί πρώτοι, να δείξετε ότι ο $p+q$ είναι γινόμενο τουλάχιστον τριών (όχι απαραίτητα διακεκριμένων) πρώτων.

Απόδειξη. Έχουμε $p < q$. Εφ' όσον οι p, q είναι περιττοί, μπορούμε να βρούμε φυσικό k ώστε $q = p + 2k$. Έχουμε λοιπόν ότι

$$p + q = 2(p + k)\,,$$

οπότε αρκεί να δείξουμε ότι ο $p + k$ έχει τουλάχιστον δύο πρώτους παράγοντες. Τώρα, παρατηρούμε ότι $p < p + k < q$. Εφ' όσον οι p, q είναι διαδοχικοί πρώτοι, ο $p + k$ δεν είναι πρώτος και άρα έχει τουλάχιστον 2 πρώτους παράγοντες, όπως θέλαμε να δείξουμε. ■

Άσκηση 4.3.4. Βρείτε όλους τους πρώτους οι οποίοι γράφονται και ως αθροίσματα και ως διαφορές δύο πρώτων.

Λύση. Θα αποδείξουμε ότι ο μόνος πρώτος με τις ζητούμενες ιδιότητες είναι ο 5. Πράγματι, έστω p πρώτος που μπορεί να γραφεί και ως άθροισμα και ως διαφορά δύο πρώτων. Θα πρέπει (προφανώς) να έχουμε $p > 2$ και άρα ο p είναι περιττός. Το άθροισμα και η διαφορά δύο περιττών αριθμών είναι άρτιος, άρα ο ένας από τους δύο πρώτους είναι αναγκαστικά ο 2. Θα πρέπει δηλαδή να έχουμε

$$p = r + 2 = q - 2\,,$$

όπου r, q πρώτοι. Άρα η τριάδα $(p-2, p, p+2)$ αποτελείται από περιττούς πρώτους και αυτό συμβαίνει μόνο για την τριάδα $(3, 5, 7)$. Για να δικαιολογήσουμε αυτόν τον τελευταίο ισχυρισμό, παρατηρούμε ότι μεταξύ τριών διαδοχικών περιττών αριθμών ένας τουλάχιστον διαιρείται με το 3. Επομένως έχουμε $5 = 3 + 2 = 7 - 2$. ■

Άσκηση 4.3.5. Να αποδείξετε ότι αν ο $a^n - 1$ είναι πρώτος για κάποιους φυσικούς $a > 1$ και $n > 1$, τότε $a = 2$ και ο n είναι πρώτος.

Σημείωση: Οι φυσικοί της μορφής $2^p - 1$, όπου p πρώτος, καλούνται αριθμοί Mersenne. Τους συμβολίζουμε συνήθως ως M_p στην μνήμη του Marin Mersenne $(1588 - 1648)$, ο οποίος είχε διατυπώσει ότι ο M_p είναι πρώτος για

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

και σύνθετος για όλους τους άλλους πρώτους $p < 257$. Τον ισχυρισμό αυτόν του Mersenne μπορεί να τον βρει κανείς στον πρόλογο του βιβλίου του Cogita Physico-mathematica, το οποίο δημοσιεύθηκε στο Παρίσι το 1644. Έκτοτε έχουμε βρει διάφορα λάθη στους υπολογισμούς του Mersenne: ο M_p δεν είναι πρώτος για $p = 67$ και $p = 257$, ενώ είναι πρώτος για $p = 61$, $p = 89$ και $p = 109$. Μέχρι σήμερα έχουμε βρει 51 πρώτους Mersenne, ο μεγαλύτερος εκ των οποίων είναι ο $2^{82,589,933} - 1$ με $24,862,048$ ψηφία. Θα δούμε αργότερα ότι οι πρώτοι του Mersenne συνδέονται στενά με τους λεγόμενους *τέλειους αριθμούς*.

Απόδειξη. Βλέπουμε εύκολα ότι

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1)\,,$$

όπου ο δεύτερος όρος είναι μεγαλύτερος του 1. Αφού ο $a^n - 1$ είναι πρώτος, θα πρέπει $a - 1 = 1$ ή $a = 2$.

Επιπλέον, αν ο n είναι σύνθετος, τότε υπάρχουν φυσικοί $r > 1$, $s > 1$ τέτοιοι ώστε $n = rs$ και άρα

$$a^n - 1 = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \ldots + 2^r + 1)\,,$$

όπου κάθε όρος είναι μεγαλύτερος του 1. Έπεται ότι ο $a^n - 1$ είναι σύνθετος που είναι άτοπο. ■

Άσκηση 4.3.6. Να αποδείξετε ότι αν υπάρχουν φυσικοί n και $a \geqslant 2$ τέτοιοι ώστε ο $a^n + 1$ να είναι πρώτος, τότε ο a είναι άρτιος και $n = 2^r$ για κάποιον φυσικό r.

Σημείωση: Οι πρώτοι της μορφής $2^{2^k} + 1$, όπου $k = 0, 1, 2, \ldots$, καλούνται πρώτοι του Fermat. Ο λόγος γι' αυτό είναι ότι ο Pierre de Fermat είχε ισχυριστεί το έτος 1640 (παρόλο που παραδεχόταν ότι δεν μπορούσε να το αποδείξει) ότι όλοι οι αριθμοί της μορφής $2^{2^k} + 1$ είναι πρώτοι. Εκατό χρόνια αργότερα, ο Leonhard Euler απέδειξε ότι

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417\,.$$

Ακόμα και σήμερα δεν γνωρίζουμε αν υπάρχουν πρώτοι της μορφής $2^{2^k} + 1$ για $k \geqslant 5$.

Απόδειξη. Αν ο a είναι περιττός, τότε ο $a^n + 1 \geqslant 4$ και είναι άρτιος, άρα όχι πρώτος. Από την άλλη, αν ο n έχει έναν περιττό πρώτο παράγοντα $s > 1$, τότε υπάρχει φυσικός m ώστε $n = ms$ και σ' αυτήν την περίπτωση έχουμε

$$a^n + 1 = (a^m + 1)(a^{m(s-1)} - a^{m(s-2)} + \ldots - a^m + 1)\,.$$

Εφ' όσον $s \geqslant 3$, και οι δύο παράγοντες είναι μεγαλύτεροι του 1, που αντιβαίνει στο δεδομένο ότι ο $a^n + 1$ είναι πρώτος. Άρα ο n δεν διαιρείται από περιττό αριθμό μεγαλύτερο του 1 που σημαίνει ότι ο n είναι της μορφής 2^r. ■

Κεφάλαιο 5

5η Παράδοση

Στο σημερινό μάθημα συνεχίζουμε την μελέτη των πρώτων αριθμών που ξεκινήσαμε στο προηγούμενο. Σε αδρές γραμμές, το κεντρικό ερώτημα που θα μας απασχολήσει σε αυτό και τα επόμενα μαθήματα είναι το εξής:

Πώς κατανέμονται οι πρώτοι ανάμεσα στους φυσικούς;

Συνοπτικά: στο σημερινό μάθημα θα δούμε το Κόσκινο του Ερατοσθένη, θα μιλήσουμε για την πληθικότητα των πρώτων αριθμών και θα αναφερθούμε στην ιδιότητα που έχει η ακολουθία των πρώτων να παρουσιάζει οσοδήποτε μεγάλα κενά μεταξύ διαδοχικών όρων.

5.1 Το Κόσκινο του Ερατοσθένη

Ξεκινούμε με το ακόλουθο ερώτημα:

Για τυχαίο φυσικό n τι διαδικασία μπορούμε να ακολουθήσουμε για να αποφανθούμε αν ο n είναι πρώτος ή σύνθετος; Αν είναι σύνθετος, πώς βρίσκουμε έναν πρώτο διαιρέτη του;

Η απλούστερη διαδικασία είναι η εξής: διαιρούμε τον n διαδοχικά με κάθε αριθμό μικρότερό του. Αν κάποιος φυσικός μεγαλύτερος του 1 τον διαιρεί, είναι σύνθετος. Αν όχι, τότε είναι πρώτος. Το απλοϊκό αυτό επιχείρημα όμως μπορούμε να το βελτιώσουμε με ελάχιστο κόπο, όπως θα δούμε αμέσως.

Θεώρημα 5.1.1 (Κριτήριο Ρίζας). *Κάθε σύνθετος φυσικός $n > 1$ έχει τουλάχιστον έναν πρώτο παράγοντα $p \leqslant \sqrt{n}$.*

Απόδειξη. Αν ο ακέραιος $n > 1$ είναι σύνθετος, τότε γράφεται ως $n = \ell m$, όπου $1 < \ell < n$ και $1 < m < n$. Δεν βλάπτεται η γενικότητα να θεωρήσουμε $\ell \leqslant m$, οπότε έχουμε

$$\ell^2 \leqslant \ell m = n$$

και άρα $\ell \leqslant \sqrt{n}$. Εφ' όσον $1 < \ell$, το Θεώρημα 4.2.1 μας εξασφαλίζει την ύπαρξη ενός πρώτου διαιρέτη p του ℓ. Επομένως $p \leqslant \ell \leqslant \sqrt{n}$. Επιπλέον, $p \mid \ell \mid n$ και άρα $p \mid n$. Από αυτήν την τελευταία σχέση προκύπτει το ζητούμενο. ■

Για να δούμε πώς δουλεύει το Κριτήριο Ρίζας με ένα συγκεκριμένο παράδειγμα, ας θεωρήσουμε τον αριθμό $a = 907$. Έχουμε αρχικά ότι[1] $30 < \sqrt{a} < 31$, ενώ οι πρώτοι που είναι μικρότεροι

[1] Αυτό φαίνεται και χωρίς κομπιουτεράκι.

του 30 είναι οι

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29\,.$$

Εκτελούμε τις απαραίτητες διαιρέσεις και παρατηρούμε ότι κανένας από τους παραπάνω πρώτους δεν διαιρεί τον 907 και άρα ο 907 είναι πρώτος. Το όφελος είναι προφανές. Αντί για 905 διαιρέσεις (ή, εν πάσει περιπτώσει, 453 αν προσέξουμε ότι ο μεγαλύτερος γνήσιος διαιρέτης ενός αριθμού είναι το πολύ ο μισός του), εκτελέσαμε μόνο 10. Η εφαρμογή του Κριτηρίου Ρίζας βέβαια προϋποθέτει να διαθέτουμε μία λίστα με πρώτους που θα καλύπτει το μέγεθος του ακεραίου που θέλουμε να εξετάσουμε.

Ο Ερατοσθένης ο Κυρηναίος ($276 - 194$ π.Χ.) ήταν Έλληνας μαθηματικός της αρχαιότητας με σημαντική συνεισφορά σε πολλές επιστήμες, πραγματικός πολυμαθής και διευθυντής της φημισμένης βιβλιοθήκης της Αλεξάνδρειας. Η συνεισφορά του στην Θεωρία Αριθμών είναι όμως αυτό που μας ενδιαφέρει εδώ και έχει ως εξής: είδαμε ότι αν ένας ακέραιος $a > 1$ δεν διαιρείται από κανέναν πρώτο $p \leqslant \sqrt{a}$, τότε ο a είναι αναγκαστικά πρώτος. Ο Ερατοσθένης χρησιμοποίησε αυτήν την παρατήρηση ως βάση μιας έξυπνης τεχνικής εύρεσης πρώτων, το λεγόμενο *Κόσκινο του Ερατοσθένη*.

Αν θέλουμε να βρούμε όλους τους πρώτους $\leqslant n$, γράφουμε διαδοχικά τους αριθμούς από το 2 έως το n και αφαιρούμε συστηματικά όλους τους σύνθετους διαγράφοντας όλα τα πολλαπλάσια $2p, 3p, 4p, 5p, \ldots$ των πρώτων $\leqslant \sqrt{n}$. Οι ακέραιοι που απομένουν (όσοι δηλαδή δεν «έπεσαν από το κόσκινο») είναι οι πρώτοι $\leqslant n$.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Σχήμα 5.1: Το Κόσκινο του Ερατοσθένη για $n = 100$

Για να δούμε με ένα παράδειγμα πώς λειτουργεί το Κόσκινο του Ερατοσθένη, ας υποθέσουμε ότι ψάχνουμε να βρούμε όλους τους πρώτους $\leqslant 100$.

- Ξεχωρίζουμε τον αρχικό πρώτο 2 τον οποίο και «κρατάμε» και διαγράφουμε όλα τα πολλαπλάσιά του, δηλαδή όλους τους άρτιους $\leqslant 100$.

- Ο αρχικός αριθμός από τους εναπομείναντες είναι ο 3, ο οποίος αναγκαστικά είναι πρώτος. Τον «κρατάμε» και διαγράφουμε όλα τα πολλαπλάσιά του που δεν έχουν ήδη διαγραφεί στο προηγούμενο βήμα. (Δεν κάνει καμία διαφορά αν θα ξαναδιαγράψουμε αριθμό που έχει ήδη διαγραφεί.)

- Ο αρχικός αριθμός από αυτούς που έχουν μείνει είναι ο 5 και είναι αναγκαστικά και αυτός πρώτος. Διαγράφουμε τα πολλαπλάσια του 5 που δεν έχουν ήδη διαγραφεί και εφαρμόζουμε την ίδια ακριβώς διαδικασία με τον 7, ο οποίος είναι ο μεγαλύτερος πρώτος $\leqslant \sqrt{100} = 10$.

- Αφού διαγράψουμε τα πολλαπλάσια του 7 που είναι μεγαλύτερα του 7 και δεν έχουν ήδη διαγραφεί, οι αριθμοί που μένουν είναι ακριβώς οι πρώτοι $\leqslant 100$.

Στο Σχήμα 5.1 απεικονίζεται αυτή η διαδικασία. Η διαγραφή των άρτιων αριθμών από το 4 και μετά δηλώνεται με μωβ χρώμα (το οποίο σε 'μένα μοιάζει με φούξια), των πολλαπλασίων του 3 από το 6 και μετά που δεν είναι μωβ, με μπλε, των πολλαπλασίων του 5 από το 10 και μετά που δεν είναι μωβ ή μπλε, με κίτρινο και με κόκκινο τα πολλαπλάσια του 7 που έχουν μείνει. Οι αριθμοί που παραμένουν αχρωμάτιστοι, με εξαίρεση τον 1, είναι οι πρώτοι που ψάχναμε να βρούμε.

5.2 Η πληθικότητα των Πρώτων

Ένα καίριο ερώτημα το οποίο έχουμε αφήσει αναπάντητο μέχρι στιγμής (πιο συγκεκριμένα: δεν το έχουμε θέσει καν) είναι κατά πόσο η λίστα των πρώτων αριθμών έχει τέλος· αν υπάρχει δηλαδή ένας «τελευταίος» πρώτος. Το ερώτημα αυτό απαντήθηκε πολύ νωρίς από (ποιον άλλο;) τον Ευκλείδη. Η απόδειξη που έδωσε ο Ευκλείδης είναι εξαιρετικά απλή και θεωρείται υπόδειγμα μαθηματικής κομψότητας. Επειδή το πιθανότερο είναι ότι την έχετε ήδη συναντήσει, θα την επαναλάβουμε εν τάχει τώρα και ως επίσημη απόδειξη για το θεώρημα που ακολουθεί σε λίγο, θα δούμε μία άλλη.

Το επιχείρημα του Ευκλείδη λοιπόν έχει ως εξής: έστω ότι το πλήθος των πρώτων είναι πεπερασμένο και ότι όλοι οι πρώτοι είναι οι $2, 3, 5, \ldots, p$. Θέτουμε

$$q = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1 \,.$$

Από το Θεμελιώδες Θεώρημα της Αριθμητικής ο q έχει (τουλάχιστον) έναν πρώτο διαιρέτη, έστω τον r. Τότε ο r είναι ένας από τους $2, 3, 5, \ldots, p$ και άρα διαιρεί το γινόμενο $2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$. Επομένως ο r διαιρεί την διαφορά

$$q - 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p = 1 \,,$$

που είναι άτοπο, αφού $r > 1$.

Αξίζει να σημειώσουμε εδώ ότι το επιχείρημα αυτό δεν είναι *ακριβώς* αυτό που έδωσε ο Ευκλείδης στα Στοιχεία του. Οι μαθηματικοί της εποχής του σκέφτονταν γεωμετρικά και σίγουρα δεν διέθεταν τον απαραίτητο αλγεβρικό συμβολισμό για να εκφραστούν όπως εμείς παραπάνω. (Πιθανότατα καταλάβαιναν διαφορετικά και την έννοια του απείρου.) Προσεγγίζει όμως πολύ καλά την ουσία της απόδειξής του.

Θεώρημα 5.2.1 (Η Απειρία των Πρώτων). *Υπάρχουν άπειροι πρώτοι.*

Απόδειξη. Οι αριθμοί Fermat ορίζονται από τον τύπο $F_n = 2^{2^n} + 1$, όπου n φυσικός.[2] Θα δείξουμε πρώτα ότι δύο διακεκριμένοι αριθμοί Fermat είναι σχετικά πρώτοι. Έστω F_n, F_{n+k} δύο τέτοιοι αριθμοί με $k > 0$ και m ένας κοινός διαιρέτης τους. Θέτουμε $s = 2^{2^n}$ και έχουμε

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{s^{2^k} - 1}{s + 1} = s^{2^k - 1} - s^{2^k - 2} + \ldots - 1\,,$$

και άρα $F_n \mid F_{n+k} - 2$. Επομένως,

$$m \mid F_{n+k}\,, \qquad m \mid F_{n+k} - 2\,.$$

Προκύπτει λοιπόν ότι $m \mid 2$ και, αφού ο F_n είναι περιττός, έχουμε $m = 1$, όπως θέλαμε να δείξουμε.

Έπεται τώρα ότι καθένας από τους αριθμούς $F_1, F_2, \ldots, F_n$ διαιρείται από έναν περιττό πρώτο ο οποίος δεν διαιρεί κανέναν άλλο. Ως εκ τούτου, υπάρχουν τουλάχιστον n περιττοί πρώτοι $\leqslant F_n$ και, αφού το n μπορεί να γίνει όσο μεγάλο θέλουμε, η απόδειξη είναι πλήρης. ■

Η παραπάνω απόδειξη συνήθως αποδίδεται στον Pólya. Ο Ribenboim αναφέρει στο βιβλίο του όμως ότι σύμφωνα με τον Narkiewicz, η απόδειξη πρέπει να αποδοθεί στον Goldbach, όπως προκύπτει από γράμμα του τελευταίου προς τον Euler το έτος 1730. Αν είναι όντως έτσι, η παραπάνω απόδειξη είναι η μοναδική του Goldbach που διαθέτουμε. Θα συναντήσουμε λίγο αργότερα ξανά αυτό το όνομα.

Όποιος κι αν ήταν ο πραγματικός πατέρας της απόδειξης πάντως, η κεντρική ιδέα που περιέχει είναι αρκετά απλή αλλά και πρόσφορη. Για να δείξουμε την απειρία των πρώτων, αρκεί να βρούμε μία άπειρη ακολουθία φυσικών $1 < a_1 < a_2 < \ldots$, τέτοια ώστε οι όροι της να είναι σχετικά πρώτοι ανά δύο. Τότε, αν p_1 είναι ένας πρώτος διαιρέτης του a_1, p_2 ένας πρώτος διαιρέτης του a_2 και ούτω καθεξής, προκύπτει ότι οι $p_1, p_2, \ldots,$ είναι όλοι διακεκριμένοι.

Τώρα, χωρίς να υποθέτουμε ότι η απειρία των πρώτων έχει αποδειχθεί, θα θέλαμε ίσως να έχουμε στην διάθεσή μας περισσότερες τέτοιες άπειρες ακολουθίες των οποίων οι όροι να είναι σχετικά πρώτοι ανά δύο. Σε άρθρο του το 1964, ο Edwards ασχολήθηκε με αυτό το ζήτημα και υπέδειξε διάφορες τέτοιες αναδρομικές ακολουθίες. Για παράδειγμα, αν S_0, a είναι σχετικά πρώτοι ακέραιοι με $S_0 > a \geqslant 1$, τότε η ακολουθία που ορίζεται αναδρομικά από την σχέση

$$S_n - a = S_{n-1}(S_{n-1} - a) \qquad \text{για} \quad n \geqslant 1\,,$$

αποτελείται εξ ολοκλήρου από αριθμούς που είναι σχετικά πρώτοι ανά δύο. Στην «καλύτερη» των περιπτώσεων, όταν δηλαδή $S_0 = 3$ και $a = 2$, η ακολουθία S_n ταυτίζεται με την ακολουθία των αριθμών Fermat: $S_n = F_n = 2^{2^n} + 1$.

Έχοντας δείξει ότι ο αριθμός των πρώτων είναι άπειρος, ένα επόμενο φυσιολογικό ερώτημα είναι:

Πώς συμπεριφέρεται η ακολουθία των διαδοχικών διαφορών μεταξύ πρώτων;

Αν δηλαδή συμβολίσουμε με (p_n) την ακολουθία των πρώτων αριθμών (κάτι που στην πραγματικότητα έχουμε ήδη κάνει), τι μπορούμε να πούμε για την ακολουθία $(p_n - p_{n-1})$, όπου $n \geqslant 2$;

[2] Συναντήσαμε μία έκφανση αυτών των αριθμών στην Σημείωση έπειτα από την Άσκηση 4.3.6.

Αρκούμαστε προς το παρόν να επισημάνουμε ότι αυτό είναι ένα πολύ δύσκολο ερώτημα το οποίο έχει κεντρίσει το ενδιαφέρον πολλών από τους καλύτερους μαθηματικούς της Θεωρίας Αριθμών. Αυτό που εμείς είμαστε σίγουρα σε θέση να δείξουμε είναι το ακόλουθο αποτέλεσμα.[3]

Θεώρημα 5.2.2. *Η ακολουθία των διαδοχικών διαφορών μεταξύ πρώτων δεν είναι φραγμένη.*

Απόδειξη. Για να δείξουμε το ζητούμενο, είναι αρκετό να δείξουμε ότι για κάθε φυσικό αριθμό n μπορούμε να βρούμε n συνεχόμενους φυσικούς που είναι όλοι σύνθετοι.

Αυτό τώρα το πετυχαίνουμε θεωρώντας (έξυπνα) τους n διαδοχικούς φυσικούς

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)\,.$$

Οι αριθμοί αυτοί είναι προφανώς διαδοχικοί και n το πλήθος. Επιπλέον, καθένας από τους παραπάνω φυσικούς είναι σύνθετος, διότι αν $2 \leqslant k \leqslant n+1$, τότε ο k διαιρεί τον $(n+1)!+k$ και μάλιστα γνήσια (δηλαδή με πηλίκο διάφορο της μονάδας). ■

Στα μαθηματικά (και αυτό αποτελεί προσωπική μου άποψη) υπάρχει ένα σύστημα ιδιάζουσας δικαιοσύνης το οποίο φαίνεται ότι δεν κάνει ποτέ διάλειμμα. Δεν παίρνεις ποτέ (ή τουλάχιστον σχεδόν ποτέ) ως αποτέλεσμα κάτι δυσανάλογα μεγαλύτερο της προσπάθειας που αφιέρωσες για να το αποδείξεις. Η παραπάνω απόδειξη, αν και ευρηματική, παραείναι απλή για να μας δώσει κάτι ισχυρό.

Για $n = 10$ για παράδειγμα, μας δίνει ότι οι φυσικοί

$$39916802, 39916803, \ldots, 39916811$$

είναι όλοι σύνθετοι. Παρατηρήστε όμως ότι αυτό συμβαίνει για πρώτη φορά με τους φυσικούς

$$114, 115, \ldots, 123$$

και συγκρίνετε τα σχετικά μεγέθη.

5.3 Ασκήσεις

Άσκηση 5.3.1. Παρατηρήστε ότι μπορούμε να βελτιώσουμε λίγο την απόδειξη του Θεωρήματος 5.2.2 ως εξής: έστω k φυσικός και $N = 2 \cdot 3 \cdots p$ το γινόμενο όλων των πρώτων που είναι μικρότεροι του $k+2$. Θεωρήστε τους k διαδοχικούς φυσικούς

$$N+2,\ N+3,\ N+4,\ \ldots,\ N+k,\ N+(k+1)$$

και δείξτε ότι είναι όλοι τους σύνθετοι.

Απόδειξη. Για κάθε i τέτοιο ώστε $2 \leqslant i \leqslant k+1$, ο i έχει έναν πρώτο διαιρέτη μικρότερο του $k+2$. Αυτός ο πρώτος διαιρεί επίσης τον N, διότι εμφανίζεται στο γινόμενο που ορίζει τον N και άρα διαιρεί και τον $N+i$. Προφανώς ο i διαιρεί γνήσια τον $N+i$ (δηλαδή, με πηλίκο διάφορο της μονάδας), οπότε προκύπτει ότι ο $N+i$ είναι σύνθετος. Εφ' όσον αυτό ισχύει για κάθε i τέτοιο ώστε $2 \leqslant i \leqslant k+1$, το ζητούμενο έχει δειχθεί. ■

[3] Υπενθυμίζω τον ορισμό της συνάρτησης που καλούμε «παραγοντικό». Για έναν φυσικό n, συμβολίζουμε με $n!$ το γινόμενο όλων των φυσικών $\leqslant n$. Δηλαδή, $n! = n \cdot (n-1) \cdots 2 \cdot 1$.

Άσκηση 5.3.2. Δείξτε επαγωγικά ότι για κάθε φυσικό n ισχύει ότι

$$F_0F_1F_2\cdots F_{n-1} = F_n - 2\,,$$

όπου F_i είναι ο iοστός αριθμός Fermat.

Απόδειξη. Εφαρμόζουμε επαγωγή στο n. Για $n = 1$ έχουμε $F_0 = 3$ και $F_1 - 2 = 5 - 2 = 3$, οπότε το ζητούμενο ισχύει σε αυτήν την περίπτωση. Υποθέτουμε τώρα ότι αληθεύει η ισότητα για $n = k$ και θα δείξουμε ότι ισχύει και για $n = k + 1$. Από την επαγωγική υπόθεση έχουμε

$$\begin{aligned} F_0F_1F_2\cdots F_k = (F_k - 2)F_k &= \left(2^{2^k} - 1\right)\left(2^{2^k} + 1\right) \\ &= 2^{2^{k+1}} - 1 = \left(2^{2^{k+1}} + 1\right) - 2 = F_{k+1} - 2\,, \end{aligned}$$

όπως θέλαμε να δείξουμε. ■

Άσκηση 5.3.3. Δοθέντος φυσικού $n > 2$, να αποδείξετε ότι υπάρχει πρώτος p τέτοιος ώστε $n < p < n!$.

Απόδειξη. Ας υποθέσουμε ότι δεν υπάρχει πρώτος μεταξύ των n και $n!$. Θεωρούμε τον αριθμό $N = n! - 1$. Αν ο N είναι πρώτος, έχουμε βρει έναν πρώτο μεταξύ n και $n!$, άτοπο. Αν ο N είναι σύνθετος, τότε υπάρχει πρώτος q τέτοιος ώστε $q \mid N$. Από την υπόθεσή μας όμως, δεν ισχύει ότι $n < q < n!$ αφού δεν υπάρχει πρώτος σ' αυτό το διάστημα. Άρα $q \leqslant n$ από το οποίο προκύπτει ότι $q \mid n!$. Επομένως $q \mid 1 = n! - N$ και άρα οδηγούμαστε πάλι σε άτοπο. Το ζητούμενο έχει δειχθεί. ■

Άσκηση 5.3.4. Έστω n φυσικός. Να δείξετε ότι αν ο n είναι σύνθετος, τότε $n \mid (n-1)!$ εκτός αν $n = 4$.

Απόδειξη. Θέτουμε $n = pr$, όπου p πρώτος και $r > 1$ εξ υποθέσεως. Αν $p \neq r$, τότε οι p και r εμφανίζονται ως παράγοντες στο γινόμενο $(n-1)!$ και από αυτό προκύπτει ότι ο n διαιρεί τον $(n-1)!$. Αν $p = r$, τότε $n = p^2$ και

$$(n-1)! = (p^2 - 1)(p^2 - 2)\cdots p\cdots 1\,.$$

Επομένως, για να διαιρείται ο $(n-1)!$ με τον p^2 θα πρέπει ο $(n-1)!$ να περιέχει ως παράγοντες τους p και $2p$. Δηλαδή, θα πρέπει $p^2 - m = 2p$ για κάποιον φυσικό $m \geqslant 2$. Για $p > 2$, αυτό είναι δυνατό με $m = p(p-2)$. Αν $p = 2$ (δηλαδή $n = 4$), προφανώς το ζητούμενο δεν ισχύει, αφού $4 \nmid 6$. ■

Άσκηση 5.3.5. Για ποιους θετικούς ακεραίους $n > 1$ ισχύει ότι

$$\text{ο } \sum_{j=1}^{n} j \text{ διαιρεί τον } \prod_{j=1}^{n} j\,;$$

Λύση. Παρατηρούμε αρχικά ότι

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$$

και φυσικά

$$\prod_{j=1}^{n} j = n!\,,$$

εξ ορισμού. Θέλουμε επομένως να βρούμε τους φυσικούς n για τους οποίους ο $\frac{n(n+1)}{2}$ διαιρεί τον $n!$ ή ισοδύναμα $n+1 \mid 2(n-1)!$. Αναζητούμε δηλαδή τους φυσικούς n για τους οποίους υπάρχει *φυσικός* $M = M(n)$ ώστε

$$2\frac{(n-1)!}{(n+1)} = M.$$

Αν $n+1 = p$, όπου p πρώτος, βλέπουμε ότι ο M δεν είναι φυσικός, αφού ο p δεν διαιρεί κανέναν όρο του γινομένου $2(n-1)!$. Θα πρέπει επομένως ο $n+1$ να είναι σύνθετος· δηλαδή, θα πρέπει να έχουμε $n+1 = pr$ για κάποιον πρώτο p και κάποιον φυσικό $r > 1$.

Προκύπτει τώρα, όπως και στην προηγούμενη άσκηση, ότι αν $p \neq r$, τότε οι p και r εμφανίζονται ως παράγοντες στο γινόμενο $(n-1)!$ και άρα ο M *είναι* φυσικός. Μένει λοιπόν να δούμε την περίπτωση $n+1 = p^2$ όπου και έχουμε

$$2(n-1)! = 2(p^2-2)! = 2(p^2-2)(p^2-3)\cdots p \cdots 1\,.$$

Για να διαιρεί ο p^2 τον $2(n-1)!$, πρέπει ο $2(n-1)!$ να περιέχει ως παράγοντες τους p και $2p$. Δηλαδή, θα πρέπει $p^2 - m = 2p$ για κάποιον φυσικό $m \geqslant 2$. Για $p > 2$, αυτό είναι δυνατό με $m = p(p-2)$.

Καταλήγουμε λοιπόν ότι το σύνολο των φυσικών n που αναζητούσαμε είναι εκείνοι οι $n \neq p-1$, όπου p πρώτος αριθμός. ■

Για την επόμενη άσκηση υπενθυμίζουμε ότι σύμφωνα με τον Ορισμό 4.2.3, ο φυσικός $v_p(n)$ είναι η δύναμη του p που εμφανίζεται στην κανονική μορφή του n, ενώ με $\lfloor x \rfloor$ συμβολίζουμε την οικεία συνάρτηση «ακέραιο μέρος», δηλαδή τον μεγαλύτερο ακέραιο που είναι μικρότερος ή ίσος του x.

Άσκηση 5.3.6. Να δειχθεί ο ακόλουθος τύπος που οφείλεται στον Legendre. Αν n φυσικός και p πρώτος διαιρέτης του n, τότε

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

Απόδειξη. Πριν ξεκινήσουμε την απόδειξη, κάνουμε την εξής προκαταρκτική παρατήρηση. Αν και το άθροισμα στον τύπο που θέλουμε να αποδείξουμε εκτείνεται ως το άπειρο, για οποιαδήποτε επιλογή του φυσικού n και πρώτου διαιρέτη p του n το άθροισμα αυτό είναι πεπερασμένο, αφού $\lfloor n/p^k \rfloor = 0$ για $p^k > n$.

Μεταξύ των πρώτων n φυσικών, αυτοί που διαιρούνται με τον p είναι οι $p, 2p, \ldots, tp$, όπου t είναι ο μεγαλύτερος ακέραιος τέτοιος ώστε $tp \leqslant n$, δηλαδή $t = \lfloor n/p \rfloor$. Επομένως, εμφανίζονται $\lfloor n/p \rfloor$ πολλαπλάσια του p στο γινόμενο που ορίζει τον $n!$· ήτοι, τα

$$p, 2p, \ldots, \left\lfloor \frac{n}{p} \right\rfloor p. \tag{5.3.1}$$

Ο εκθέτης του p στην κανονική μορφή του $n!$ λαμβάνεται αν προσθέσουμε στον αριθμό των φυσικών που εμφανίζονται στην (5.3.1) των αριθμό των φυσικών μεταξύ των $1, 2, \ldots, n$

που διαιρούνται με τον p^2, μετά με τον p^3 και ούτω καθεξής. Επιχειρηματολογώντας όπως παραπάνω, οι φυσικοί μεταξύ 1 και n που διαιρούνται με τον p^2 είναι οι

$$p^2, 2p^2, \ldots, \left\lfloor \frac{n}{p^2} \right\rfloor p^2.$$

οι οποίοι είναι $\lfloor n/p^2 \rfloor$ το πλήθος. Εξ αυτών, $\lfloor n/p^3 \rfloor$ διαιρούνται ξανά με τον p:

$$p^3, 2p^3, \ldots, \left\lfloor \frac{n}{p^3} \right\rfloor p^3.$$

Έπειτα από πεπερασμένο πλήθος επαναλήψεων, οδηγούμαστε στο συμπέρασμα ότι ο συνολικός αριθμός που ο p διαιρεί τον $n!$ είναι

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor,$$

όπως θέλαμε να δείξουμε. ■

Σημείωση: Ο τύπος του Legendre παίρνει και την ακόλουθη ισοδύναμη μορφή

$$n! = \prod_{p \leqslant n} p^{\sum_{i=1}^{\infty} \lfloor n/p^i \rfloor},$$

όπου το γινόμενο εκτείνεται σε όλους τους πρώτους οι οποίοι είναι μικρότεροι ή ίσοι του n. Στην πραγματικότητα, το επιχείρημα που παρουσιάσαμε δεν είναι ιδιαίτερα αυστηρό (θα έπρεπε ίσως να είχαμε δώσει ένα επαγωγικό επιχείρημα). Πιο σημαντικό όμως είναι να γίνει κατανοητό *γιατί* δουλεύει αυτός ο τύπος και μάλλον το καλύτερο όλων είναι να τον δείτε εν δράσει με μερικά παραδείγματα.

Παράδειγμα 5.3.7. Θα βρούμε τον αριθμό των μηδενικών στα οποία λήγει ο αριθμός 50!. Για να βρούμε πόσες φορές εμφανίζεται ο 10 στο γινόμενο που ορίζει ο 50!, είναι αρκετό να προσδιορίσουμε τους $v_2(50!)$ και $v_5(50!)$ και να επιλέξουμε μετά τον μικρότερο από τους δύο.

Από τον τύπο του Legendre για $p = 2$ και $n = 50$ έχουμε ότι

$$v_2(50!) = \left\lfloor \frac{50}{2} \right\rfloor + \left\lfloor \frac{50}{2^2} \right\rfloor + \left\lfloor \frac{50}{2^3} \right\rfloor + \left\lfloor \frac{50}{2^4} \right\rfloor + \left\lfloor \frac{50}{2^5} \right\rfloor = 25 + 12 + 6 + 3 + 1 = 47,$$

ενώ για $p = 5$ έχουμε

$$v_2(50!) = \left\lfloor \frac{50}{5} \right\rfloor + \left\lfloor \frac{50}{5^2} \right\rfloor = 10 + 2 = 12.$$

Συμπεραίνουμε ότι ο 50! λήγει σε 12 μηδενικά.

Θα δούμε μία ακόμα εφαρμογή του τύπου του Legendre, αν και αυτό που θα δείξουμε παρακάτω είναι μάλλον γνωστό και σε κάθε περίπτωση μπορεί να αποδειχθεί καλύτερα με ένα συνδυαστικό επιχείρημα.

Εφαρμογή 5.3.8. Θα δείξουμε ότι αν οι n, r είναι φυσικοί με $1 \leqslant r < n$, τότε ο **διωνυμικός συντελεστής**

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

είναι και αυτός φυσικός.

Το επιχείρημα βασίζεται στην παρατήρηση ότι αν οι a, b είναι πραγματικοί αριθμοί, τότε $\lfloor a+b \rfloor \geqslant \lfloor a \rfloor + \lfloor b \rfloor$. Συγκεκριμένα, για κάθε πρώτο διαιρέτη p του $r!(n-r)!$ και για κάθε k φυσικό έχουμε

$$\left\lfloor \frac{n}{p^k} \right\rfloor \geqslant \left\lfloor \frac{r}{p^k} \right\rfloor + \left\lfloor \frac{n-r}{p^k} \right\rfloor$$

Προσθέτοντας αυτές τις ανισότητες για όλους τους φυσικούς k παίρνουμε

$$v_p(n!) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor \geqslant \sum_{k \geqslant 1} \left\lfloor \frac{r}{p^k} \right\rfloor + \sum_{k \geqslant 1} \left\lfloor \frac{n-r}{p^k} \right\rfloor = v_p(r!) + v_p((n-r)!)\,.$$

Προκύπτει από την παραπάνω εξίσωση ότι ο p εμφανίζεται στο γινόμενο που ορίζει ο $n!$ τουλάχιστον όσες φορές εμφανίζεται στο γινόμενο $r!(n-r)!$. Εφ' όσον αυτό ισχύει για τυχαίο πρώτο p, συμπεραίνουμε ότι ο $r!(n-r)!$ διαιρεί τον $n!$, όπως θέλαμε να δείξουμε. ■

Πόρισμα 5.3.9. *Για κάθε φυσικό r, το γινόμενο r διαδοχικών φυσικών διαιρείται με το $r!$.*

Απόδειξη. Το γινόμενο r διαδοχικών φυσικών εκ των οποίων ο μεγαλύτερος είναι ο n είναι το

$$n(n-1)(n-2)\cdots(n-r+1) = \left(\frac{n!}{r!(n-r)!}\right) \cdot r! = \binom{n}{r} \cdot r!\,.$$

Από την Εφαρμογή 5.3.8 ο $\binom{n}{r}$ είναι φυσικός, επομένως ο $r!$ διαιρεί το γινόμενο

$$n(n-1)(n-2)\cdots(n-r+1),$$

όπως θέλαμε να δείξουμε. ■

Κεφάλαιο 6

6η Παράδοση

Στο σημερινό μάθημα συνεχίζουμε την μελέτη των πρώτων. Θα δούμε ένα από τα πιο κλασικά αποτελέσματα της Θεωρίας Αριθμών που είναι γνωστό ως Αίτημα του Bertrand και την φημισμένη απόδειξη που έδωσε ο Erdős. Θα πρέπει να επισημάνουμε ότι το σημερινό μάθημα θα είναι μεγαλύτερης δυσκολίας από τα προηγούμενα ή επόμενα μαθήματα. Επιπλέον, προϋποθέτει μερικές βασικές γνώσεις. Συγκεκριμένα, υποθέτουμε ότι οι στοιχειώδεις ιδιότητες της συνάρτησης «ακέραιο μέρος» είναι γνωστές και δεν θα τις αποδείξουμε. Υποθέτουμε ακόμα ότι το διωνυμικό ανάπτυγμα

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{k} x^{n-j} y^j$$

το γνωρίζετε ήδη και το θυμάστε. Διαφορετικά μπορείτε να παρακολουθήσετε αυτήν την διάλεξη του κ. Κολουντζάκη.

6.1 Το Αίτημα του Bertrand

Είδαμε στο Θεώρημα 5.2.2 ότι η ακολουθία $g_n = p_n - p_{n-1}$ των διαδοχικών διαφορών μεταξύ πρώτων δεν είναι φραγμένη. Αυτό φυσικά δεν σημαίνει ότι δεν μπορούμε να βρούμε κανενός είδους φράγμα για τα «κενά» που παρουσιάζονται στην ακολουθία των πρώτων αριθμών. Σύμφωνα με ένα τέτοιο φημισμένο φράγμα

Το κενό από έναν αριθμό στον επόμενο πρώτο δεν είναι μεγαλύτερο από τον αριθμό που ξεκινήσαμε.

Το αποτέλεσμα αυτό είναι γνωστό ως το Αίτημα του Bertrand. Διατυπώθηκε ως εικασία το 1845 από τον Joseph Bertrand $(1821-1894)$ και ελέγχθηκε υπολογιστικά για $n < 3 \cdot 10^6$ από τον ίδιο. Την εικασία τελικά απέδειξε ο Pafnuty Chebyshev το 1850 και γι' αυτό τον λόγο είναι γνωστή και ως Θεώρημα του Chebyshev ή Θεώρημα των Bertrand - Chebyshev.

Αργότερα, δόθηκε απλούστερη απόδειξη από τον Ινδό μαθηματικό Ramanujan. Η απόδειξη που θα παρουσιάσουμε, οφείλεται στον μεγάλο αριθμοθεωρητικό Paul Erdős και βασίζεται στο πρώτο άρθρο που δημοσίευσε το 1932 σε ηλικία 19(!) ετών.

Μερικά προκαταρκτικά σχόλια πριν ξεκινήσουμε. Η απόδειξη που θα παρουσιάσουμε, αν και στοιχειώδης, είναι αρκετά απαιτητική. Είναι όμως μία από τις κανονικές αποδείξεις των Μαθηματικών και γι' αυτό πιστεύω ότι αξίζει να την δείτε. Παρ' όλ' αυτά, η δυσκολία της μου απαγορεύει να την θεωρήσω «εντός ύλης». Το ίδιο το Θεώρημα όμως (δηλαδή το Θεώρημα 6.1.1

που ακολουθεί) θα πρέπει να το γνωρίζετε είτε κληθείτε να το διατυπώσετε είτε κληθείτε να το χρησιμοποιήσετε για να λύσετε κάποια άσκηση.

Θεώρημα 6.1.1 (Το Αίτημα του Bertrand). *Για κάθε φυσικό n υπάρχει πρώτος p τέτοιος ώστε $n < p \leqslant 2n$.*

Απόδειξη. Η κεντρική ιδέα της απόδειξης είναι να εκτιμήσουμε το μέγεθος του διωνυμικού συντελεστή $\binom{2n}{n}$ αρκετά προσεκτικά ώστε να διαπιστώσουμε ότι, αν δεν είχε πρώτους διαιρέτες στο διάστημα $n < p \leqslant 2n$, τότε θα ήταν «πολύ μικρός».

Το επιχείρημα δίνεται σε 5 βήματα.

(Βήμα 1) Δείχνουμε το ζητούμενο για $n \leqslant 511$. Για να το πετύχουμε αυτό, δεν χρειάζεται να εξετάσουμε 511 περιπτώσεις. Αρκεί να παρατηρήσουμε (και αυτό είναι γνωστό ως «κόλπο του Landau») ότι η

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521$$

είναι μια ακολουθία πρώτων αριθμών της οποίας ο κάθε όρος είναι μικρότερος από τον διπλάσιο του προηγούμενου. Επομένως, κάθε διάστημα $(n, 2n]$ με $n \leqslant 511$ περιέχει έναν από αυτούς τους 11 πρώτους.

(Βήμα 2) Θα δείξουμε τώρα ότι

$$\prod_{p \leqslant x} p \leqslant 4^{x-1} \qquad \text{για κάθε πραγματικό} \quad x \geqslant 2\,, \tag{6.1.1}$$

όπου με τον παραπάνω συμβολισμό – από εδώ και στο εξής – εννοούμε ότι το γινόμενο εκτείνεται σε όλους εκείνους τους *πρώτους* αριθμούς $p \leqslant x$. Η απόδειξη της παραπάνω ανισότητας θα γίνει με Ισχυρή Επαγωγή στο πλήθος αυτών των πρώτων. Αρχικά παρατηρούμε ότι, αν ο q είναι ο μεγαλύτερος πρώτος ώστε $q \leqslant x$, τότε

$$\prod_{p \leqslant x} p = \prod_{p \leqslant q} p \qquad \text{και} \qquad 4^{q-1} \leqslant 4^{x-1}\,.$$

Επομένως, αρκεί να δείξουμε την ανισότητα (6.1.1) για $x = q$ πρώτο αριθμό. Για $q = 2$ τώρα έχουμε $2 \leqslant 4$ που ισχύει, και επομένως η επαγωγή μας ξεκινάει. Συνεχίζουμε θεωρώντας περιττούς πρώτους $q = 2m + 1$, ενώ η επαγωγική μας υπόθεση είναι ότι η (6.1.1) ισχύει για όλους τους φυσικούς x στο σύνολο $\{2, 3, \ldots, 2m\}$.

Για $q = 2m + 1$ λοιπόν, «σπάμε» το γινόμενο και έχουμε

$$\prod_{p \leqslant 2m+1} p = \prod_{p \leqslant m+1} p \cdot \prod_{m+1 < p \leqslant 2m+1} p \leqslant 4^m \binom{2m+1}{m} \leqslant 4^m 2^{2m} = 4^{2m}\,.$$

Ας δούμε λίγο προσεκτικά τι ακριβώς κάναμε στην παραπάνω ανισοεξίσωση της μίας γραμμής. Πρώτον, η

$$\prod_{p \leqslant m+1} p \leqslant 4^m$$

ισχύει από την επαγωγική μας υπόθεση. Έπειτα, η

$$\prod_{m+1 < p \leqslant 2m+1} p \leqslant \binom{2m+1}{m}$$

προκύπτει από την παρατήρηση (δείτε Εφαρμογή 5.3.8) ότι ο διωνυμικός συντελεστής

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$

είναι ακέραιος και ότι οι πρώτοι που εμφανίζονται στο γινόμενο, δηλαδή οι πρώτοι p τέτοιοι ώστε $m+1 < p \leqslant 2m+1$, είναι *όλοι* παράγοντες του αριθμητή $(2m+1)!$, αλλά *όχι* του παρονομαστή $m!(m+1)!$. Τέλος, η

$$\binom{2m+1}{m} \leqslant 2^{2m}$$

ισχύει, εφ' όσον οι

$$\binom{2m+1}{m} \quad \text{και} \quad \binom{2m+1}{m+1}$$

είναι δύο **ίσοι** συντελεστές οι οποίοι εμφανίζονται στο διωνυμικό ανάπτυγμα

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}\,.$$

(Βήμα 3) Από τον τύπο του Legendre (δείτε Άσκηση 5.3.6 και την απόδειξη της Εφαρμογής 5.3.8), ο διωνυμικός συντελεστής $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ περιέχει τον πρώτο p ακριβώς

$$\sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

φορές. Παρατηρήστε τώρα ότι κάθε προσθετέος στο παραπάνω άθροισμα είναι το πολύ 1, αφού ικανοποιεί την

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1 \right) = 2\,,$$

και είναι ακέραιος. Επιπλέον, προσθετέοι για τους οποίους ισχύει $p^k > 2n$ δεν εμφανίζονται καν. Προκύπτει επομένως ότι ο p εμφανίζεται στην ανάλυση του $\binom{2n}{n}$ σε πρώτους ακριβώς

$$\sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leqslant \max\{r : p^r \leqslant 2n\}$$

φορές. Συμπεραίνουμε ότι η μέγιστη δύναμη του p που διαιρεί τον $\binom{2n}{n}$ δεν είναι μεγαλύτερη του $2n$. Συγκεκριμένα, πρώτοι $p > \sqrt{2n}$ εμφανίζονται το πολύ μία φορά στην κανονική μορφή του $\binom{2n}{n}$.

Κατά τον ίδιο τον Erdős τώρα, η βασικότερη παρατήρηση σε όλο το επιχείρημα είναι ότι οι πρώτοι που ικανοποιούν την

$$\frac{2}{3}n < p \leqslant n$$

δεν διαιρούν καν τον $\binom{2n}{n}$.

Πράγματι, αν $3p > 2n$ τότε (για $n \geqslant 3$ άρα και $p \geqslant 3$) τα μόνα πολλαπλάσια του p που εμφανίζονται ως παράγοντες στον αριθμητή του $\frac{(2n)!}{n!n!}$ είναι τα p και $2p$, επομένως ο p εμφανίζεται στην δεύτερη δύναμη στον αριθμητή. Το ίδιο όμως ισχύει και για τον παρονομαστή, αφού για καθένα από τα δύο $n!$, $p \mid n!$ (αφού $p \leqslant n$), αλλά $2p > 4/3n > n$ και άρα ο $1 \cdot p$ είναι το μοναδικό πολλαπλάσιο του p που εμφανίζεται στο $n!$.

(Βήμα 4) Από το διωνυμικό ανάπτυγμα έχουμε ότι

$$4^n = 2^{2n} = (1+1)^{2n} = 2 + \binom{2n}{1} + \binom{2n}{2} + \ldots + \binom{2n}{2n-1} \leqslant 2n\binom{2n}{n}.$$

Για να δικαιολογήσουμε την τελευταία ανισότητα παραπάνω, χρησιμοποιούμε την ιδιότητα σύμφωνα με την οποία οι διωνυμικοί συντελεστές σχηματίζουν **μονοκόρυφη** ακολουθία, που σημαίνει ότι ο μεγαλύτερος από τους $\binom{2n}{i}$ για $0 \leqslant i \leqslant 2n$ είναι ο $\binom{2n}{n}$, δηλαδή αυτός που είναι «στην μέση».

Είμαστε σε θέση τώρα να εκτιμήσουμε τον $\binom{2n}{n}$ ως εξής:

$$\frac{4^n}{2n} \leqslant \binom{2n}{n} \leqslant \prod_{p \leqslant \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \leqslant \frac{2}{3}n} p \cdot \prod_{n < p \leqslant 2n} p\,.$$

Τώρα, δεν υπάρχουν περισσότεροι από $\sqrt{2n}$ πρώτοι στο πρώτο γινόμενο στο δεξί μέλος· χρησιμοποιώντας την (6.1.1) για το δεύτερο γινόμενο και συμβολίζοντας με $P(n)$ τον αριθμό των πρώτων $n < p \leqslant 2n$ παίρνουμε την ανισότητα

$$\frac{4^n}{2n} < \left((2n)^{\sqrt{2n}}\right) \cdot \left(4^{\frac{2}{3}n}\right) \cdot (2n)^{P(n)}$$

ή ισοδύναμα την

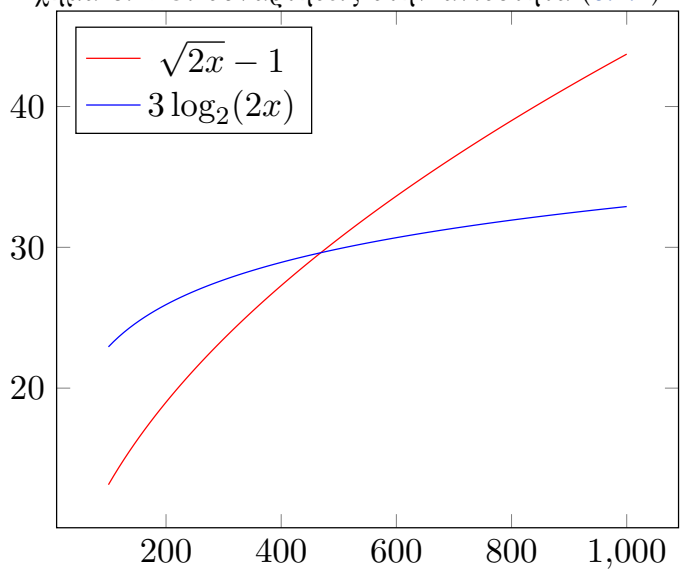
$$4^{\frac{n}{3}} < (2n)^{\sqrt{2n}+1+P(n)}\,. \tag{6.1.2}$$

(Βήμα 5) Το τελευταίο κομμάτι της απόδειξης είναι πρακτικά άσκηση Απειροστικού Λογισμού. Παίρνοντας λογάριθμο με βάση το 2 στην ανισότητα (6.1.2), έχουμε την

$$P(n) > \frac{2n}{3\log_2(2n)} - (\sqrt{2n}+1)\,. \tag{6.1.3}$$

Αρκεί λοιπόν να δείξουμε ότι το δεξί μέλος της (6.1.3) είναι θετικό για αρκετά μεγάλο n και θα το κάνουμε αυτό για $n \geqslant 2^9 = 512$ (αν και ισχύει και για μικρότερες τιμές).

Σχήμα 6.1: Οι συναρτήσεις στην ανισότητα (6.1.4)



Εφ' όσον το καταφέρουμε αυτό, θα είμαστε καλυμμένοι για όλους τους φυσικούς n από το Βήμα 1.

Γράφουμε $2n-1 = (\sqrt{2n}-1)(\sqrt{2n}+1)$ και απλοποιώντας τον όρο $(\sqrt{2n}+1)$ αρκεί να δείξουμε την

$$\sqrt{2n} - 1 > 3\log_2(2n) \quad \text{για} \quad n \geqslant 2^9 = 512. \tag{6.1.4}$$

Για $n = 2^9$ η παραπάνω ανισότητα γίνεται $31 > 30$ που ισχύει. Συγκρίνοντας τώρα τις παραγώγους

$$(\sqrt{x} - 1)' = \frac{1}{2}\frac{1}{\sqrt{x}}$$

και

$$(3\log_2 x)' = \frac{3}{\log 2}\frac{1}{x},$$

βλέπουμε ότι η $\sqrt{x} - 1$ μεγαλώνει ταχύτερα από την $3\log_2 x$ για $x > (\frac{6}{\log 2})^2 \approx 75$ και άρα και για $x \geqslant 2^{10} = 1024$. ■

Έχοντας, επί τέλους, αποδείξει το Αίτημα του Bertrand, είναι ώρα να δούμε μια όμορφη εφαρμογή του. Διάφορες άλλες (επίσης όμορφες κατά την γνώμη μου) εφαρμογές, δίνονται στις ασκήσεις στο τέλος του μαθήματος.

Χρειαζόμαστε πρώτα μία έννοια.

Ορισμός 6.1.2. Μία ακολουθία (a_n) λέγεται **πλήρης** αν κάθε φυσικός n είναι άθροισμα κάποιας υπακολουθίας της (a_n). Δηλαδή, αν για κάθε φυσικό n υπάρχουν $b_i \in \{0, 1\}$ έτσι ώστε

$$n = \sum_{i=1}^{\infty} b_i a_i.$$

Η ίδια η ακολουθία των φυσικών $1, 2, 3, \ldots$ για παράδειγμα είναι πλήρης. (Η επιλογή των συντελεστών b_i είναι η προφανής.) Προσέξτε σε αυτό το σημείο ότι για να είναι πλήρης η ακολουθία (a_n) θα πρέπει αναγκαστικά να έχουμε $a_1 = 1$. Διάφορες άλλες επώνυμες ακολουθίες όμως, όπως φερ' ειπείν η ακολουθία των αριθμών Fibonacci (την οποία αν και δεν έχουμε αναφέρει έως τώρα, πιθανότατα ήδη γνωρίζετε), είναι και αυτές πλήρεις.

Το κεντρικό αποτέλεσμα αποτέλεσμα σχετικά με τις πλήρεις ακολουθίες είναι το επόμενο, το οποίο απλώς θα διατυπώσουμε, αλλά δεν θα αποδείξουμε.

Θεώρημα 6.1.3 (Το Κριτήριο του Brown). *Η ακολουθία (a_n) είναι πλήρης, αν και μόνο αν ισχύουν τα ακόλουθα:*

(i) $a_1 = 1$, *και*

(ii) *για κάθε $k = 2, 3, \ldots$ έχουμε*

$$\sum_{i=1}^{k-1} a_i = a_1 + a_2 + \ldots + a_{k-1} \geqslant a_k - 1\,.$$

Έχοντας στην διάθεσή μας το Κριτήριο του Brown, μπορούμε να αποδείξουμε εύκολα το επόμενο αποτέλεσμα.

Πόρισμα 6.1.4. *Αν η ακολουθία (a_n) είναι τέτοια ώστε $a_1 = 1$ και $a_{k+1} \leqslant 2a_k$ για κάθε k φυσικό, τότε η (a_n) είναι πλήρης.*

Απόδειξη. Θα δείξουμε ότι η (a_n) ικανοποιεί το Κριτήριο του Brown. Αρχικά έχουμε ότι $a_1 = 1$ εξ υποθέσεως, οπότε η πρώτη συνθήκη του Θεωρήματος 6.1.3 ικανοποιείται.

Δείχνουμε τώρα επαγωγικά για $k \geqslant 2$ ότι

$$\sum_{i=1}^{k-1} a_i = a_1 + a_2 + \ldots + a_{k-1} \geqslant a_k - 1\,.$$

Για $k = 2$ μας δίνεται από την υπόθεση ότι $a_2 \leqslant 2a_1 = 2$, άρα ισχύει η $a_2 - 1 \leqslant a_1$ και η επαγωγή ξεκινάει. Δεχόμαστε τώρα ότι το ζητούμενο ισχύει για k και έχουμε

$$a_{k+1} - 1 \leqslant 2a_k - 1 = (a_k - 1) + a_k \leqslant (a_1 + a_2 + \ldots + a_{k-1}) + a_k = a_1 + a_2 + \ldots + a_k\,,$$

όπου για την πρώτη ανισότητα χρησιμοποιήσαμε την συνθήκη της υπόθεσης, ενώ για την δεύτερη ανισότητα χρησιμοποιήσαμε την επαγωγική υπόθεση. Η επαγωγή είναι πλήρης επομένως και άρα το ζητούμενο έχει δειχθεί. ■

Θα χρησιμοποιήσουμε τώρα το Πόρισμα 6.1.4 για να δείξουμε το ακόλουθο μάλλον αναπάντεχο αποτέλεσμα.

Εφαρμογή 6.1.5. Συμβολίζουμε με (a_n) την ακολουθία των πρώτων αριθμών (p_n) έχοντας επισυνάψει ως πρώτο όρο τον 1. Δηλαδή, $a_1 = 1$ και $a_k = p_{k-1}$ για $k \geqslant 2$. Θα δείξουμε ότι η ακολουθία (a_n) είναι πλήρης.

Ισχύει ότι $a_1 = 1$ και $a_2 = p_1 = 2 \leqslant 2 = 2 \cdot a_1$ από την υπόθεση. Για $k \geqslant 2$ τώρα έχουμε

$$a_{k+1} = p_k \leqslant 2p_{k-1} = 2a_k\,,$$

όπου η ανισότητα προκύπτει εφαρμόζοντας το Θεώρημα 6.1.1 για τον p_k στο διάστημα $(p_{k-1}, 2p_{k-1}]$. Έπεται λοιπόν ότι η ακολουθία (a_n) πληρεί τις προϋποθέσεις του Πορίσματος 6.1.4 και άρα είναι πλήρης. ■

Δείξαμε λοιπόν ότι κάθε φυσικός γράφεται σαν άθροισμα διακεκριμένων πρώτων συν την μονάδα. Σημειώνουμε εδώ ότι θα μπορούσαμε να το είχαμε αποδείξει αυτό και κατ' ευθείαν με επαγωγή, χωρίς επίκληση στο Κριτήριο του Brown (αλλά χρησιμοποιώντας το Αίτημα του Bertrand).

Ισχύει δε κάτι ακόμα ισχυρότερο. Χρησιμοποιώντας το Αίτημα του Bertrand, ο Richert απέδειξε το 1949 ότι κάθε ακέραιος $n \geqslant 7$ γράφεται σαν άθροισμα διακεκριμένων πρώτων (χωρίς δηλαδή να χρειάζεται να προστεθεί ο 1 στο άθροισμα). Παρατηρήστε ότι αυτό δεν ισχύει για μικρότερους αριθμούς όπως ο 6 ή ο 4. Στο επόμενο μάθημα (και τελευταίο για πρώτους) θα αναφερθούμε σε μία φημισμένη εικασία που σχετίζεται με το πώς γράφονται οι φυσικοί ως αθροίσματα πρώτων.

6.2 Ασκήσεις

Άσκηση 6.2.1. Να δείξετε ότι για κάθε φυσικό $n > 1$ υπάρχει πρώτος p τέτοιος ώστε $n < p < 2n$.

Απόδειξη. Έστω $n > 1$. Από το Θεώρημα 6.1.1 υπάρχει πρώτος p τέτοιος ώστε $n < p \leqslant 2n$. Αφού $n > 1$ όμως, ο $2n$ είναι σύνθετος και άρα $p \neq 2n$. Έπεται ότι $p < 2n$, όπως θέλαμε να δείξουμε. ■

Άσκηση 6.2.2. Δείξτε ότι από το Αίτημα του Bertrand έπεται ότι για κάθε φυσικό n έχουμε $p_{n+1} < 2p_n$, όπου με (p_n) συμβολίζουμε, ως συνήθως, την ακολουθία των πρώτων αριθμών.

Απόδειξη. Από το Θεώρημα 6.1.1 έχουμε ότι για κάθε φυσικό n υπάρχει πρώτος q τέτοιος ώστε

$$p_n < q \leqslant 2p_n.$$

Όμως $p_n > 1$ για κάθε n και άρα ο $2p_n$ είναι σύνθετος. Προκύπτει λοιπόν ότι

$$p_n < q < 2p_n\,,$$

δηλαδή η δεύτερη ανισότητα είναι γνήσια. Εφ' όσον ο q είναι πρώτος με $p_n < q$, έπεται ότι ο q δεν μπορεί να είναι μικρότερος του πρώτου που ακολουθεί τον p_n, δηλαδή του p_{n+1}. Επομένως $p_{n+1} \leqslant q < 2p_n$, όπως θέλαμε να δείξουμε. ■

Άσκηση 6.2.3. Αποδείξτε επαγωγικά ότι για κάθε φυσικό $n \geqslant 2$ έχουμε $p_n < 2^n$.

Απόδειξη. Κάνουμε επαγωγή στο n. Πιο συγκεκριμένα, προσέξτε ότι χρησιμοποιούμε την μορφή της Επαγωγής που δείξαμε στην Άσκηση 1.3.5.

Για $n = 2$ το ζητούμενο ισχύει, αφού $p_2 = 3 < 4 = 2^2$. Μπορούμε επομένως να υποθέσουμε ότι $n \geqslant 3$. Δεχόμαστε τώρα την ισχύ αυτού που θέλουμε να δείξουμε για n, δηλαδή ότι $p_n < 2^n$. Από το Θεώρημα 6.1.1 έχουμε ότι υπάρχει πρώτος q τέτοιος ώστε

$$2^n < q < 2^{n+1},$$

όπου η δεύτερη ανισότητα είναι γνήσια, διότι ο μόνος άρτιος πρώτος είναι ο 2. Εφ' όσον $p_n < 2^n < q$, όπου η πρώτη ανισότητα ισχύει από την επαγωγική υπόθεση, προκύπτει ότι $p_n < q$ και άρα $p_{n+1} \leqslant q < 2^{n+1}$. Έτσι η επαγωγή είναι πλήρης και έχουμε δείξει το ζητούμενο. ■

Άσκηση 6.2.4 (Ανισότητα του Bonse). Να αποδείξετε την ακόλουθη ανισότητα που οφείλεται στον H. Bonse: για κάθε φυσικό $n \geqslant 5$ ισχύει ότι

$$p_n^2 < p_1 p_2 \cdots p_{n-1}\,.$$

Απόδειξη. Δουλεύουμε με επαγωγή στο n. Για $n = 5$ έχουμε

$$p_5^2 = 11^2 = 121 < 210 = 2 \cdot 3 \cdot 5 \cdot 7 = p_1 p_2 p_3 p_4,$$

οπότε το ζητούμενο ισχύει σε αυτήν την περίπτωση.

Έστω τώρα ότι η πρόταση ισχύει για τον φυσικό $n \geqslant 5$. Από την Άσκηση 6.2.2 έχουμε ότι $p_{n+1} < 2p_n$ και άρα

$$p_{n+1}^2 < 4p_n^2 < 4p_1 p_2 \cdots p_{n-1},$$

όπου για την δεύτερη ανισότητα χρησιμοποιήσαμε την επαγωγική υπόθεση. Εφ' όσον $n \geqslant 5$, έχουμε ότι $p_n > 4$ κι επομένως

$$p_{n+1}^2 < 4p_1p_2\cdots p_{n-1} < p_1p_2\cdots p_{n-1}p_n\,.$$

Άρα η επαγωγή μας είναι πλήρης και το ζητούμενο έπεται. ■

Άσκηση 6.2.5. Μία από τις συναρτήσεις που εισήγαγε ο Chebyshev στο άρθρο του, όπου μεταξύ άλλων αποδεικνύει το Αίτημα του Bertrand, είναι η συνάρτηση «θήτα» την οποία όρισε για x πραγματικό ως

$$\theta(x) = \sum_{p\leqslant x} \log p.$$

Δείξτε ότι το Αίτημα του Bertrand είναι πόρισμα της διπλής ανισότητας

$$0.73x < \theta(x) < 1.12x$$

η οποία ισχύει για $x \geqslant 41$.

Απόδειξη. Ελέγχουμε ότι υπάρχει πρώτος σε κάθε διάστημα $(n, 2n]$ για $n < 41$ θεωρώντας τους πρώτους $2, 3, 5, 7, 13, 23, 43$. Έστω τώρα ότι υπάρχει φυσικός $n > 41$ με την ιδιότητα ότι δεν υπάρχει πρώτος στο διάστημα $(n, 2n]$. Έπεται τότε ότι $\theta(2n) = \theta(n)$. Χρησιμοποιώντας την ανισότητα $0.73x < \theta(x) < 1.12x$, παίρνουμε

$$1.46n = 2 \cdot 0.73n < \theta(2n) = \theta(n) < 1.12n,$$

άτοπο. ■

Άσκηση 6.2.6. $(*)$ Έστω m, n φυσικοί. Να δειχθεί ότι ο

$$A = \frac{1}{m} + \frac{1}{m+1} + \ldots + \frac{1}{m+n}$$

δεν είναι ακέραιος.

Απόδειξη. Παρατηρούμε αρχικά ότι για $n \leqslant m-1$ έχουμε

$$A < m \cdot \frac{1}{m} = 1\,,$$

επομένως ο A δεν είναι ακέραιος σ' αυτήν την περίπτωση.

Υποθέτουμε τώρα ότι $n \geqslant m$. Για $n = m = 1$ έχουμε $A = 3/2$, που δεν είναι ακέραιος, οπότε μπορούμε να υποθέσουμε επιπλέον ότι $m + n > 2$. Από το Αίτημα του Bertrand έπεται ότι υπάρχει πρώτος p τέτοιος ώστε

$$\frac{m+n}{2} < p < m+n\,.$$

Εφ' όσον $2p > m+n$ και $p > \frac{m+n}{2} \geqslant m$, ο p είναι το μοναδικό πολλαπλάσιο του p στο διάστημα $[m, m+n]$.

Φτιάχνουμε τώρα ένα κοινό κλάσμα

$$A = \frac{p\cdot B + C}{m\cdot(m+1)\cdots(m+n)} \tag{6.2.1}$$

όπου B φυσικός και

$$C = m \cdot (m+1) \cdots (p-1)(p+1) \cdots (m+n).$$

Παρατηρούμε τώρα ότι στην (6.2.1) ο p δεν διαιρεί τον αριθμητή αφού δεν διαιρεί τον C, ενώ διαιρεί τον παρονομαστή. Προκύπτει λοιπόν ότι ο A δεν είναι ακέραιος, όπως θέλαμε να δείξουμε. ■

Κεφάλαιο 7

7η Παράδοση

Το σημερινό μάθημα είναι το τέταρτο κατά σειρά και τελευταίο που είναι αφιερωμένο αποκλειστικά στους πρώτους. Δεν είμαστε σε θέση να αποδείξουμε κανένα από τα μεγάλα αποτελέσματα στα οποία θα αναφερθούμε, επομένως ο σκοπός του μαθήματος είναι να σας μεταφέρω διάφορα ιστορικά στοιχεία και να σας παρουσιάσω μερικά κεντρικά αποτελέσματα. Συγκεκριμένα, θα αναφερθούμε στο λεγόμενο «Θεώρημα των Πρώτων Αριθμών», θα δούμε το Θεώρημα του Dirichlet για πρώτους σε αριθμητικές προόδους και θα κλείσουμε αναφέροντας μερικές από τις διαχρονικότερες Εικασίες που έχουν διατυπωθεί για τους μυστήριους αυτούς αριθμούς.

Σε ό,τι έχει να κάνει με το ιστορικό υλικό του μαθήματος: δεν είστε υποχρεωμένοι να θυμάστε ποιος απέδειξε τι και πότε. Τα ιστορικά στοιχεία έχουν ενσωματωθεί στο κείμενο ώστε να έχετε μια εποπτεία για την εξέλιξη της Θεωρίας Αριθμών, ο κεντρικότερος ερευνητικός άξονας της οποίας είναι η καλύτερη κατανόηση της φύσης των πρώτων. Σε ό,τι αφορά όμως το Θεώρημα των Πρώτων Αριθμών και το Θεώρημα του Dirichlet για πρώτους σε αριθμητικές προόδους, θα πρέπει να κατανοείτε το περιεχόμενό τους και να μπορείτε να τα χρησιμοποιήσετε αν σας ζητηθεί.

7.1 Το Θεώρημα των Πρώτων Αριθμών

Εδώ είναι μάλλον το πιο κατάλληλο σημείο για να εισαγάγουμε έναν ορισμό.

Ορισμός 7.1.1. Για έναν (θετικό) πραγματικό αριθμό x, συμβολίζουμε με $\pi(x)$ το πλήθος των πρώτων αριθμών μικρότερων ή ίσων του x. Δηλαδή,

$$\pi(x) = \#\{p \leqslant x : p \text{ πρώτος}\}.$$

Για παράδειγμα, έχουμε $\pi(10^2) = 25$ μετρώντας τα λευκά τετράγωνα στο Σχήμα 5.1, ενώ $\pi(10^3) = 168$, $\pi(10^4) = 1,229$ και θα μπορούσαμε να συνεχίσουμε να μετράμε, εφ' όσον έχουμε την απαραίτητη ιδιοσυγκρασία. Τι μπορούμε να πούμε τώρα για την συνάρτηση $\pi(x)$; Μια πρώτη παρατήρηση: είναι αύξουσα συνάρτηση (όχι όμως *γνησίως* αύξουσα). Είναι ακόμα *βαθμωτή*, αφού παραμένει σταθερή κατά διαστήματα (π.χ. $\pi(3) = \pi(4) = 2$ ή $\pi(7) = \pi(8) = \pi(9) = \pi(10) = 4$).

Δείξαμε στο Θεώρημα 5.2.1 ότι η $\pi(x)$ δεν είναι φραγμένη και άρα

$$\lim_{x \to +\infty} \pi(x) = \infty\,.$$

Από το Αίτημα του Bertrand που δείξαμε στο προηγούμενο μάθημα, προκύπτει ότι $\pi(2^n) \geqslant n$ για κάθε n φυσικό, αφού υπάρχει τουλάχιστον ένας πρώτος στο διάστημα $(2^i, 2^{i+1}]$ (δείτε και Άσκηση 6.2.3) και άρα

$$\pi(x) > \log_2(x) - 1$$

για κάθε πραγματικό $x \geqslant 2$. Αυτό μπορούμε να το δούμε ως εξής: αν $p_{n-1} \leqslant x < p_n$, τότε $\pi(x) = n - 1$ και η $x < p_n < 2^n = 2^{\pi(x)+1}$ συνεπάγεται την ανισότητα που θέλουμε.

Βλέπουμε επομένως ότι η συνάρτηση $\pi(x)$ αυξάνει συνεχώς χωρίς φράγμα, τουλάχιστον όσο γρήγορα αυξάνει και η συνάρτηση $\log_2(x)$. Ένα φυσιολογικό ερώτημα λοιπόν είναι:

Με ποια συνάρτηση «μοιάζει» η $\pi(x)$;

Η φύση της μάς υποδεικνύει ότι θα πρέπει να αναζητήσουμε μία συνάρτηση η οποία να αποτελεί απλώς *προσέγγιση* της $\pi(x)$. Το ότι η $\pi(x)$ αποκλείεται να είναι κάποιου είδους «απλή» συνάρτηση, θα το δικαιολογήσουμε μερικώς λίγο αργότερα.

Πάμε λίγο πίσω τώρα. Οι μαθηματικοί στα τέλη του 18ου αι. εξέταζαν πίνακες πρώτων αριθμών οι οποίοι είχαν κατασκευαστεί με υπολογισμούς «με το χέρι». Χρησιμοποιώντας αυτές τις τιμές, έψαχναν συναρτήσεις που υπολόγιζαν (ή καλύτερα προσέγγιζαν) την $\pi(x)$. Το 1798, ο Γάλλος μαθηματικός Adrien-Marie Legendre (τον οποίο συναντήσαμε σύντομα στον τύπο του Legendre) χρησιμοποίησε πίνακες πρώτων έως τον 400.031 για να σημειώσει ότι η $\pi(x)$ μπορούσε να προσεγγιστεί από τη συνάρτηση

$$\frac{x}{\log x - 1.08366}\,.$$

Ο μεγάλος Γερμανός μαθηματικός Karl Friedrich Gauss, ο οποίος έμεινε γνωστός και ως «ο Πρίγκηπας των Μαθηματικών», διαπίστωσε (σε ηλικία 15 ετών!) ότι η $\pi(x)$ προσεγγίζεται πολύ καλά από τις συναρτήσεις

$$\frac{x}{\log x} \qquad \text{και} \qquad \mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\mathrm{d}t\,.$$

Η συνάρτηση $\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\mathrm{d}t$ είναι γνωστή ως «λογαριθμικό ολοκλήρωμα», δηλαδή logarithmic integral και συμβολίζεται με Li για να παραπέμψει στα αρχικά του όρου.

Ούτε ο Legendre ούτε ο Gauss όμως κατάφεραν να αποδείξουν ότι αυτές οι συναρτήσεις είναι όντως καλές προσεγγίσεις της $\pi(x)$ για μεγάλες τιμές του x. Μέχρι το 1811, είχε δημιουργηθεί ένας πίνακας όλων των πρώτων έως τον αριθμό 1.020.000 από τον Chemac. Ο πίνακας αυτός τεκμηρίωνε ισχυρά αυτές τις «εικασίες» των Legendre και Gauss. Για να πειστείτε κι εσείς, δείτε τον Πίνακα 7.1.1 (οι τιμές της $\mathrm{Li}(x)$ δίνονται στον κοντινότερο ακέραιο).

Το πρώτο σημαντικό αποτέλεσμα που τεκμηριώνει ότι η συνάρτηση $x/\log x$ είναι πράγματι καλή εκτίμηση της $\pi(x)$, δόθηκε από τον Chebyshev το 1850.

Αν το όνομα ή το έτος σας θυμίζουν κάτι (και το ελπίζω), είναι γιατί τα συναντήσαμε στο μάθημα για το Αίτημα του Bertrand. Αυτό που κατάφερε ο Chebyshev ήταν να δείξει ότι υπάρχουν θετικές σταθερές $C_1 < 1 < C_2$ τέτοιες ώστε

$$C_1\left(\frac{x}{\log x}\right) < \pi(x) < C_2\left(\frac{x}{\log x}\right) \tag{7.1.1}$$

για αρκετά μεγάλες τιμές του x. Συγκεκριμένα, έδειξε ότι η (7.1.1) ισχύει με $C_1 = 0.929$ και $C_2 = 1.1$ για αρκετά μεγάλα x και χρησιμοποίησε αυτά τα φράγματα για να αποδείξει το

Πίνακας 7.1.1: Προσεγγίσεις της $\pi(x)$

x	$\pi(x)$	$x/\log x$	$\pi(x)/\frac{x}{\log x}$	$\mathrm{Li}(x)$	$\pi(x)/\mathrm{Li}(x)$
10^1	4	4.3	0.921	6	0.648 760 9
10^2	25	21.7	1.151	30	0.829 844 0
10^3	168	144.8	1.160	178	0.943 820 2
10^4	1229	1085.7	1.132	1246	0.986 356 3
10^5	9592	8685.9	1.104	9630	0.996 054 0
10^6	78 498	72 382.4	1.085	78 628	0.998 346 6

Αίτημα του Bertrand. Έδειξε ακόμα ότι *αν* το όριο της $\pi(x)/(x/\log x)$ υπάρχει, καθώς $x \to \infty$, τότε είναι ίσο με 1.

Με όσα έχουμε αναφέρει ως τώρα, ίσως έχετε υποπτευθεί τι λέει το Θεώρημα των Πρώτων Αριθμών. Αν όχι, δείτε το.

Θεώρημα 7.1.2 (Το Θεώρημα των Πρώτων Αριθμών). *Οι συναρτήσεις $\pi(x)$ και $x/\log x$ είναι ασυμπτωτικά ίσες.*[1] *Δηλαδή*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1\,.$$

Το σπουδαίο αυτό Θεώρημα αποδείχτηκε τελικά το 1896 από τον Γάλλο Jacques Hadamard και ανεξάρτητα το ίδιο έτος από τον Βέλγο (με πρώτο όνομα δυναστεία) Charles-Jean-Gustave-Nicholas de la Vallée Poussin. Οι αποδείξεις που έδωσαν βασίζονταν σε αποτελέσματα της θεωρίας της μιγαδικής ανάλυσης, ενώ χρησιμοποίησαν ιδέες που είχε αναπτύξει το 1859 ο Γερμανός μαθηματικός Bernhard Riemann.

Σύμφωνα με αυτές τις ιδέες, η $\pi(x)$ σχετίζεται στενά με την συμπεριφορά της συνάρτησης

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

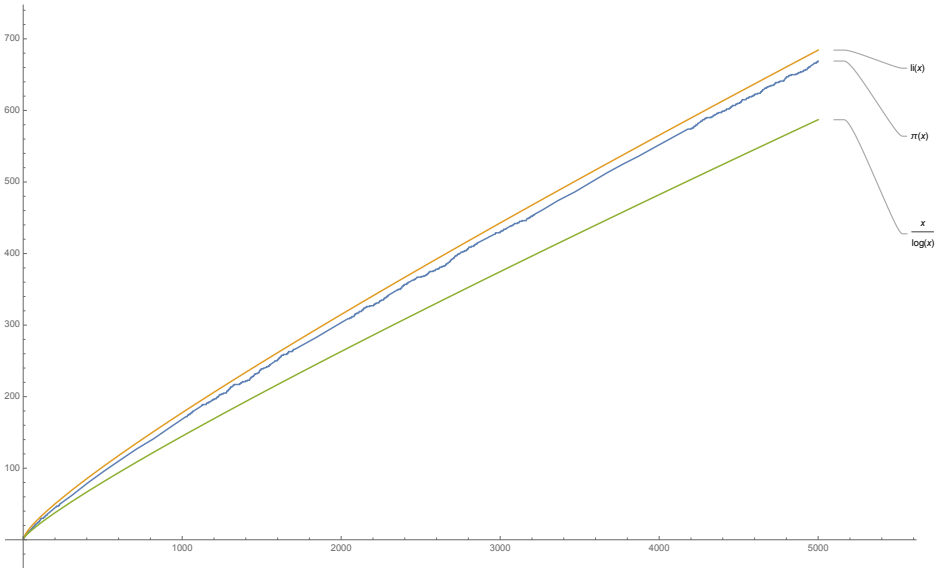
στο μιγαδικό επίπεδο. Η σχέση της ανωτέρω συνάρτησης «ζήτα» του Riemann με τους πρώτους προκύπτει από την ισότητα

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1},$$

όπου το γινόμενο στην ισότητα αυτή εκτείνεται σε όλους τους πρώτους αριθμούς.

Ο de la Vallée Poussin μάλιστα, πέρα από την απόδειξη που έδωσε για το Θεώρημα των Πρώτων, απέδειξε επίσης ότι η συνάρτηση $\mathrm{Li}(x)$ δίνει καλύτερη εκτίμηση της $\pi(x)$ απ' ό,τι η $x/(\log x - \alpha)$ για οποιαδήποτε τιμή της σταθεράς α. Το φαινόμενο αυτό παρατηρείται ήδη στον Πίνακα 7.1.1, ενώ βλέπουμε ακόμα ότι η διαφορά $\mathrm{Li}(x) - \pi(x)$ είναι θετική και μεγαλώνει καθώς το x αυξάνεται. Δείτε επίσης και το Σχήμα 7.1 όπου φαίνεται καλύτερα ότι η $\mathrm{Li}(x)$ είναι καλύτερη εκτίμηση της $\pi(x)$ απ' ό,τι η $x/\log x$. Αυτό οδήγησε τον Gauss να εικάσει ότι αυτή

[1] Προσέξτε τα εξής: αν και γνωρίζαμε από το 1850 περίπου ότι, αν το όριο υπάρχει, τότε είναι ίσο με 1, η ίδια η ύπαρξη του ορίου δεν είναι καθόλου προφανής. Επίσης, η απόσταση μεταξύ αυτού που έδειξε ο Chebyshev (ότι δηλαδή η $\pi(x)/(x/\log x)$ είναι φραγμένη συνάρτηση) και του περιεχομένου του Θεωρήματος των Πρώτων Αριθμών, αν και δεν της φαίνεται ίσως, είναι εξαιρετικά μεγάλη.



Σχήμα 7.1: Οι συναρτήσεις $\mathrm{Li}(x)$, $\pi(x)$ και $x/\log x$ για $x \leqslant 5 \cdot 10^3$

η τάση διατηρείται για όλους τους πραγματικούς x. Το 1914 όμως, ο Άγγλος μαθηματικός J. E. Littlewood απέδειξε ότι η $\mathrm{Li}(x) - \pi(x)$ αλλάζει πρόσημο άπειρες φορές. Στην απόδειξή του ο Littlewood δεν έδωσε καμία ένδειξη πότε συμβαίνει αυτή η αλλαγή στο πρόσημο για πρώτη φορά. Αυτό το πέτυχε πρώτος ο Stanley Skewes, μαθητής του Littlewood, ο οποίος απέδειξε (δεχόμενος την αλήθεια της «Εικασίας του Riemann») ότι η $\mathrm{Li}(x) - \pi(x)$ γίνεται αρνητική για τουλάχιστον έναν $x < 10^{10^{10^{34}}}$. Ο εντελώς εξωφρενικός αυτός αριθμός, που είναι γνωστός ως «σταθερά του Skewes», είναι διάσημος ως ένας από τους μεγαλύτερους αριθμούς που έχουν εμφανιστεί ποτέ με φυσικό τρόπο σε μαθηματική απόδειξη.

7.2 Το Θεώρημα του Dirichlet

Λίγο πριν διατυπώσουμε το Θεώρημα 5.2.1, αναφερθήκαμε στην απόδειξη που είχε δώσει ο Ευκλείδης στα Στοιχεία του για την Απειρία των Πρώτων. Θα δούμε σε λίγο πώς το επιχείρημα του Ευκλείδη μπορεί να αναπτυχθεί και σε άλλες κατευθύνσεις, αλλά πρώτα μία παρατήρηση.

Έστω ότι μας δίνονται δύο ακέραιοι a, b που είναι και οι δύο της μορφής $4x+1$. Ισχυριζόμαστε ότι και ο ab είναι της ίδιας μορφής. Αν $a = 4y + 1$ και $b = 4w + 1$, τότε

$$ab = (4y + 1)(4w + 1) = 4 \cdot (4yw + y + w) + 1\,.$$

Με μια εύκολη επαγωγή στο πλήθος των όρων, έπεται ότι το γινόμενο οσωνδήποτε ακεραίων της μορφής $4x + 1$ είναι της ίδιας μορφής.

Θεώρημα 7.2.1. *Υπάρχουν άπειροι πρώτοι της μορφής* $4n + 3$.

Απόδειξη. Έστω αντιθέτως ότι υπάρχουν πεπερασμένου πλήθους πρώτοι της μορφής $4n + 3$ και ότι ο μεγαλύτερος από αυτούς είναι ο p. Θεωρούμε τώρα τον φυσικό

$$q = 2^2 \cdot 3 \cdot 5 \cdots p - 1.$$

Ο q είναι της μορφής $4n - 1 = 4(n - 1) + 3$ και δεν διαιρείται με κανέναν από τους πρώτους μέχρι τον p. Όμως ο q δεν μπορεί να είναι γινόμενο πρώτων της μορφής $4x + 1$ μόνο, αφού

σύμφωνα με την προκαταρκτική παρατήρηση ένα γινόμενο αριθμών της μορφής $4x+1$ είναι της ίδιας μορφής. Προκύπτει επομένως ότι ο q διαιρείται με κάποιον πρώτο της μορφής $4x+3$ που είναι αναγκαστικά μεγαλύτερος από τον p και αυτό είναι άτοπο. Άρα υπάρχουν όντως άπειροι πρώτοι της ζητούμενης μορφής. ■

Μπορούμε να δείξουμε ότι υπάρχουν άπειροι πρώτοι *και* της μορφής $4n+1$, αλλά αυτή η περίπτωση είναι πιο δύσκολη. Η δυσκολία προκύπτει επειδή ένας αριθμός της μορφής $4n+1$ *μπορεί* να είναι γινόμενο αριθμών της μορφής $4n+3$.

Θα δούμε μία ακόμα τέτοια εφαρμογή «τύπου Ευκλείδη». Πριν την δούμε, μια παρατήρηση. Με εξαίρεση τους 2 και 3, κάθε πρώτος είναι της μορφής $6n+1$ ή της μορφής $6n+5$, διότι διαφορετικά είτε ο 2 είτε ο 3 διαιρεί *γνήσια* τον αριθμό. Ακόμα, αν δύο ακέραιοι a, b είναι και οι δύο της μορφής $6x+1$, τότε και το γινόμενό τους είναι της ίδιας μορφής και άρα (επαγωγικά) το γινόμενο οσωνδήποτε αριθμών της μορφής $6x+1$ είναι αυτής της μορφής. Πάμε τώρα.

Θεώρημα 7.2.2. *Υπάρχουν άπειροι πρώτοι της μορφής* $6n+5$.

Απόδειξη. Επιχειρηματολογούμε όπως στην προηγούμενη απόδειξη, μόνο που εδώ ορίζουμε τον αριθμό που θα μας δώσει το άτοπο ως

$$q = 2 \cdot 3 \cdot 5 \cdots p - 1.$$

Ο q είναι της μορφής $6n-1 = 6(n-1)+5$ και δεν διαιρείται με κανέναν από τους πρώτους μέχρι τον p. Θα πρέπει επομένως να υπάρχει πρώτος της μορφής $6x+5$ που είναι εκτός της λίστας μας. ■

Προσέξτε τώρα ότι οι ακολουθίες $(4n+1)$ και $(6n+5)$ είναι και οι δύο αριθμητικές πρόοδοι. Κάθε όρος δηλαδή διαφέρει από τον προηγούμενό του μία σταθερή ποσότητα (4 ή 6 αντίστοιχα). Επίσης, την Απειρία των Πρώτων την δείξαμε ουσιαστικά για την πρόοδο (n), στην οποία κάθε όρος διαφέρει από τον προηγούμενό του κατά 1. Αν έχουμε μία αριθμητική πρόοδο $(an+b)$, μπορούμε (και πρέπει) να ρωτήσουμε αν είναι ικανή να μας δώσει άπειρους πρώτους.

Παρατηρούμε το εξής: αν ο d είναι ένας κοινός διαιρέτης των a, b, τότε ο d διαιρεί κάθε όρο της ακολουθίας $(an+b)$, επομένως αποκλείεται η $(an+b)$ να μας δώσει άπειρους πρώτους. Για να είναι λοιπόν μια πρόοδος «γεννήτρια» πρώτων, θα πρέπει οι a, b να είναι σχετικά πρώτοι.

Το λαμπρό Θεώρημα που έδειξε ο Peter Gustav Lejeune Dirichlet το 1837 είναι ότι η συνθήκη $\gcd(a,b)=1$ εκτός από αναγκαία είναι και ικανή.

Θεώρημα 7.2.3 (Το Θεώρημα του Dirichlet). *Αν οι* a, b *είναι ακέραιοι με* $a>0$ *και* $\gcd(a,b)=1$, *τότε υπάρχουν άπειροι πρώτοι της μορφής* $an+b$.

Αν, όπως ισχυριζόταν ο Gauss, η Θεωρία Αριθμών είναι η βασίλισσα των Μαθηματικών, τότε σίγουρα το Θεώρημα του Dirichlet είναι ένα από τα διαμάντια στο στέμμα της. Την απόδειξη του Θεωρήματος δεν είμαστε σε θέση να την δούμε, αφού απαιτεί βαθύτερες έννοιες και πιο προχωρημένα εργαλεία. Αρκούμαστε στο να αναφέρουμε ότι, με αυτό το Θεώρημα και τις μεθόδους που ανέπτυξε για να το αποδείξει, ο Dirichlet ουσιαστικά εκκίνησε ολόκληρο τον κλάδο της Αναλυτικής Θεωρίας Αριθμών.

Χρησιμοποιώντας το Θεώρημα του Dirichlet για παράδειγμα, μπορούμε να δείξουμε ότι υπάρχουν άπειροι πρώτοι οι οποίοι τελειώνουν σε οσοδήποτε μεγάλο αριθμό από διαδοχικά 9

θέλουμε. Φερ' ειπείν, υπάρχουν άπειροι πρώτοι που τελειώνουν σε 999, όπως οι

$$1999, 100999, 1000999, \ldots,$$

αφού αυτοί εμφανίζονται στην πρόοδο $1000n+999$, όπου έχουμε $\gcd(1000, 999) = 1$. Προσέξτε όμως ότι καμία πρόοδος δεν παράγει *μόνο* πρώτους, δηλαδή δεν υπάρχει πρόοδος $a, a+b, a+2b, \ldots$, τέτοια ώστε όλοι της οι όροι να είναι πρώτοι. Αν $a+nb = p$, όπου n φυσικός και p πρώτος, τότε θέτουμε $n_k = n+kp$, $k = 1, 2, 3, \ldots$, και έχουμε ότι ο n_kοστός όρος της ακολουθίας είναι ο

$$a + n_k b = a + (n + kp)b = (a + nb) + kpb = p + kpb$$

και το δεξί μέλος διαιρείται γνήσια με τον p.

7.3 Εικασίες για Πρώτους

Οι πρώτοι ασκούν την γοητεία τους σε επαγγελματίες και ερασιτέχνες μαθηματικούς εξίσου. Ο αριθμός των εικασιών που έχουν διατυπωθεί γι' αυτούς είναι τόσο μεγάλος που μπορούμε μόνο να αναφερθούμε στις σημαντικότερες από αυτές. Δείξαμε στο Θεώρημα 5.2.2 ότι τα «κενά» μεταξύ διαδοχικών πρώτων δεν είναι φραγμένα. Συμβαίνει συχνά όμως η διαφορά μεταξύ διαδοχικών πρώτων να είναι 2, όπως με τους $(3, 5)$, $(5, 7)$, $(11, 13)$, $(101, 103)$, $(4967, 4969)$ κλπ. Οι φυσικοί αυτοί καλούνται *δίδυμοι πρώτοι*. Τα αριθμητικά δεδομένα που έχουμε υποδεικνύουν ότι υπάρχουν άπειροι τέτοιοι δίδυμοι πρώτοι. Έχουμε 35 ζεύγη μέχρι το 10^3, 8169 ζεύγη μέχρι το 10^6, 3.424.506 ζεύγη μέχρι το 10^9 και 1.870.585.220 ζεύγη μέχρι το 10^{12}. Οδηγούμαστε λοιπόν στο εξής.

Εικασία 7.3.1 (Η Εικασία των Δίδυμων Πρώτων). Υπάρχουν άπειρα ζεύγη πρώτων p και $p+2$.

Το 1966 ο κινέζος μαθηματικός J. R. Chen έδειξε, χρησιμοποιώντας ιδιαίτερα εκλεπτυσμένες τεχνικές με κόσκινα (όπως αυτό του Ερατοσθένη), ότι υπάρχουν άπειροι πρώτοι p τέτοιοι ώστε ο $p+2$ να έχει το πολύ 2 πρώτους παράγοντες. Από το 2007 δύο ερευνητικά έργα παράλληλου υπολογισμού, το Twin Prime Search και το PrimeGrid, μας έχουν δώσει διάφορους τεράστιους δίδυμους πρώτους, ξεπερνώντας κάθε φορά το ρεκόρ της προηγούμενης. Το μεγαλύτερο ζεύγος δίδυμων πρώτων που γνωρίζουμε βρέθηκε τον Σεπτέμβρη του 2016 και είναι οι

$$2996863034895 \cdot 2^{1290000} \pm 1$$

με 388.342 δεκαδικά ψηφία.

Σε ό,τι αφορά τα «κενά» μεταξύ διαδοχικών πρώτων, σημειώνουμε ότι το Θεώρημα των Πρώτων Αριθμών μάς λέει ότι καθώς το n μεγαλώνει, το κενό μεταξύ του p_n και του p_{n+1} θα είναι περίπου $\log p_n$. Αρκετή δουλειά έχει γίνει για να δειχθεί ότι για άπειρους διαδοχικούς πρώτους το κενό μεταξύ τους είναι πολύ μικρότερο από τον «μέσο όρο». Το 2005 οι Daniel Goldston, János Pintz και Cem Yildirim έδειξαν ότι για κάθε θετική σταθερά c, υπάρχουν άπειρα ζεύγη διαδοχικών πρώτων p_n και p_{n+1} τέτοια ώστε $p_{n+1} - p_n < c \cdot \log p_n$. Έδειξαν ακόμα ότι, αν δεχτούμε την ισχύ των Εικασιών Elliott-Halberstam, τότε υπάρχουν άπειρα ζεύγη πρώτων που απέχουν το πολύ 16 μεταξύ τους. Για πιο πρόσφατα αποτελέσματα σε αυτόν τον τομέα, σας παραπέμπω στο βιβλίο των Αντωνιάδη και Κοντογεώργη.

Ο Viggo Brun έδειξε ότι το άθροισμα

$$\sum{}^{*} \frac{1}{p} = \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \ldots$$

όπου το $*$ συμβολίζει άθροισμα που εκτείνεται μόνο σε δίδυμους πρώτους, συγκλίνει σε μία σταθερά που καλείται «σταθερά του Brun» και είναι ίση περίπου με 1.902 160 582 4.

Κάτι αξιοπερίεργο τώρα: ο υπολογισμός της σταθεράς του Brun έπαιξε ρόλο στην ανακάλυψη σφαλμάτων στο τσιπ Pentium της Intel. Το 1994 ο Thomas Nicely στο Lynchberg College της Virginia υπολόγισε την σταθερά του Brun με δύο διαφορετικούς τρόπους χρησιμοποιώντας ένα PentiumPC και βρήκε δύο διαφορετικά αποτελέσματα. Ενημέρωσε την Intel, η οποία, όπως φάνηκε τελικά, γνώριζε ότι υπήρχε πρόβλημα με τον τρόπο που τα τσιπάκια της εκτελούσαν αριθμητική κινητής υποδιαστολής, αλλά εφ' όσον το πρόβλημα θα επηρέαζε ελάχιστους χρήστες, αποφάσισε να το κάνει γαργάρα το θέμα. Το αποτέλεσμα εν ολίγοις ήταν να γίνει ρόμπα η εταιρεία και να χάσει πολλά εκατομμύρια δολάρια και βασικός υπεύθυνος γι' αυτό ήταν η σταθερά του Brun!

Ας δούμε τώρα την πιο περιβόητη εικασία για πρώτους.

Εικασία 7.3.2 (Η Εικασία του Goldbach). Κάθε άρτιος φυσικός μεγαλύτερος του 2 γράφεται σαν άθροισμα δύο πρώτων.

Η εικασία αυτή διατυπώθηκε από τον Christian Goldbach σε γράμμα του προς τον Leonhard Euler το 1742. Έκτοτε έχουν καταβληθεί σημαντικές προσπάθειες για την απόδειξή της, ενώ έχει επιβεβαιωθεί για όλους τους άρτιους μικρότερους του $4 \cdot 10^{18}$. Παραμένει όμως ακόμα αλώβητη.

Αξίζει να αναφέρουμε ότι υπάρχει και μια δεύτερη εικασία ή ασθενής εικασία του Goldbach σύμφωνα με την οποία κάθε περιττός ακέραιος αριθμός μεγαλύτερος του 5 μπορεί να εκφραστεί ως άθροισμα τριών πρώτων. (Η εικασία ονομάζεται ασθενής, γιατί αν αποδειχθεί η κύρια εικασία, η απόδειξη αυτής είναι εύκολη. Κάθε άρτιος ακέραιος σύμφωνα με την εικασία, μπορεί να γραφεί ως άθροισμα δύο πρώτων. Προσθέτοντας σε αυτό το άθροισμα το 3, κατασκευάζονται όλοι οι περιττοί αριθμοί οι οποίοι είναι μεγαλύτεροι του 5.) Η ασθενής εικασία αποδείχτηκε τελικά το 2013 από τον περουβιανό μαθηματικό Harald Andrés Helfgott.

Υπάρχουν ακόμα διάφορες εικασίες για πρώτους συγκεκριμένης μορφής, όπως για παράδειγμα η επόμενη.

Εικασία 7.3.3 (Η Εικασία n^2+1). Υπάρχουν άπειροι πρώτοι της μορφής n^2+1, όπου n φυσικός.

Για παράδειγμα, έχουμε $2 = 1^2 + 1$, $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$, $101 = 10^2 + 1$, $197 = 14^2 + 1$, κλπ. Το καλύτερο αποτέλεσμα που έχουμε στην διάθεσή μας είναι αυτό του Henryk Iwaniec από το 1973, σύμφωνα με το οποίο υπάρχουν άπειροι φυσικοί n τέτοιοι ώστε ο $n^2 + 1$ είναι είτε πρώτος είτε γινόμενο δύο πρώτων.

Μέχρι τώρα έχουμε αναφερθεί σε τρία από τα τέσσερα προβλήματα για πρώτους τα οποία ο σπουδαίος αριθμοθεωρητικός Edmund Landau χαρακτήρισε ως «απόρθητα» στην ομιλία του στο Διεθνές Μαθηματικό Συνέδριο του 1912. Ιδού το τελευταίο.

Εικασία 7.3.4 (Η Εικασία του Legendre). Υπάρχει τουλάχιστον ένας πρώτος μεταξύ δύο διαδοχικών τέλειων τετραγώνων.

Την Εικασία διατύπωσε ο γνωστός μας Adrien-Marie Legendre. Με βάση πίνακες για κενά μεταξύ πρώτων, η Εικασία ισχύει για $n \leqslant 4 \cdot 10^{18}$, ενώ από αποτέλεσμα του Ingham προκύπτει το ασθενέστερο: υπάρχει πρώτος μεταξύ διαδοχικών κύβων για αρκετά μεγάλες τιμές.

Να αναφέρουμε κλείνοντας ότι, αν και όλα τα παραπάνω προβλήματα παραμένουν ανοιχτά,

έχει σημειωθεί στο μεταξύ τουλάχιστον μερική πρόοδος σε όλα. Τα δε μαθηματικά που χρησιμοποιούνται για να δειχθούν τα διάφορα μερικά αποτελέσματα είναι εξαιρετικά δύσκολα.

7.4 Ασκήσεις

Άσκηση 7.4.1. Δείξτε ότι κάθε ακέραιος > 11 είναι το άθροισμα δύο σύνθετων φυσικών.

Απόδειξη. Έστω $n > 11$. Αν ο n είναι άρτιος, τότε $n = (n-4)+4$ και άρα ο n γράφεται ως άθροισμα δύο σύνθετων (ο $n-4$ είναι σύνθετος, γιατί είναι άρτιος και μεγαλύτερος του 2). Αν ο n είναι περιττός, τότε $n = (n-9)+9$ και άρα πάλι ο n γράφεται γράφεται ως άθροισμα δύο σύνθετων (ο $n-9$ εδώ είναι σύνθετος, γιατί είναι άρτιος και μεγαλύτερος του 2). ■

Άσκηση 7.4.2. Αν $\{q_1, q_2, \ldots, q_m\}$ είναι ένα σύνολο πρώτων, να δείξετε ότι ο

$$\frac{1}{q_1} + \frac{1}{q_2} + \ldots + \frac{1}{q_m}$$

δεν είναι ακέραιος.

Απόδειξη. Ας υποθέσουμε αντίθετα ότι $q_1 < q_2 < \ldots < q_m$ είναι πρώτοι τέτοιοι ώστε

$$\frac{1}{q_1} + \frac{1}{q_2} + \ldots + \frac{1}{q_m} = n$$

για κάποιον φυσικό $n \geqslant 1$. Τότε

$$\frac{1}{q_1} = n - \frac{1}{q_2} - \ldots - \frac{1}{q_m} = \frac{r}{q_2 \cdots q_m},$$

όπου r ακέραιος. Προκύπτει τώρα ότι ο q_1 διαιρεί τον $q_2 \cdots q_m$ και άρα ο q_1 θα πρέπει να διαιρεί κάποιον q_i από το Πόρισμα 4.1.3. Αυτό όμως είναι άτοπο. ■

Άσκηση 7.4.3. Δείξτε ότι η Εικασία του Goldbach είναι ισοδύναμη με την εξής πρόταση: κάθε ακέραιος > 5 γράφεται ως άθροισμα τριών πρώτων.

Απόδειξη. Έστω ακέραιος $n > 5$ και ότι ισχύει η Εικασία του Goldbach. Αν ο n είναι άρτιος, τότε υπάρχουν δύο πρώτοι p, q τέτοιοι ώστε $n-2 = p+q$, δηλαδή $n = p+q+2$. Αν ο n είναι περιττός, τότε υπάρχουν δύο πρώτοι p, q τέτοιοι ώστε $n-3 = p+q$, δηλαδή $n = p+q+3$. Σε κάθε περίπτωση έχουμε ότι ο n γράφεται ως άθροισμα τριών πρώτων.

Έστω τώρα ότι κάθε ακέραιος > 5 γράφεται ως άθροισμα τριών πρώτων. Έστω ακόμα $n \geqslant 4$ άρτιος. Τότε υπάρχουν τρεις πρώτοι p, q, r τέτοιοι ώστε $n+2 = p+q+r$. Εφ' όσον ο $n+2$ είναι άρτιος, ένας εκ των p, q, r είναι ο 2, ας πούμε ο r. Τότε $n = p+q$ και άρα ο n γράφεται ως άθροισμα δύο πρώτων. ■

Άσκηση 7.4.4. Δείξτε ότι υπάρχουν άπειροι πρώτοι p τέτοιοι ώστε οι $p-2$, $p+2$ να είναι και οι δύο σύνθετοι.

Υπόδειξη: Χρησιμοποιήστε το Θεώρημα του Dirichlet για κατάλληλους a, b.

Απόδειξη. Από το Θεώρημα του Dirichlet προκύπτει ότι η πρόοδος $(15n+7)$, όπου n φυσικός, περιέχει άπειρους πρώτους, εφ' όσον $\gcd(15, 7) = 1$. Αν τώρα ο $p = 15k+7$ είναι πρώτος, τότε

οι $p-2 = 15k+5 = 5(3k+2)$ και $p+2 = 15k+9 = 3(5k+3)$ είναι σίγουρα και οι δύο σύνθετοι και το ζητούμενο έπεται. ■

Άσκηση 7.4.5. $(*)$ Χρησιμοποιήστε το Θεώρημα των Πρώτων Αριθμών για να δείξετε ότι το σύνολο των ρητών της μορφής p/q, όπου p, q πρώτοι, είναι πυκνό στο σύνολο των θετικών πραγματικών.

Σημείωση: Σε περίπτωση που δεν έχετε δει ήδη ή δεν θυμάστε την έννοια της πυκνότητας, καλείστε εδώ να δείξετε ότι μεταξύ δύο οποιωνδήποτε θετικών πραγματικών αριθμών x, y με $x < y$, υπάρχει $s = p/q$ τέτοιο ώστε $x < s < y$.

Απόδειξη. Έστω x, y θετικοί πραγματικοί με $x < y$. Έστω ακόμα q πρώτος. Τότε θα υπάρχει πρώτος p τέτοιος ώστε $x < p/q < y$ αν και μόνο αν $\pi(yq) > \pi(xq)$. Από το Θεώρημα των Πρώτων Αριθμών και βασικές ιδιότητες των ορίων έχουμε

$$\lim_{q\to\infty} \frac{\pi(yq)}{\pi(xq)} = \lim_{q\to\infty} \frac{y\log(xq)}{x\log(yq)} = \lim_{q\to\infty} \frac{y(\log q + \log x)}{x(\log q + \log y)} = \frac{y}{x} > 1.$$

Επομένως για q αρκετά μεγάλο θα έχουμε $\pi(yq)/\pi(xq) > 1$, όπως θέλαμε. ■

Κεφάλαιο 8

8η Παράδοση

Έχοντας μιλήσει για τους πρώτους στα τέσσερα προηγούμενα μαθήματα (τα οποία ίσως να ήταν και κάπως αγχωτικά με όλο αυτόν τον όγκο πληροφοριών, τα προχωρημένα θεωρήματα και την δύσκολη απόδειξη του Αιτήματος του Bertrand) επιστρέφουμε τώρα σε μια μεγαλύτερη κανονικότητα.

Στο σημερινό μάθημα θα αναφερθούμε στις *ισοτιμίες* και την *αριθμητική* τους. Θα προσέξατε ίσως ότι σε πολλές περιπτώσεις μάς ενδιαφέρει μόνο το υπόλοιπο που αφήνει ένας αριθμός αν διαιρεθεί με κάποιον άλλο. Πριν διατυπώσουμε το Θεώρημα 7.2.1 για παράδειγμα, δείξαμε ότι, αν μας δίνονται δύο ακέραιοι a, b που είναι και οι δύο της μορφής $4n+1$, τότε και ο ab είναι της ίδιας μορφής. Το μόνο που είχε σημασία στην απόδειξη, ήταν το υπόλοιπο που αφήνουν οι a, b αν διαιρεθούν με το 4, ενώ τα πηλίκα τους μάς ήταν πρακτικά αδιάφορα. Η αριθμητική των ισοτιμιών λοιπόν είναι ουσιαστικά η αριθμητική των υπολοίπων.

8.1 Η Αριθμητική των Ισοτιμιών

Τον συμβολισμό που θα εισαγάγουμε σε λίγο, τον επινόησε ο μεγάλος Gauss και κάνει την εμφάνισή του για πρώτη φορά στο μνημειώδες έργο του Disquisitiones Arithmeticae (1801), το οποίο έγραψε όταν ήταν 24 ετών και το οποίο έβαλε ουσιαστικά τα θεμέλια της μοντέρνας Θεωρίας Αριθμών.

Ορισμός 8.1.1. Δύο ακέραιοι a, b λέγονται **ισότιμοι** ως προς μέτρο n ή $\bmod n$, όπου n είναι ένας φυσικός, αν ο n διαιρεί τον $a-b$. Αυτό το συμβολίζουμε γράφοντας

$$a \equiv b \pmod{n},$$

ενώ αν ο n δεν διαιρεί τον $a-b$, τότε λέμε ότι οι a, b είναι **ανισότιμοι** και γράφουμε

$$a \not\equiv b \pmod{n}.$$

Έχουμε για παράδειγμα ότι $24 \equiv 3 \pmod 7$, $65 \equiv 44 \pmod 3$ και $11 \equiv -9 \pmod{10}$. Παρατηρήστε ότι η ισοτιμία $a \equiv b \pmod 1$ ισχύει για οποιουσδήποτε δύο ακεραίους a, b, επομένως δεν είναι ιδιαίτερα ενδιαφέρουσα. Παρατηρήστε ακόμα ότι $a \equiv b \pmod 2$ αν και μόνο αν οι a, b είναι είτε και οι δύο άρτιοι είτε και οι δύο περιττοί.

Έστω τώρα a ακέραιος και q, r αντίστοιχα το πηλίκο και το υπόλοιπο της διαίρεσής του με τον n, έτσι ώστε

$$a = qn + r \qquad 0 \leqslant r < n.$$

Τότε έχουμε εξ ορισμού $a \equiv r \pmod{n}$. Εφ' όσον υπάρχουν n τιμές που μπορεί να πάρει το r, βλέπουμε ότι κάθε ακέραιος είναι ισότιμος $\bmod n$ με μία ακριβώς από τις τιμές $0, 1, 2, \ldots, n-1$. Επίσης, $a \equiv 0 \pmod{n}$ αν και μόνο αν $n \mid a$. Το σύνολο των n ακεραίων $0, 1, 2, \ldots, n-1$ λέγεται *σύνολο ελάχιστων μη αρνητικών υπολοίπων* $\bmod n$.

Γενικότερα, μια συλλογή n ακεραίων $a_1, a_2, \ldots, a_n$ καλείται πλήρες σύστημα (ή σύνολο) υπολοίπων $\bmod n$ αν κάθε ακέραιος είναι ισότιμος $\bmod n$ με έναν και μόνο έναν από τους a_k. Για παράδειγμα, οι

$$-12, \ -4, \ 11, \ 13, \ 22, \ 82, \ 91$$

είναι ένα πλήρες σύστημα υπολοίπων $\bmod 7$, αφού

$$-12 \equiv 2 \qquad -4 \equiv 3 \qquad 11 \equiv 4 \qquad 13 \equiv 6 \qquad 22 \equiv 1 \qquad 82 \equiv 5 \qquad 91 \equiv 0$$

με όλες τις ισοτιμίες θεωρούμενες $\bmod 7$. Μια σημαντική παρατήρηση: ένα σύνολο n ακεραίων είναι ένα πλήρες σύστημα υπολοίπων $\bmod n$, αν και μόνο αν ανά δύο αυτοί οι ακέραιοι είναι ανισότιμοι $\bmod n$. Έχουμε τώρα το εξής.

Θεώρημα 8.1.2. *Έστω a, b ακέραιοι. Τότε $a \equiv b \pmod{n}$, αν και μόνο αν οι a, b αφήνουν το ίδιο υπόλοιπο όταν διαιρούνται με τον n.*

Απόδειξη. Αν $a \equiv b \pmod{n}$, τότε $a = b + kn$ για κάποιον ακέραιο k. Αν τώρα ο b αφήνει υπόλοιπο r κατά την διαίρεσή του με τον n, δηλαδή $b = qn + r$ για κάποιον ακέραιο q και $0 \leqslant r < n$, τότε

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

και από αυτή την σχέση προκύπτει ότι ο a αφήνει το ίδιο υπόλοιπο με τον b.

Αντίστροφα τώρα, έστω ότι $a = q_1 n + r$ και $b = q_2 n + r$, όπου $0 \leqslant r < n$. Τότε

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$$

και άρα $n \mid a - b$, δηλαδή $a \equiv b \pmod{n}$. ■

Η σχέση της ισοτιμίας μπορεί να ιδωθεί ως μια γενικευμένη μορφή ισότητας με την έννοια ότι η συμπεριφορά της ως προς την πρόσθεση και τον πολλαπλασιασμό είναι παρόμοια με αυτήν της κανονικής ισότητας. Αυτό το κάνουμε πιο συγκεκριμένο στο επόμενο θεώρημα.

Θεώρημα 8.1.3. *Έστω $n > 1$ φυσικός και a, b, c, d ακέραιοι. Τότε ισχύουν τα ακόλουθα:*

(i) $a \equiv a \pmod{n}$.

(ii) *Αν* $a \equiv b \pmod{n}$, *τότε* $b \equiv a \pmod{n}$.

(iii) *Αν* $a \equiv b \pmod{n}$ *και* $b \equiv c \pmod{n}$, *τότε* $a \equiv c \pmod{n}$.

(iv) *Αν* $a \equiv b \pmod{n}$ *και* $c \equiv d \pmod{n}$, *τότε* $a + c \equiv b + d \pmod{n}$ *και* $ac \equiv bd \pmod{n}$.

(v) *Αν* $a \equiv b \pmod{n}$, *τότε* $a + c \equiv b + c \pmod{n}$ *και* $ac \equiv bc \pmod{n}$.

(vi) *Αν* $a \equiv b \pmod{n}$, *τότε* $a^k \equiv b^k \pmod{n}$ *για κάθε φυσικό* k.

Απόδειξη. (i) Έχουμε $a - a = 0 \cdot n$ και άρα $a \equiv a \pmod{n}$.

(ii) Αν $a \equiv b \pmod{n}$, τότε $a - b = kn$ για κάποιον ακέραιο k. Επομένως, $b - a = -(kn) = (-k)n$ και εφ' όσον ο $-k$ είναι επίσης ακέραιος, παίρνουμε $b \equiv a \pmod{n}$.

(iii) Από την σχέση $a \equiv b \pmod{n}$ έχουμε ότι υπάρχει ακέραιος h τέτοιος ώστε $a - b = hn$. Ομοίως, η σχέση $b \equiv c \pmod{n}$ μας δίνει $b - c = kn$ για κάποιον ακέραιο k. Έχουμε τώρα

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n,$$

δηλαδή $a \equiv c \pmod{n}$.

(iv) Παρόμοια με πριν, οι δοθείσες σχέσεις μάς δίνουν ακέραιους k_1, k_2 τέτοιους ώστε $a - b = k_1 n$ και $c - d = k_2 n$. Προσθέτοντας, παίρνουμε

$$(a + c) - (b + d) = (a - b) + (c - d) = k_1 n + k_2 n = (k_1 + k_2)n,$$

δηλαδή $a + c \equiv b + d \pmod{n}$. Σχετικά με τον δεύτερο ισχυρισμό, έχουμε

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n.$$

Ο $bk_2 + dk_1 + k_1 k_2 n$ είναι ακέραιος, που σημαίνει ότι ο n διαιρεί τον $ac - bd$. Επομένως $ac \equiv bd \pmod{n}$.

(v) Παρατηρήστε ότι αυτή η ιδιότητα προκύπτει από την προηγούμενη, αφού $c \equiv c \pmod{n}$ (παίρνοντας δηλαδή $c = d$).

(vi) Δείχνουμε την τελευταία ιδιότητα με επαγωγή στο k. Για $k = 1$ ο ισχυρισμός ισχύει ταυτοτικά. Έστω τώρα ότι το ζητούμενο ισχύει για k. Από την (iv) γνωρίζουμε ότι οι σχέσεις $a \equiv b \pmod{n}$ και $a^k \equiv b^k \pmod{n}$ (την δεύτερη την έχουμε από την επαγωγική υπόθεση) μας δίνουν από κοινού ότι $aa^k \equiv bb^k \pmod{n}$ ή ισοδύναμα $a^{k+1} \equiv b^{k+1} \pmod{n}$. Επομένως η επαγωγή είναι πλήρης και έχουμε το ζητούμενο. ■

Το θεώρημα που μόλις δείξαμε, περιγράφει στην ουσία τον *λογισμό* των ισοτιμιών. Κάτι που δεν είδαμε και θα το δούμε σε λίγο, είναι πότε και πώς μπορούμε να «διαιρούμε» στις ισοτιμίες. Ας δούμε όμως μερικά παραδείγματα πρώτα.

Παράδειγμα 8.1.4. Θα δείξουμε ότι $41 \mid 2^{20} - 1$. Έχουμε αρχικά ότι $2^5 \equiv -9 \pmod{41}$ και άρα $(2^5)^4 \equiv (-9)^4 \pmod{41}$ από την (vi) του Θεωρήματος 8.1.3. Δηλαδή, $2^{20} \equiv 81 \cdot 81 \pmod{41}$. Όμως $81 \equiv -1 \pmod{41}$, άρα $81 \cdot 81 \equiv 1 \pmod{41}$. Χρησιμοποιώντας τώρα τις (ii) και (v) του Θεωρήματος 8.1.3, φτάνουμε στο ζητούμενο

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}.$$

Άρα $41 \mid 2^{20} - 1$, όπως ισχυριστήκαμε.

Παράδειγμα 8.1.5. Ας υποθέσουμε τώρα ότι θέλουμε να βρούμε το υπόλοιπο της διαίρεσης του

$$1! + 2! + 3! + \ldots + 99! + 100!$$

με τον 12. Παρατηρούμε ότι $4! = 24 \equiv 0 \pmod{12}$. Άρα για $k \geqslant 4$ έχουμε

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}$$

από την οποία προκύπτει ότι

$$1! + 2! + 3! + \ldots + 99! + 100! \equiv 1! + 2! + 3! + 0 + \ldots + 0 \equiv 9 \pmod{12}.$$

Επομένως το υπόλοιπο που ψάχναμε είναι ίσο με 9.

Στην πραγματικότητα, δεν υπάρχει κάτι που μπορούμε να κάνουμε *μόνο* με ισοτιμίες και όχι κάπως αλλιώς. Θα μπορούσαμε να είχαμε δείξει το ζητούμενο και στα δύο παραδείγματα που μόλις είδαμε, χρησιμοποιώντας απλά ιδιότητες της διαιρετότητας. Αυτό που παρατηρούμε όμως είναι ότι ο λογισμός των ισοτιμιών που έχουμε πλέον στην διάθεσή μας, κάνει την ζωή μας ευκολότερη. Ο συμβολισμός της ισοτιμίας (ο οποίος παραπέμπει σε αυτόν της ισότητας) είναι εύχρηστος και δυναμικός· αυτά ακριβώς είναι τα χαρακτηριστικά που ψάχνουμε σε ένα μαθηματικό σύμβολο.

Επιστρέφουμε τώρα σε μία πλάγια ερώτηση που θέσαμε πριν. Είδαμε στο Θεώρημα 8.1.3 ότι αν $a \equiv b \pmod{n}$, τότε $ca \equiv cb \pmod{n}$ για κάθε ακέραιο c. Προσέξτε τώρα ότι το αντίστροφο **δεν** ισχύει. Ένα εύκολο παράδειγμα:

$$2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}, \quad \text{αλλά} \quad 4 \not\equiv 1 \pmod{6}.$$

Επομένως δεν είμαστε σε θέση *πάντα* να απλοποιούμε μια σχέση ισοτιμίας διαγράφοντας κοινούς όρους. Αυτό που μπορούμε να κάνουμε όμως είναι το εξής.

Θεώρημα 8.1.6. *Αν* $ca \equiv cb \pmod{n}$, *τότε* $a \equiv b \pmod{n/d}$, *όπου* $d = \gcd(c, n)$.

Απόδειξη. Εξ υποθέσεως, μπορούμε να γράψουμε

$$c(a - b) = ca - cb = kn$$

για κάποιον ακέραιο k. Με δεδομένο το $\gcd(c, n) = d$, υπάρχουν σχετικά πρώτοι ακέραιοι r, s τέτοιοι ώστε $c = dr$, $n = ds$. (Ότι οι r, s είναι σχετικά πρώτοι προκύπτει από το Πόρισμα 2.2.9.) Αντικαθιστούμε και έχουμε

$$dr(a - b) = kds.$$

Διαγράφοντας τον d, παίρνουμε

$$r(a - b) = ks.$$

Προκύπτει επομένως ότι $s \mid r(a - b)$, ενώ ταυτόχρονα $\gcd(r, s) = 1$. Από το Λήμμα τώρα του Ευκλείδη (Θεώρημα 2.2.11) παίρνουμε ότι $s \mid a - b$ και άρα $a \equiv b \pmod{n/d}$. ■

Προκύπτει άμεσα από το θεώρημα που μόλις δείξαμε, το εξής χρήσιμο.

Πόρισμα 8.1.7. *Αν* $ca \equiv cb \pmod{n}$ *και* $\gcd(c, n) = 1$, *τότε* $a \equiv b \pmod{n}$.

Έχουμε μία ακόμα ειδική περίπτωση να καταγράψουμε ξεχωριστά.

Πόρισμα 8.1.8. *Αν* $ca \equiv cb \pmod{p}$ *και* $p \nmid c$, *όπου* p *πρώτος, τότε* $a \equiv b \pmod{p}$.

Απόδειξη. Αφού ο p είναι πρώτος και $p \nmid c$, έπεται ότι $\gcd(c, p) = 1$. Άρα μπορούμε να εφαρμόσουμε το Πόρισμα 8.1.7 με $n = p$. ■

Παράδειγμα 8.1.9. Θεωρήστε την ισοτιμία $33 \equiv 15 \pmod{9}$, δηλαδή την $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$. Εφ' όσον $\gcd(3, 9) = 3$, έχουμε από το Θεώρημα 8.1.6 ότι $11 \equiv 5 \pmod{3}$. Επίσης, $-35 \equiv 45 \pmod{8}$, δηλαδή $5 \cdot (-7) \equiv 5 \cdot 9 \pmod{8}$. Οι ακέραιοι 5 και 8 είναι σχετικά πρώτοι, επομένως ο κοινός όρος 5 μπορεί να διαγραφεί και να πάρουμε $-7 \equiv 9 \pmod{8}$.

Προσέξτε κάτι τελευταίο. Μια περίεργη κατάσταση μπορεί να προκύψει με τις ισοτιμίες. Το γινόμενο δύο ακεραίων, κανένας εκ των οποίων δεν είναι ισότιμος με 0 ως προς κάποιο μέτρο, μπορεί να είναι ισότιμο με 0. Για παράδειγμα, $4 \cdot 3 \equiv 0 \pmod{12}$, αλλά $4 \not\equiv 0 \pmod{12}$ και $3 \not\equiv 0 \pmod{12}$. Αν όμως $ab \equiv 0 \pmod{n}$ και $\gcd(a, n) = 1$, τότε $b \equiv 0 \pmod{n}$, αφού το Πόρισμα 8.1.7 μας επιτρέπει να διαγράψουμε τον κοινό όρο a από την $ab \equiv a \cdot 0 \pmod{n}$. Συγκεκριμένα, αν $ab \equiv 0 \pmod{p}$, όπου p πρώτος, τότε είτε $a \equiv 0 \pmod{p}$ είτε $b \equiv 0 \pmod{p}$.

8.2 Ασκήσεις

Άσκηση 8.2.1. Δείξτε καθέναν από τους παρακάτω ισχυρισμούς:

(i) Αν $a \equiv b \pmod{n}$ και $m \mid n$, τότε $a \equiv b \pmod{m}$.

(ii) Αν $a \equiv b \pmod{n}$ και $c > 0$, τότε $ca \equiv cb \pmod{cn}$.

(iii) Αν $a \equiv b \pmod{n}$ και οι ακέραιοι a, b, n διαιρούνται όλοι με τον d, τότε

$$a/d \equiv b/d \pmod{n/d}\,.$$

Απόδειξη. (i) Έχουμε ότι $m \mid n$ και $n \mid (a - b)$. Άρα $m \mid (a - b)$, δηλαδή $a \equiv b \pmod{m}$.

(ii) Από την σχέση $a \equiv b \pmod{n}$ προκύπτει ότι υπάρχει ακέραιος k τέτοιος ώστε $a - b = kn$, δηλαδή $c \cdot (a - b) = k \cdot (cn)$. Άρα $ca \equiv cb \pmod{cn}$.

(iii) Όπως και πριν, από την σχέση $a \equiv b \pmod{n}$ προκύπτει ότι υπάρχει ακέραιος k τέτοιος ώστε $a - b = kn$. Αν διαιρέσουμε τώρα με d, παίρνουμε $a/d - b/d = k(n/d)$, όπου οι a/d, b/d και n/d είναι όλοι ακέραιοι. Επομένως $a/d \equiv b/d \pmod{n/d}$, όπως θέλαμε. ■

Άσκηση 8.2.2. Δείξτε με ένα παράδειγμα ότι από την σχέση $a^2 \equiv b^2 \pmod{n}$ δεν έπεται ότι $a \equiv b \pmod{n}$.

Απόδειξη. Μπορούμε να βρούμε πολλά τέτοια παραδείγματα. Ένα είναι το $4^2 \equiv 2^2 \pmod{12}$, αλλά $4 \not\equiv 2 \pmod{12}$. ■

Άσκηση 8.2.3. Σε γράμμα του στον Christian Huygens $(1629 - 1695)$ το 1659, ο Fermat έγραφε ότι χρησιμοποιώντας την Άπειρη Κάθοδό του (ίσως την ξανασυναντήσουμε αργότερα αυτή την μέθοδο) κατάφερε να δείξει ότι κανένας φυσικός της μορφής $3k - 1$ δεν γράφεται ως $x^2 + 3y^2$, όπου x, y φυσικοί. Βρείτε μια απλή απόδειξη αυτού του ισχυρισμού.

Απόδειξη. Αν η εξίσωση $3k - 1 = x^2 + 3y^2$ είχε λύση, τότε θα είχαμε $x^2 \equiv -1 \pmod{3}$ κάτι που είναι αδύνατο αφού $x^2 \equiv 0, 1 \pmod{3}$. ■

Άσκηση 8.2.4. Δείξτε ότι αν $a \equiv b \pmod{n}$, τότε $\gcd(a, n) = \gcd(b, n)$.

Απόδειξη. Θέτουμε $d_1 = \gcd(a, n)$, $d_2 = \gcd(b, n)$ και παρατηρούμε ότι για να δείξουμε την $d_1 = d_2$, αρκεί να δείξουμε ότι $d_1 \mid d_2$ και $d_2 \mid d_1$.

Αρχικά η σχέση $a \equiv b \pmod{n}$ μας δίνει το ισοδύναμο $n \mid (a - b)$. Αφού ο d_1 διαιρεί και τον a και τον n, προκύπτει ότι $d_1 \mid a$ και $d_1 \mid (a - b)$. Άρα ο d_1 διαιρεί και την διαφορά τους, δηλαδή τον αριθμό $a - (a - b) = b$. Έπεται λοιπόν ότι ο d_1 είναι κοινός διαιρέτης των b και n, επομένως $d_1 \mid d_2$.

Ανάλογα προκύπτει και η άλλη σχέση. Δηλαδή, ο d_2 διαιρεί και τον b και τον n, επομένως $d_2 \mid b$ και $d_2 \mid (a-b)$. Άρα ο d_2 διαιρεί το άθροισμα $b+(a-b)=a$. Συνεπώς ο d_2 είναι κοινός διαιρέτης των a και n, οπότε έχουμε $d_2 \mid d_1$, όπως θέλαμε να δείξουμε. ■

Άσκηση 8.2.5. Για ποιους φυσικούς n είναι ο 3^n+1 πολλαπλάσιο του 10;

Λύση. Παρατηρούμε αρχικά ότι

$$3^4 = 81 \equiv 1 \pmod{10}.$$

Επομένως

$$3^{4m} \equiv 1 \pmod{10}$$

για κάθε ακέραιο $m \geqslant 0$. Κάθε φυσικός n τώρα γράφεται ως $4m$, $4m+1$, $4m+2$ ή $4m+3$ για κάποιον ακέραιο $m \geqslant 0$.

Άρα έχουμε τις εξής περιπτώσεις:

- αν $n = 4m$, τότε $3^{4m}+1 \equiv 1 \cdot 1 + 1 \equiv 2 \pmod{10}$,
- αν $n = 4m+1$, τότε $3^{4m+1}+1 \equiv 3 \cdot 1 + 1 \equiv 4 \pmod{10}$,
- αν $n = 4m+2$, τότε $3^{4m+2}+1 \equiv 3^2 \cdot 1 + 1 \equiv 0 \pmod{10}$,
- αν $n = 4m+3$, τότε $3^{4m+3}+1 \equiv 3^3 \cdot 1 + 1 \equiv 8 \pmod{10}$.

Προκύπτει λοιπόν ότι $3^n+1 \equiv 0 \pmod{10}$, αν και μόνο αν ο n είναι της μορφής $4m+2$ με $m \geqslant 0$, δηλαδή όταν $n \equiv 2 \pmod{4}$. ■

Άσκηση 8.2.6. Δείξτε ότι αν ο a είναι περιττός, τότε $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ για κάθε φυσικό n.

Υπόδειξη: Δουλέψτε με επαγωγή στο n. Το Παράδειγμα 2.1.3 είναι σχετικό.

Απόδειξη. Θα δείξουμε το ζητούμενο κάνοντας (απλή) επαγωγή στο n.

Για $n=1$ το ζητούμενο ισχύει και είναι το περιεχόμενο του Παραδείγματος 2.1.3.

Υποθέτουμε τώρα ότι το ζητούμενο ισχύει για n και θέλουμε να δείξουμε ότι ισχύει και για $n+1$. Για μεγαλύτερη ευκολία στον συμβολισμό, ας θέσουμε $b = a^{2^n}$. Ξέρουμε (από την επαγωγική υπόθεση) ότι $b \equiv 1 \pmod{2^{n+2}}$, δηλαδή $b-1 \equiv 0 \pmod{2^{n+2}}$. Επομένως υπάρχει ακέραιος k τέτοιος ώστε $b-1 = k \cdot 2^{n+2}$. Τότε

$$b^2 - 1 = (b+1)k2^{n+2} = \left(k \cdot \frac{b+1}{2}\right) 2^{n+3}$$

Όμως ο $\left(k \cdot \frac{b+1}{2}\right)$ είναι ακέραιος, αφού ο b είναι περιττός. Έπεται ότι $b^2 - 1 \equiv 0 \pmod{2^{n+3}}$ και άρα έχουμε ολοκληρώσει την επαγωγή. ■

Άσκηση 8.2.7. Δείξτε ότι ο $2222^{5555} + 5555^{2222}$ είναι πολλαπλάσιο του 7.

Απόδειξη. Παρατηρούμε αρχικά ότι $2222 \equiv 3 \pmod{7}$ και $5555 \equiv 4 \pmod{7}$. Έχουμε ακόμα ότι

$$3^6 \equiv 729 \equiv 1 \pmod{7} \quad \text{και} \quad 4^3 \equiv 64 \equiv 1 \pmod{7}.$$

Άρα

$$\begin{aligned} 2222^{5555} + 5555^{2222} &\equiv 3^{5555} + 4^{2222} \pmod 7 \\ &\equiv 3^5 \cdot (3^6)^{925} + 4^2 \cdot (4^3)^{740} \pmod 7 \\ &\equiv 3^5 + 4^2 \pmod 7 \\ &\equiv 243 + 16 \pmod 7 \\ &\equiv 259 \pmod 7 \\ &\equiv 0 \pmod 7 \end{aligned}$$

Άρα όντως ο αριθμός $2222^{5555} + 5555^{2222}$ είναι πολλαπλάσιο του 7. ■

Κεφάλαιο 9

9η Παράδοση

Στο σημερινό μάθημα (και για τα επόμενα ένα ή δύο μαθήματα) συνεχίζουμε με την θεωρία των ισοτιμιών. Συνοπτικά, θα δούμε την έννοια της γραμμικής ισοτιμίας, θα αναφερθούμε στην γραμμική Διοφαντική εξίσωση με δύο αγνώστους την οποία και θα λύσουμε πλήρως και στο τέλος θα χρησιμοποιήσουμε όσα έχουμε δείξει για να λύσουμε πλήρως την γραμμική ισοτιμία (με έναν άγνωστο).

9.1 Γραμμικές Ισοτιμίες

Στο προηγούμενο μάθημα κάναμε μία πρώτη εισαγωγή στην έννοια της ισοτιμίας και είδαμε κάποια βασικά θεωρήματα που περιγράφουν τον λογισμό των ισοτιμιών, δηλαδή πώς τις χειριζόμαστε, σε ποιους κανόνες υπακούουν (και σε ποιους όχι) και κάποια πρώτα πράγματα που μπορούμε να κάνουμε με αυτές.

Συνεχίζοντας την ανάπτυξη της θεωρίας των ισοτιμιών, θα θέλαμε να μπορούμε να λύνουμε στοιχειώδεις «εξισώσεις» με ισοτιμίες και σ' αυτό το σημείο ακριβώς μπαίνει η έννοια της γραμμικής ισοτιμίας. Με τον όρο **γραμμική ισοτιμία** εννοούμε μια εξίσωση της μορφής

$$ax \equiv b \pmod{n}, \tag{9.1.1}$$

όπου n φυσικός και a, b ακέραιοι. Μας ενδιαφέρει να είμαστε σε θέση να λύσουμε πλήρως μια γραμμική ισοτιμία, που σημαίνει να μπορούμε να προσδιορίσουμε πότε έχει λύσεις και πότε όχι και, σε περίπτωση που έχει λύσεις, να μπορούμε να τις περιγράψουμε όλες. Ως λύση της (9.1.1) εννοούμε έναν ακέραιο x_0 που την ικανοποιεί, δηλαδή που είναι τέτοιος ώστε $ax_0 \equiv b \pmod{n}$.

Εξ ορισμού, έχουμε $ax_0 \equiv b \pmod{n}$, αν και μόνο αν $n \mid ax_0 - b$ ή ισοδύναμα, αν και μόνο αν $ax_0 - b = ny_0$ για κάποιον ακέραιο y_0. Βλέπουμε λοιπόν ότι για να λύσουμε την (9.1.1) αρκεί να λύσουμε την εξίσωση

$$ax + ny = b \tag{9.1.2}$$

ως προς τους ακεραίους x, y.

9.2 Η γραμμική Διοφαντική εξίσωση με 2 αγνώστους

Αλλάζοντας για λίγο κατεύθυνση (και, για λίγο μόνο, συμβολισμό), θα ασχοληθούμε πρώτα με την (9.1.2), την οποία θα λύσουμε πλήρως και μετά θα δούμε πώς μεταφράζονται οι λύσεις

που θα βρούμε σε λύσεις της (9.1.1). Η (9.1.2) είναι ένα παράδειγμα Διοφαντικής εξίσωσης. Θα έχουμε περισσότερα να πούμε για αυτού του είδους τις εξισώσεις λίγο αργότερα. Προς το παρόν αρκούμαστε στο να δώσουμε τις λύσεις μιας γραμμικής Διοφαντικής εξίσωσης με δύο αγνώστους.

Θεώρημα 9.2.1. *Η εξίσωση*

$$ax + by = c \tag{9.2.1}$$

έχει λύση αν και μόνο αν $d \mid c$, *όπου* $d = \gcd(a, b)$ *και* a, b *ακέραιοι όχι και οι δύο* 0. *Αν* x_0, y_0 *είναι μια συγκεκριμένη λύση της εξίσωσης, τότε όλες οι άλλες λύσεις δίνονται από τους τύπους*

$$x = x_0 + \left(\frac{b}{d}\right) t \qquad y = y_0 - \left(\frac{a}{d}\right) t,$$

όπου t *ακέραιος.*

Απόδειξη. Εξετάζουμε αρχικά την συνθήκη για την επιλυσιμότητα της (9.2.1). Εφ' όσον ο d είναι ο μέγιστος κοινός διαιρέτης των a, b, υπάρχουν ακέραιοι r, s τέτοιοι ώστε $a = dr$ και $b = ds$. Αν υπάρχει λύση της (9.2.1), έτσι ώστε $ax_0 + by_0 = c$ για κατάλληλους ακέραιους x_0, y_0, τότε

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$$

που συνεπάγεται ότι $d \mid c$.

Αντίστροφα, έστω ότι $d \mid c$ με $c = dt$. Τότε υπάρχουν ακέραιοι x_0 και y_0 τέτοιοι ώστε $d = ax_0 + by_0$. Η ύπαρξη αυτών των ακεραίων εξασφαλίζεται από το βασικό Θεώρημα 2.2.5. Έχουμε δηλαδή

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0).$$

Συμπεραίνουμε ότι η (9.2.1) έχει ως λύσεις τις $x = tx_0$ και $y = ty_0$.

Έστω τώρα ότι x_0, y_0 είναι συγκεκριμένη λύση της (9.2.1). Αν x', y' είναι οποιαδήποτε άλλη λύση, τότε

$$ax_0 + by_0 = ax' + by'$$

ή ισοδύναμα

$$a(x' - x_0) = b(y_0 - y'). \tag{9.2.2}$$

Από το Πόρισμα 2.2.9 υπάρχουν σχετικά πρώτοι ακέραιοι r, s τέτοιοι ώστε $a = dr$, $b = ds$. Αν αντικαταστήσουμε και διαγράψουμε τον d, παίρνουμε

$$r(x' - x_0) = s(y_0 - y').$$

Έχουμε επομένως ότι $r \mid s(y_0 - y')$ και $\gcd(r, s) = 1$. Από το Λήμμα του Ευκλείδη $r \mid (y_0 - y')$, δηλαδή $y_0 - y' = rt$ για κάποιον ακέραιο t. Αντικαθιστώντας στην (9.2.2), παίρνουμε

$$x' - x_0 = st.$$

Οδηγούμαστε λοιπόν στους τύπους

$$x' = x_0 + st = x_0 + \left(\frac{b}{d}\right) t$$
$$y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right) t.$$

Βλέπουμε εύκολα ότι ανεξάρτητα της τιμής του t, οι x', y' ικανοποιούν την (9.2.1), αφού

$$ax' + by' = a\left[x_0 + \left(\frac{b}{d}\right)t\right] + b\left[y_0 - \left(\frac{a}{d}\right)t\right] = (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t = c + 0 \cdot t = c.$$

Υπάρχει επομένως άπειρο πλήθος λύσεων και κάθε μία αντιστοιχεί σε μία τιμή του t. ■

Το επόμενο είναι άμεση συνέπεια του θεωρήματος που μόλις δείξαμε.

Πόρισμα 9.2.2. *Αν* $\gcd(a, b) = 1$ *και* x_0, y_0 *είναι συγκεκριμένη λύση της εξίσωσης* $ax + by = c$, *τότε οι λύσεις δίνονται από τους τύπους*

$$x = x_0 + bt \qquad y = y_0 - at$$

για t *ακέραιο.*

Ας δούμε τώρα με ένα παράδειγμα **πώς βρίσκουμε συγκεκριμένη λύση x_0, y_0** και πώς εφαρμόζουμε το Θεώρημα 9.2.1.

Παράδειγμα 9.2.3. Θα λύσουμε την Διοφαντική εξίσωση

$$172x + 20y = 1000. \tag{9.2.3}$$

Εφαρμόζουμε τον Ευκλείδειο Αλγόριθμο για να βρούμε τον $\gcd(172, 20)$:

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0. \end{aligned}$$

Άρα $\gcd(172, 20) = 4$ και αφού $4 \mid 1000$, η (9.2.3) έχει λύση. Για να γράψουμε τον ακέραιο 4 ως γραμμικό συνδυασμό των 172 και 20, δουλεύουμε προς τα πίσω στους παραπάνω υπολογισμούς, ως εξής:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2(172 - 8 \cdot 20) - 20 \\ &= 2 \cdot 172 + (-17)20. \end{aligned}$$

Πολλαπλασιάζουμε τώρα με $250 = 1000/4$ και παίρνουμε

$$\begin{aligned} 1000 = 250 \cdot 4 &= 250[2 \cdot 172 + (-17)20] \\ &= 500 \cdot 172 + (-4250)20. \end{aligned}$$

Άρα η $x_0 = 500$, $y_0 = -4250$ είναι μια συγκεκριμένη λύση της (9.2.3). Όλες οι άλλες λύσεις βρίσκονται από τους τύπους

$$\begin{aligned} x &= 500 + (20/4)t = 500 + 5t \\ y &= -4250 - (172/4)t = -4250 - 43t. \end{aligned}$$

9.3 Η πλήρης λύση μιας γραμμικής ισοτιμίας

Με αυτήν την προετοιμασία είμαστε σε θέση να επιστρέψουμε στο κυρίως θέμα μας που είναι οι γραμμικές ισοτιμίες. Δύο λύσεις της $ax \equiv b \pmod{n}$ θα τις θεωρούμε «ίδιες» αν είναι ισότιμες ως προς το μέτρο n, ακόμα κι αν δεν είναι ίδιες με την κανονική έννοια. Για παράδειγμα, οι $x = 3$ και $x = -9$ ικανοποιούν και οι δύο την $3x \equiv 9 \pmod{12}$. Επειδή όμως $3 \equiv -9 \pmod{12}$, δεν τις θεωρούμε διαφορετικές λύσεις. Εν ολίγοις, όταν αναφερόμαστε στο πλήθος των λύσεων της $ax \equiv b \pmod{n}$, εννοούμε τον αριθμό των ανισότιμων ακεραίων που ικανοποιούν την ισοτιμία.

Θεώρημα 9.3.1. *Η γραμμική ισοτιμία $ax \equiv b \pmod{n}$ έχει λύση αν και μόνο αν $d \mid b$, όπου $d = \gcd(a, n)$. Αν $d \mid b$, τότε η ισοτιμία έχει ακριβώς d ανά δύο ανισότιμες λύσεις $\bmod n$.*

Απόδειξη. Έχουμε ήδη εξηγήσει γιατί η ισοτιμία $ax \equiv b \pmod{n}$ είναι ισοδύναμη με την $ax - ny = b$. Από το Θεώρημα 9.2.1, ξέρουμε ότι η $ax - ny = b$ έχει λύση αν και μόνο αν $d \mid b$. Επιπλέον, αν είναι επιλύσιμη και x_0, y_0 είναι μια συγκεκριμένη λύση, τότε κάθε άλλη λύση έχει την μορφή

$$x = x_0 + \left(\frac{n}{d}\right) t \qquad y = y_0 + \left(\frac{a}{d}\right) t$$

για κάποια επιλογή του t.

Θεωρούμε τώρα τις διαδοχικές τιμές που παίρνει ο x για $t = 0, 1, 2, \ldots d - 1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d} \tag{9.3.1}$$

Ισχυριζόμαστε δύο πράγματα εδώ. Πρώτον ότι οι παραπάνω ακέραιοι είναι ανά δύο ανισότιμοι και δεύτερον ότι οποιοσδήποτε άλλος ακέραιος είναι ισότιμος με κάποιον από αυτούς. Αν συνέβαινε

$$x_0 + \frac{n}{d} t_1 \equiv x_0 + \frac{n}{d} t_2 \pmod{n}$$

όπου $0 \leqslant t_1 < t_2 \leqslant d - 1$, τότε θα είχαμε

$$\frac{n}{d} t_1 \equiv \frac{n}{d} t_2 \pmod{n}.$$

Όμως $\gcd(n/d, n) = n/d$, οπότε από το Θεώρημα 8.1.6 προκύπτει ότι

$$t_1 \equiv t_2 \pmod{d},$$

δηλαδή $d \mid t_2 - t_1$. Αυτό όμως είναι αδύνατο λόγω της $0 < t_2 - t_1 < d$. Μας μένει να δείξουμε ότι οποιαδήποτε άλλη λύση $x_0 + (n/d)t$ είναι ισότιμη $\bmod n$ με έναν από τους d ακέραιους στην λίστα (9.3.1). Ο Αλγόριθμος της Διαίρεσης μας επιτρέπει να γράψουμε $t = qd + r$, με $0 \leqslant r \leqslant d - 1$. Οπότε

$$\begin{aligned} x_0 + (n/d)t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d} r \\ &\equiv x_0 + \frac{n}{d} r \pmod{n}, \end{aligned}$$

όπου ο $x_0 + \frac{n}{d} r$ είναι ένας από τους d ακέραιους στην λίστα (9.3.1). ■

Βλέπουμε λοιπόν ότι αν x_0 είναι μία λύση της $ax \equiv b \pmod{n}$, τότε οι $d = \gcd(a, n)$ ανισότιμες ανά δύο λύσεις της ισοτιμίας δίνονται από τους

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\left(\frac{n}{d}\right), \ldots, x_0 + (d-1)\left(\frac{n}{d}\right).$$

Έχουμε ακόμα την εξής ειδική περίπτωση.

Πόρισμα 9.3.2. *Αν* $\gcd(a, n) = 1$, *τότε η γραμμική ισοτιμία* $ax \equiv b \pmod{n}$ *έχει μοναδική λύση* $\bmod n$.

Άρα αν οι a, n είναι σχετικά πρώτοι, η ισοτιμία $ax \equiv 1 \pmod{n}$ έχει μοναδική λύση. Αυτή η λύση καλείται ο **πολλαπλασιαστικός αντίστροφος** του $a \bmod n$.

Ας δούμε τώρα δύο παραδείγματα.

Παράδειγμα 9.3.3. Θεωρούμε την γραμμική ισοτιμία $18x \equiv 30 \pmod{42}$. Εφ' όσον $\gcd(18, 42) = 6$ και $6 \mid 30$, το Θεώρημα 9.3.1 εξασφαλίζει την ύπαρξη 6 ακριβώς λύσεων που είναι ανά δύο ανισότιμες ως προς το μέτρο 42.

Δοκιμάζοντας μερικές μικρές τιμές, βλέπουμε ότι μία λύση είναι η $x = 4$, επομένως οι λύσεις τις ισοτιμίας έχουν ως εξής:

$$x \equiv 4 + (42/6)t \equiv 4 + 7t \pmod{42} \qquad t = 0, 1, \ldots, 5.$$

Τις λύσεις μπορούμε να τις δώσουμε και πιο απλά ως

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}.$$

Παράδειγμα 9.3.4. Θεωρούμε την γραμμική ισοτιμία $9x \equiv 21 \pmod{30}$. Βλέπουμε αρχικά ότι $\gcd(9, 30) = 3$ και $3 \mid 21$, άρα υπάρχουν 3 ανισότιμες λύσεις.

Ένας τρόπος να προχωρήσουμε θα ήταν να απλοποιήσουμε κάθε όρο διαιρώντας με 3 και να πάρουμε την ισοδύναμη $3x \equiv 7 \pmod{10}$. Αφού λύσουμε αυτήν την τελευταία όμως (η οποία έχει μοναδική λύση), θα πρέπει να «μεταφράσουμε» την λύση σε λύσεις $\bmod 30$.

Η «κανονική» προσέγγιση λοιπόν είναι αυτή που υποδεικνύει και η απόδειξη του Θεωρήματος 9.3.1. Η ισοτιμία $9x \equiv 21 \pmod{30}$ είναι ισοδύναμη με την Διοφαντική εξίσωση

$$9x - 30y = 21.$$

Για να λύσουμε την τελευταία, γράφουμε τον $3 = \gcd(9, 30)$ ως γραμμικό συνδυασμό των 9, 30. Είτε με παρατήρηση είτε χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο, έχουμε ότι $3 = 9(-3) + 30 \cdot 1$, επομένως

$$21 = 7 \cdot 3 = 9(-21) - 30(-7).$$

Άρα οι $x = -21$, $y = -7$ ικανοποιούν την Διοφαντική εξίσωση, επομένως οι λύσεις της δίνονται από τον τύπο

$$x = -21 + (30/3)t = -21 + 10t.$$

Οι ακέραιοι $x = -21 + 10t$, όπου $t = 0, 1, 2$ είναι ανισότιμοι (ανά δύο) $\bmod 30$, οπότε παίρνουμε τις λύσεις

$$x \equiv -21 \pmod{30} \qquad x \equiv -11 \pmod{30} \qquad x \equiv -1 \pmod{30}$$

ή πιο απλά

$$x \equiv 9, 19, 29 \pmod{30}.$$

9.4 Ασκήσεις

Άσκηση 9.4.1. Για κάθε μία από τις παρακάτω Διοφαντικές εξισώσεις, βρείτε όλες τις λύσεις ή δείξτε ότι δεν έχει καμία ακέραια λύση.

(i) $2x + 5y = 11$

(ii) $17x + 13y = 100$

(iii) $21x + 14y = 147$

(iv) $60x + 18y = 97$

(v) $1402x + 1969y = 1$

Λύση. Για κάθε μία από τις εξισώσεις, εφαρμόζουμε το Θεώρημα 9.2.1.

(i) Έχουμε αρχικά ότι $\gcd(2, 5) = 1$ και $1 \mid 11$. Άρα η εξίσωση έχει λύσεις. Με απλή παρατήρηση ή χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο, έχουμε $2 \cdot (-2) + 5 \cdot 1 = 1$. Πολλαπλασιάζουμε με 11 αυτήν την ισότητα και παίρνουμε $2 \cdot (-22) + 5 \cdot 11 = 11$. Άρα η $(x_0, y_0) = (-22, 11)$ είναι μία συγκεκριμένη λύση. Το σύνολο των λύσεων επομένως δίνεται από τους τύπους $x = -22 + 5t$, $y = 11 - 2t$, όπου t ακέραιος.

(ii) Έχουμε αρχικά ότι $\gcd(17, 13) = 1$ και $1 \mid 100$. Άρα η εξίσωση έχει λύσεις. Με απλή παρατήρηση ή χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο, έχουμε $17 \cdot (-3) + 13 \cdot 4 = 1$. Πολλαπλασιάζουμε με 100 αυτήν την ισότητα και παίρνουμε $17 \cdot (-300) + 13 \cdot 400 = 100$. Άρα η $(x_0, y_0) = (-300, 400)$ είναι μία συγκεκριμένη λύση. Το σύνολο των λύσεων επομένως δίνεται από τους τύπους $x = -300 + 13t$, $y = 400 - 17t$, όπου t ακέραιος.

(iii) Έχουμε αρχικά ότι $\gcd(21, 14) = 7$ και $7 \mid 147$ με πηλίκο $147/7 = 21$. Με απλή παρατήρηση ή χρησιμοποιώντας τον Ευκλείδειο Αλγόριθμο, έχουμε $21 \cdot 1 + 14 \cdot (-1) = 7$. Πολλαπλασιάζουμε με $147/7 = 21$ αυτήν την ισότητα και παίρνουμε $21 \cdot 21 + 14 \cdot (-21) = 147$. Άρα η $(x_0, y_0) = (21, -21)$ είναι μία συγκεκριμένη λύση. Το σύνολο των λύσεων επομένως δίνεται από τους τύπους $x = 21 + 2t$, $y = -21 - 3t$, όπου t ακέραιος.

(iv) Παρατηρούμε ότι $\gcd(60, 18) = 6$, αλλά $6 \nmid 97$. Επομένως η εξίσωση δεν έχει λύσεις στους ακεραίους.

(v) Εφαρμόζουμε τον Ευκλείδειο Αλγόριθμο

$$\begin{aligned}
1969 &= 1 \cdot 1402 + 567 \\
1402 &= 2 \cdot 567 + 268 \\
567 &= 2 \cdot 268 + 31 \\
268 &= 8 \cdot 31 + 20 \\
31 &= 1 \cdot 20 + 11 \\
20 &= 1 \cdot 11 + 9 \\
11 &= 1 \cdot 9 + 2 \\
9 &= 4 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0\,.
\end{aligned}$$

Εφ' όσον $\gcd(1402, 1969) = 1 \mid 1$, η εξίσωση έχει λύσεις. Δουλεύοντας αντίστροφα στις παρα-

πάνω εξισώσεις, παίρνουμε

$$\begin{aligned}
1 &= 9 - 4 \cdot 2 \\
&= 9 - 4 \cdot (11 - 9) \\
&= 5 \cdot 9 - 4 \cdot 11 \\
&= 5(20 - 11) - 4 \cdot 11 \\
&= 5 \cdot 20 - 9 \cdot 11 \\
&= 5 \cdot 20 - 9(31 - 20) \\
&= 14 \cdot 20 - 9 \cdot 31 \\
&= 14(268 - 8 \cdot 31) - 9 \cdot 31 \\
&= 14 \cdot 268 - 121(567 - 2 \cdot 268) \\
&= 256 \cdot 268 - 121 \cdot 567 \\
&= 256(1402 - 2 \cdot 567) - 121 \cdot 567 \\
&= 256 \cdot 1402 - 633 \cdot 567 \\
&= 256 \cdot 1402 - 633(1969 - 1402) \\
&= 889 \cdot 1402 - 633 \cdot 1969\,.
\end{aligned}$$

Άρα η $(x_0, y_0) = (889, -633)$ είναι μία συγκεκριμένη λύση. Το σύνολο των λύσεων επομένως δίνεται από τους τύπους $x = 889 + 1969t$, $y = -633 - 1402t$, όπου t ακέραιος. ■

Άσκηση 9.4.2. Έστω a, b *φυσικοί* που είναι σχετικά πρώτοι. Να αποδειχθεί ότι η εξίσωση

$$ax + by = ab - a - b \tag{9.4.1}$$

δεν έχει λύσεις στους *φυσικούς*.

Απόδειξη. Εφ' όσον $1 \mid (ab - a - b)$, η εξίσωση έχει λύσεις στους *ακεραίους*. Μία συγκεκριμένη λύση της είναι η $(x_0, y_0) = (-1, a - 1)$. Άρα η γενική λύση της (9.4.1) στους ακεραίους δίνεται από τους τύπους $x = -1 + bt$, $y = a - 1 - at$.

Για να έχει επομένως λύσεις στους φυσικούς η εξίσωση, θα πρέπει να έχουμε $x = -1 + bt \geqslant 0$, δηλαδή $t \geqslant 1$ και ταυτόχρονα $y = a - 1 - at \geqslant 0$, δηλαδή $t \leqslant (a - 1)/a < 1$. Από αυτήν την αντίφαση προκύπτει ότι η (9.4.1) όντως δεν έχει λύσεις στους φυσικούς. ■

Άσκηση 9.4.3. Βρείτε τις λύσεις των ακόλουθων γραμμικών ισοτιμιών.

(i) $2x \equiv 5 \pmod 7$

(ii) $3x \equiv 6 \pmod 9$

(iii) $19x \equiv 30 \pmod{40}$

(iv) $9x \equiv 5 \pmod{25}$

Λύση. Για κάθε μία από τις ισοτιμίες, εφαρμόζουμε το Θεώρημα 9.3.1 ή το Πόρισμα 9.3.2.

(i) Εφ' όσον $\gcd(2, 7) = 1 \mid 5$, η ισοτιμία έχει μοναδική λύση. Παρατηρούμε εύκολα ότι $2 \cdot 6 \equiv 5 \pmod 7$, άρα η $x \equiv 6 \pmod 7$ είναι η μοναδική λύση της ισοτιμίας.

(ii) Εφ' όσον $\gcd(3,9) = 3 \mid 6$, η ισοτιμία έχει τρεις ανισότιμες λύσεις. Παρατηρούμε ότι $3 \cdot 5 \equiv 6 \pmod 9$, άρα μία λύση είναι η $x = 5$. Οι λύσεις της ισοτιμίας επομένως είναι οι $x \equiv 5 + (9/3)t \pmod 9$, όπου $t = 0, 1, 2$, δηλαδή οι $x \equiv 5, 8, 2 \pmod 9$.

(iii) Εφ' όσον $\gcd(19,40) = 1 \mid 30$, η ισοτιμία έχει μοναδική λύση. Λύνοντας την Διοφαντική εξίσωση $19x - 40y = 30$, παίρνουμε $x \equiv 10 \pmod{40}$.

(iv) Εφ' όσον $\gcd(9,25) = 1 \mid 5$, η ισοτιμία έχει μοναδική λύση. Λύνοντας την Διοφαντική εξίσωση $9x - 25y = 5$, παίρνουμε $x \equiv 20 \pmod{25}$. ■

Κεφάλαιο 10

10η Παράδοση

Στο σημερινό μάθημα θα αναφερθούμε σε συστήματα γραμμικών ισοτιμιών και θα δούμε το λεγόμενο «Κινέζικο Θεώρημα Υπολοίπων».

Έχοντας δει πώς λύνουμε μία γραμμική ισοτιμία (στην περίπτωση που έχει λύσεις), μας ενδιαφέρει τώρα να λύσουμε ένα σύστημα γραμμικών ισοτιμιών:

$$a_1x \equiv b_1 \pmod{m_1}, a_2x \equiv b_2 \pmod{m_2}, \ldots, a_rx \equiv b_r \pmod{m_r}.$$

Η υπόθεση εργασίας που θα κάνουμε είναι ότι $\gcd(m_i, m_j) = 1$ για $i \neq j$. Προφανώς για να έχει το σύστημα λύση (ή λύσεις), θα πρέπει κάθε μία ισοτιμία ξεχωριστά να λύνεται. Άρα μία απαραίτητη συνθήκη ύπαρξης λύσεων είναι να έχουμε $d_k \mid b_k$ για κάθε k τέτοιο ώστε $1 \leqslant k \leqslant r$, όπου $d_k = \gcd(a_k, m_k)$. Όταν αυτή η συνθήκη ικανοποιείται, μπορούμε να απλοποιήσουμε την kοστή ισοτιμία με d_k και να πάρουμε ένα σύστημα νέων εξισώσεων που έχει το ίδιο σύνολο λύσεων με το αρχικό:

$$a_1'x \equiv b_1' \pmod{n_1}, a_2'x \equiv b_2' \pmod{n_2}, \ldots, a_r'x \equiv b_r' \pmod{n_r},$$

όπου $n_k = m_k/d_k$ και $\gcd(n_i, n_j) = 1$ για $i \neq j$. Επιπλέον, $\gcd(a_i', n_i) = 1$. Αν $(a_i')^{-1}$ είναι ο πολλαπλασιαστικός αντίστροφος του $a_i' \bmod n_i$, τότε το σύστημα παίρνει την μορφή

$$x \equiv c_1 \pmod{n_1}, x \equiv c_2 \pmod{n_2}, \ldots, x \equiv c_r \pmod{n_r},$$

όπου $c_i = (a_i')^{-1}b_i'$ για $1 \leqslant i \leqslant r$. Βλέπουμε λοιπόν ότι αρκεί να λύσουμε αυτό το απλούστερο σύστημα αντί του αρχικού.

10.1 Το Κινέζικο Θεώρημα Υπολοίπων

Τέτοιου είδους προβλήματα έχουν μεγάλη ιστορία και απασχόλησαν τους Κινέζους μαθηματικούς ήδη από τον 1ο αι. μ.Χ. οπότε και εμφανίζονται στην κινέζικη βιβλιογραφία. Ένας εξ αυτών, ο Sun-Tsu ζήταγε να βρεθεί αριθμός που να αφήνει υπόλοιπα 2, 3, 2 όταν διαιρείται αντίστοιχα με τους 3, 5, 7. Προς τιμήν των σημαντικών αρχικών συνεισφορών τους, ο κανόνας σύμφωνα με τον οποίο λύνουμε ένα σύστημα γραμμικών ισοτιμιών ονομάζεται το Κινέζικο Θεώρημα Υπολοίπων.

Θεώρημα 10.1.1 (Το Κινέζικο Θεώρημα Υπολοίπων). *Έστω $n_1, n_2, \ldots, n_r$ φυσικοί που είναι ανά δύο πρώτοι. Τότε το σύστημα γραμμικών ισοτιμιών*

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ldots, x \equiv a_r \pmod{n_r}$$

έχει κοινή λύση η οποία είναι μοναδική ως προς το μέτρο $n_1 n_2 \cdots n_r$.

Απόδειξη. Θέτουμε $n = n_1 n_2 \cdots n_r$ και $N_k = \frac{n}{n_k}$ για κάθε k τέτοιο ώστε $1 \leqslant k \leqslant r$. Παρατηρούμε τώρα ότι $\gcd(N_k, n_k) = 1$ για $k \leqslant r$. (Αν κάποιος πρώτος p είναι κοινός διαιρέτης των N_k και n_k, τότε $p \mid n_i$ για κάποιο $i \neq k$ και άρα $p \mid 1 = \gcd(n_i, n_k)$ που είναι άτοπο.) Από το Πόρισμα 9.3.2 κάθε ισοτιμία $N_k x \equiv 1 \pmod{n_k}$ έχει μοναδική λύση την οποία καλούμε x_k. Θα δείξουμε ότι ο

$$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r$$

είναι κοινή λύση του συστήματος.

Παρατηρούμε αρχικά ότι $N_i \equiv 0 \pmod{n_k}$ για $i \neq k$, αφού $n_k \mid N_i$ σε αυτήν την περίπτωση. Άρα

$$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}.$$

Όμως διαλέξαμε τον x_k ως εκείνο τον ακέραιο που ικανοποιεί την $N_k x \equiv 1 \pmod{n_k}$, άρα

$$\overline{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}.$$

Προκύπτει ότι το σύστημα έχει όντως κοινή λύση.

Σε ό,τι αφορά την μοναδικότητα της λύσης, αν x' είναι ακέραιος που ικανοποιεί το σύστημα των ισοτιμιών, τότε

$$\overline{x} \equiv a_k \equiv x' \pmod{n_k}$$

για $k = 1, 2, \ldots, r$. Επομένως για κάθε τέτοια τιμή του k έχουμε ότι $n_k \mid \overline{x} - x'$. Εφ' όσον $\gcd(n_i, n_j) = 1$, το Πόρισμα 2.2.10 μας δίνει ότι $n_1 n_2 \cdots n_r \mid \overline{x} - x'$, δηλαδή $\overline{x} \equiv x' \pmod{n}$. Μ' αυτό έχουμε ολοκληρώσει την απόδειξη. ■

Ας δούμε τώρα μερικά παραδείγματα.

Παράδειγμα 10.1.2. Το πρόβλημα του Sun-Tsu μεταφράζεται στο ακόλουθο σύστημα γραμμικών ισοτιμιών

$$x \equiv 2 \pmod{3}, \qquad x \equiv 3 \pmod{5}, \qquad x \equiv 2 \pmod{7}.$$

Χρησιμοποιώντας τον συμβολισμό του Θεωρήματος 10.1.1, έχουμε $n = 3 \cdot 5 \cdot 7 = 105$ και

$$N_1 = \frac{n}{3} = 35, \qquad N_2 = \frac{n}{5} = 21, \qquad N_3 = \frac{n}{7} = 15.$$

Οι μοναδικές λύσεις των ισοτιμιών

$$35x \equiv 1 \pmod{3}, \qquad 21x \equiv 1 \pmod{5}, \qquad 15x \equiv 1 \pmod{7}$$

είναι οι $x_1 = 2$, $x_2 = 1$, $x_3 = 1$ αντίστοιχα. Η κοινή λύση του συστήματος επομένως είναι ο

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233,$$

δηλαδή $x = 233 \equiv 23 \pmod{105}$.

Παράδειγμα 10.1.3. Ως δεύτερο παράδειγμα εφαρμογής του Κινέζικου Θεωρήματος Υπολοίπων θα λύσουμε την γραμμική ισοτιμία

$$17x \equiv 9 \pmod{276}.$$

Έχουμε αρχικά ότι $276 = 3 \cdot 4 \cdot 23$, επομένως αρκεί να λύσουμε το σύστημα ισοτιμιών

$$17x \equiv 9 \pmod 3, \qquad 17x \equiv 9 \pmod 4, \qquad 17x \equiv 9 \pmod{23},$$

ή ισοδύναμα το

$$x \equiv 0 \pmod 3, \qquad x \equiv 1 \pmod 4, \qquad 17x \equiv 9 \pmod{23}.$$

Η τελευταία γράφεται ισοδύναμα (εφαρμόζοντας τον Ευκλείδειο Αλγόριθμο για παράδειγμα) ως $19 \cdot 17x \equiv 19 \cdot 9 \pmod{23}$, δηλαδή $x \equiv 10 \pmod{23}$. Μπορούμε τώρα να συνεχίσουμε όπως πριν, δηλαδή ακολουθώντας την διαδικασία που υποδεικνύει η απόδειξη του Θεωρήματος, αλλά μπορούμε να κάνουμε και κάτι λίγο απλούστερο.

Εφ' όσον $x \equiv 0 \pmod 3$, έχουμε $x = 3k$ για ακέραιο k. Αντικαθιστούμε στην δεύτερη ισοτιμία του συστήματος και παίρνουμε

$$3k \equiv 1 \pmod 4.$$

Πολλαπλασιάζοντας με 3 και τα δύο μέρη, παίρνουμε την

$$k \equiv 9k \equiv 3 \pmod 4$$

και άρα $k = 3 + 4j$, όπου j ακέραιος. Επομένως

$$x = 3(3 + 4j) = 9 + 12j.$$

Είδαμε πριν ότι η $17x \equiv 9 \pmod{23}$ είναι ισοδύναμη με την $x \equiv 10 \pmod{23}$. Αν αντικαταστήσουμε, παίρνουμε $12j \equiv 1 \pmod{23}$ και πολλαπλασιάζοντας με 2 την $j \equiv 2 \pmod{23}$. Άρα $j = 2 + 23t$, όπου t ακέραιος και τελικά

$$x = 9 + 12(2 + 23t) = 33 + 276t.$$

Βλέπουμε δηλαδή ότι η $x \equiv 33 \pmod{276}$ είναι η λύση του συστήματος γραμμικών ισοτιμιών και άρα και της ισοτιμίας $17x \equiv 9 \pmod{276}$.

10.2 Ασκήσεις

Άσκηση 10.2.1. Βρείτε το σύνολο των ακεραίων που αφήνουν υπόλοιπο 1 κατά την διαίρεσή τους και με τον 2 και με τον 3.

Λύση. Οι ακέραιοι που ψάχνουμε είναι αυτοί που ικανοποιούν το σύστημα των ισοτιμιών $x \equiv 1 \pmod 2$ και $x \equiv 1 \pmod 3$. Χρησιμοποιώντας τον συμβολισμό του Θεωρήματος 10.1.1, έχουμε να λύσουμε τις $3x \equiv 1 \pmod 2$ και $2x \equiv 1 \pmod 3$ οι οποίες έχουν λύσεις $x_1 = 1$ και $x_2 = 2$. Επομένως η λύση αυτού του συστήματος είναι η $\overline{x} = 1 \cdot 3 \cdot 1 + 1 \cdot 2 \cdot 2 = 7 \equiv 1 \pmod 6$, δηλαδή οι ακέραιοι της μορφής $6k + 1$.

Μπορούμε και πιο απλά να εργαστούμε με την μέθοδο που περιγράψαμε στο Παράδειγμα 10.1.3. Η ισοτιμία $x \equiv 1 \pmod 2$ μας επιτρέπει να γράψουμε $x = 2k + 1$ για ακέραιο k. Αντικαθιστούμε στην $x \equiv 1 \pmod 3$ και παίρνουμε $2k+1 \equiv 1 \pmod 3$, δηλαδή $2k \equiv 0 \pmod 3$. Πολλαπλασιάζοντας με 2 την τελευταία, έχουμε $k \equiv 0 \pmod 3$, δηλαδή $k = 3j$ για ακέραιο j. Επομένως $x = 2k + 1 = 2 \cdot (3j) + 1 = 6j + 1$ και καταλήγουμε στην ίδια λύση με αυτήν που βρήκαμε πριν. ■

Άσκηση 10.2.2. Βρείτε το σύνολο των ακεραίων που αφήνουν υπόλοιπο 1 κατά την διαίρεσή τους και με τον 2 και με τον 5 και είναι πολλαπλάσια του 3.

Λύση. Έχουμε να λύσουμε το σύστημα γραμμικών ισοτιμιών

$$x \equiv 1 \pmod 2, \qquad x \equiv 0 \pmod 3, \qquad x \equiv 1 \pmod 5.$$

Χρησιμοποιώντας τον συμβολισμό του Θεωρήματος 10.1.1, έχουμε $N_1 = 15$, $N_2 = 10$ και $N_3 = 6$. Πρέπει ακόμα να λύσουμε τις

$$15x \equiv 1 \pmod 2, \qquad 10x \equiv 1 \pmod 3, \qquad 6x \equiv 1 \pmod 5$$

οι οποίες έχουν όλες τις προφανείς λύσεις $x_1 = x_2 = x_3 = 1$. Άρα ο

$$\overline{x} = 1 \cdot 15 \cdot 1 + 0 \cdot 10 \cdot 1 + 1 \cdot 6 \cdot 1 = 21 \pmod{30}$$

είναι η λύση του συστήματος.

Εναλλακτικά, η ισοτιμία $x \equiv 1 \pmod 2$ μας επιτρέπει να γράψουμε $x = 2k + 1$ για ακέραιο k. Αντικαθιστούμε στην $x \equiv 0 \pmod 3$ και παίρνουμε $2k + 1 \equiv 0 \pmod 3$, δηλαδή $2k \equiv 2 \pmod 3$. Διαγράφοντας τον 2 (που είναι σχετικά πρώτος με τον 3), παίρνουμε $k \equiv 1 \pmod 3$, δηλαδή $k = 3j + 1$ για ακέραιο j. Επομένως $x = 2(3j + 1) + 1 = 6j + 3$. Άρα $6j + 3 \equiv 1 \pmod 5$, που είναι ισοδύναμη με την $j \equiv 3 \pmod 5$. Επομένως $j = 5t + 3$ για ακέραιο t, οπότε

$$x = 6j + 3 = 6(5t + 3) + 3 = 30t + 21,$$

όπως βρήκαμε και πριν. ■

Άσκηση 10.2.3. Έστω a, b, c ακέραιοι τέτοιοι ώστε $\gcd(a, b) = 1$. Δείξτε ότι υπάρχει ακέραιος x τέτοιος ώστε $\gcd(ax + b, c) = 1$.

Λύση. Αν κάθε πρώτος διαιρέτης του c διαιρεί τον b, τότε $\gcd(c, a) = 1$ άρα $\gcd(a + b, c) = 1$, οπότε μπορούμε να πάρουμε $x = 1$. Διαφορετικά, έστω x το γινόμενο όλων των πρώτων που διαιρούν τον c αλλά όχι τον b. Αν τώρα κάποιος πρώτος p διαιρεί τον c, τότε διαιρεί ακριβώς έναν εκ των ax και b. Επομένως ο p δεν διαιρεί τον $ax + b$, από το οποίο προκύπτει ότι $\gcd(ax + b, c) = 1$. ■

Άσκηση 10.2.4. Δείξτε ότι οι ισοτιμίες $x \equiv a \pmod n$ και $x \equiv b \pmod m$ έχουν κοινή λύση, αν και μόνο αν $\gcd(n, m) \mid a - b$. Δείξτε ακόμα ότι αν υπάρχει κοινή λύση, τότε είναι μοναδική ως προς το μέτρο $\operatorname{lcm}(n, m)$.

Απόδειξη. Υποθέτουμε αρχικά ότι οι δύο ισοτιμίες έχουν κοινή λύση τον x_0. Έστω $d = \gcd(n, m)$, οπότε $n = dr$ και $m = ds$ για κάποιους ακεραίους r, s. Από την σχέση $x_0 \equiv a \pmod n$ παίρνουμε ότι $x_0 = a + nt$ για κάποιον ακέραιο t. Ομοίως, η σχέση $x_0 \equiv b \pmod m$ μας δίνει την $x_0 = b + mk$ για κάποιον ακέραιο k. Έχουμε λοιπόν ότι $a + nt = b + mk$, δηλαδή $nt - mk = b - a$. Άρα $drt - dsk = b - a$ ή $d(sk - rt) = a - b$ και βλέπουμε ότι $d \mid a - b$.

Έστω τώρα ότι $d \mid a - b$, δηλαδή $dt = a - b$ για κάποιον ακέραιο t. Από το Θεώρημα 2.2.5 υπάρχουν ακέραιοι x_0, y_0 τέτοιοι ώστε $nx_0 + my_0 = d$. Άρα $dt = nx_0t + my_0t = a - b$. Επομένως $my_0t + b = a - x_0tn$. Θέτοντας $x = a + (-x_0t)n = b + (y_0t)m$, βλέπουμε ότι $x \equiv a \pmod n$ και $x \equiv b \pmod m$. Δηλαδή υπάρχει κοινή λύση.

Αν τώρα $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$ και $y \equiv a \pmod{n}$, $y \equiv b \pmod{m}$, τότε $x \equiv y \pmod{n}$ και $x \equiv y \pmod{n}$. Από την Άσκηση 3.3.1 προκύπτει ότι $x \equiv y \pmod{\operatorname{lcm}(n, m)}$, όπως θέλαμε να δείξουμε. ■

Κεφάλαιο 11

11η Παράδοση

Στο σημερινό μάθημα θα αναφερθούμε σε ένα επώνυμο θεώρημα που αφορά σε ισοτιμίες και έχει σχέση με πρώτους. Είναι γνωστό ως «το μικρό Θεώρημα του Fermat». Θα μιλήσουμε ακόμα για *ψευδοπρώτους* και *απόλυτους ψευδοπρώτους*.

11.1 Το μικρό Θεώρημα του Fermat

Ο Pierre de Fermat (1607 – 1665) ήταν Γάλλος νομικός και ερασιτέχνης μαθηματικός του 17ου αι. με σημαντικές συνεισφορές σε διάφορους τομείς των μαθηματικών. Στην Θεωρία Αριθμών συγκεκριμένα, είναι γνωστός για την μέθοδο της Άπειρης Καθόδου (στην οποία ίσως αναφερθούμε αργότερα) και τους πρώτους του Fermat τους οποίους συναντήσαμε στην Άσκηση 4.3.6. Περισσότερο γνωστός είναι μάλλον για το διαβόητο Τελευταίο Θεώρημά του, στο οποίο θα αναφερθούμε αργότερα στα μαθήματα για τις Διοφαντικές Εξισώσεις. Σε αντίθεση με το Τελευταίο (ή Μεγάλο) Θεώρημά του, για το θεώρημα που θα παρουσιάσουμε εδώ δεν έχουμε ιδιαίτερες αμφιβολίες ότι είχε βρει όντως απόδειξη. Πάντως η πρώτη δημοσιευμένη απόδειξη του θεωρήματος που ακολουθεί, δόθηκε από τον Euler το 1736.

Θεώρημα 11.1.1 (Το μικρό Θεώρημα του Fermat). *Αν ο p είναι πρώτος και ο a ακέραιος τέτοιος ώστε $p \nmid a$, τότε $a^{p-1} \equiv 1 \pmod{p}$.*

Απόδειξη. Θεωρούμε τα πρώτα $p-1$ θετικά πολλαπλάσια του ακεραίου a, δηλαδή τους

$$a, 2a, 3a, \ldots, (p-1)a.$$

Οι αριθμοί αυτοί είναι ανά δύο ανισότιμοι ως προς το μέτρο p, ενώ κανένας δεν είναι ίσος με $0 \bmod p$. Πράγματι, αν $ra \equiv sa \pmod{p}$, όπου $1 \leqslant r < s \leqslant p-1$, τότε (από το Πόρισμα 8.1.8 για παράδειγμα) μπορούμε να απλοποιήσουμε τον a παίρνοντας $r \equiv s \pmod{p}$, που είναι αδύνατο. Επομένως οι ακέραιοι $a, 2a, 3a, \ldots, (p-1)a$ είναι ισότιμοι ως προς το μέτρο p με τους $1, 2, 3, \ldots, p-1$ σε κάποια σειρά. Πολλαπλασιάζοντας τις ισοτιμίες, βρίσκουμε ότι

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

δηλαδή

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Κάθε παράγοντας στο γινόμενο που ορίζει τον $(p-1)!$ είναι σχετικά πρώτος με τον p και άρα ο p είναι σχετικά πρώτος με τον $(p-1)!$. Προκύπτει λοιπόν ότι μπορούμε να απλοποιήσουμε

τον $(p-1)!$ στην ανωτέρω ισοτιμία και να πάρουμε

$$a^{p-1} \equiv 1 \pmod{p},$$

που είναι ο ισχυρισμός του θεωρήματος. ■

Έχουμε τώρα την εξής ήπια γενίκευση του παραπάνω αποτελέσματος.

Πόρισμα 11.1.2. *Αν ο p είναι πρώτος, τότε $a^p \equiv a \pmod{p}$ για κάθε ακέραιο a.*

Απόδειξη. Όταν ο p διαιρεί τον a, τότε ο ισχυρισμός ισχύει, αφού $a^p \equiv 0 \equiv a \pmod{p}$. Αν $p \nmid a$, τότε σύμφωνα με το Θεώρημα 11.1.1, έχουμε $a^{p-1} \equiv 1 \pmod{p}$. Πολλαπλασιάζοντας με a παίρνουμε $a^p \equiv a \pmod{p}$ και έχουμε δείξει το ζητούμενο. ■

Η χρησιμότητα του Θεωρήματος 11.1.1 (ή του Πορίσματος 11.1.2) είναι μεγάλη. Αν μη τι άλλο, συντομεύει διάφορους υπολογισμούς. Αν θέλουμε για παράδειγμα να επαληθεύσουμε ότι $5^{38} \equiv 4 \pmod{11}$, τότε ξεκινάμε με την ισοτιμία $5^{10} \equiv 1 \pmod{11}$ και συνεχίζουμε ως εξής:

$$5^{38} = 5^{10\cdot 3+8} = (5^{10})^3(5^2)^4 \equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}.$$

Μπορούμε επίσης να χρησιμοποιήσουμε το μικρό Θεώρημα του Fermat για να ελέγξουμε αν ένας αριθμός είναι πρώτος ή όχι. Αυτό διότι αν για κάποιον φυσικό n και κάποια επιλογή ακεραίου a η ισοτιμία

$$a^n \equiv a \pmod{n}$$

δεν ισχύει, τότε ο n είναι σίγουρα *σύνθετος*. Ας ελέγξουμε, για παράδειγμα, αν ο 117 είναι πρώτος ή σύνθετος. Διαχειριζόμαστε την πολυπλοκότητα των υπολογισμών διαλέγοντας έναν μικρό ακέραιο, για παράδειγμα τον $a = 2$. Έπειτα γράφουμε τον 2^{117} ως

$$2^{117} = 2^{7\cdot 16+5} = (2^7)^{16}2^5,$$

ενώ παράλληλα έχουμε $2^7 = 128 \equiv 11 \pmod{117}$. Προκύπτει λοιπόν ότι

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}.$$

Έχουμε όμως ότι $2^{21} = (2^7)^3$, άρα

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}.$$

Τελικά

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117},$$

άρα ο 117 είναι σίγουρα σύνθετος.

11.2 Ψευδοπρώτοι και απόλυτοι ψευδοπρώτοι

Αξίζει να αναφέρουμε ότι το αντίστροφο του Θεωρήματος 11.1.1 **δεν** ισχύει. Δηλαδή, αν $a^{n-1} \equiv 1 \pmod{n}$ για κάποιον ακέραιο a, τότε δεν προκύπτει ότι ο n είναι πρώτος. Δείχνουμε πρώτα το εξής.

Λήμμα 11.2.1. *Αν οι p, q είναι διακεκριμένοι πρώτοι τέτοιοι ώστε $a^p \equiv a \pmod{q}$ και $a^q \equiv a \pmod{p}$ για κάποιον ακέραιο a, τότε $a^{pq} \equiv a \pmod{pq}$.*

Απόδειξη. Από το Πόρισμα 11.1.2 έχουμε ότι $(a^q)^p \equiv a^q \pmod{p}$, ενώ η $a^q \equiv a \pmod{p}$ ισχύει εξ υποθέσεως. Άρα $a^{pq} \equiv a \pmod{p}$, ήτοι $p \mid a^{pq} - a$. Εντελώς παρόμοια βρίσκουμε ότι $q \mid a^{pq} - a$. Από το Πόρισμα 2.2.10 έχουμε ότι $pq \mid a^{pq} - a$, δηλαδή $a^{pq} \equiv a \pmod{pq}$, όπως θέλαμε να δείξουμε. ■

Ισχυριζόμαστε τώρα ότι $2^{340} \equiv 1 \pmod{341}$, όπου $341 = 11 \cdot 31$. Γράφουμε $2^{10} = 1024 = 31 \cdot 33 + 1$ και έχουμε

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$$

και

$$2^{31} = 2(2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}.$$

Χρησιμοποιώντας το Λήμμα 11.2.1 παίρνουμε ότι

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31},$$

δηλαδή $2^{341} \equiv 2 \pmod{341}$. Απλοποιώντας τον παράγοντα 2, καταλήγουμε ότι

$$2^{340} \equiv 1 \pmod{341},$$

όπως ισχυριστήκαμε.

Το ενδιαφέρον για αριθμούς της μορφής $2^n - 2$ έχει τις ρίζες του στην αρχαία Κίνα και σε ισχυρισμούς των μαθηματικών εκείνης της εποχής ότι ο n είναι πρώτος, αν και μόνο αν $n \mid 2^n - 2$. Φυσικά αυτό δεν ισχύει για $n = 341$, όπως δείξαμε παραπάνω (το παράδειγμα αυτό βρέθηκε το 1819). Προσέξτε όμως ότι ο ισχυρισμός είναι αληθής για $n \leqslant 340$. Το σενάριο αυτό (δηλαδή κάποιος σύνθετος n να διαιρεί τον $2^n - 2$) συμβαίνει αρκετά σπάνια για να χρήζει ξεχωριστής ονομασίας.

Ορισμός 11.2.2. Ένας σύνθετος φυσικός n καλείται **ψευδοπρώτος** αν $n \mid 2^n - 2$.

Μπορούμε να δείξουμε ότι υπάρχουν άπειροι ψευδοπρώτοι, οι μικρότεροι τέσσερις εκ των οποίων είναι οι 341, 561, 645, 1105.

Θεώρημα 11.2.3. *Αν ο n είναι ένας περιττός ψευδοπρώτος, τότε ο $M_n = 2^n - 1$ είναι ένας ακόμα μεγαλύτερος ψευδοπρώτος.*

Απόδειξη. Εφ' όσον ο n είναι σύνθετος, μπορούμε να γράψουμε $n = rs$, με $1 < r \leqslant s < n$. Έχουμε τώρα ότι

$$M_n = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \ldots + 2^r + 1),$$

άρα $2^r - 1 \mid M_n$. Οπότε ο M_n είναι σύνθετος, ενώ εξ υποθέσεως έχουμε $2^n \equiv 2 \pmod{n}$. Προκύπτει λοιπόν ότι $2^n - 2 = kn$ για κάποιον φυσικό k. Συνεπώς

$$2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}.$$

Συμπεραίνουμε λοιπόν ότι

$$\begin{aligned} 2^{M_n - 1} &= 2^{kn} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \ldots + 2^n + 1) \\ &= M_n(2^{n(k-1)} + 2^{n(k-2)} + \ldots + 2^n + 1) \\ &\equiv 0 \pmod{M_n}. \end{aligned}$$

Προκύπτει άμεσα ότι $2^{M_n} - 2 \equiv 0 \pmod{M_n}$ και άρα ο M_n είναι όντως ψευδοπρώτος. ■

Πιο γενικά, ένας σύνθετος φυσικός n ο οποίος ικανοποιεί την ισοτιμία $a^n \equiv a \pmod{n}$ λέγεται **ψευδοπρώτος ως προς την βάση *a***. Σε περίπτωση που $a = 2$, τότε καλείται απλά ψευδοπρώτος. Για παράδειγμα, ο 91 είναι ο μικρότερος ψευδοπρώτος ως προς την βάση 3, ενώ ο 215 είναι ο μικρότερος ψευδοπρώτος ως προς την βάση 5. Έχει αποδειχθεί (1913) ότι υπάρχουν άπειροι ψευδοπρώτοι ως προς οποιαδήποτε βάση.

Αυτοί οι μασκαράδες αριθμοί που ντύνονται ως πρώτοι είναι στην πραγματικότητα πολύ σπανιότεροι των πραγματικών πρώτων. Υπάρχουν μόλις 247 ψευδοπρώτοι μικρότεροι ή ίσοι του 10^6, ενώ υπάρχουν 78498 πρώτοι $\leqslant 10^6$. Το πρώτο παράδειγμα δε άρτιου ψευδοπρώτου, δηλαδή ο αριθμός

$$161038 = 2 \cdot 73 \cdot 1103,$$

βρέθηκε το 1950.

Αυτό που είναι μάλλον αναπάντεχο σε σχέση με όσα έχουμε αναφέρει μέχρι τώρα, είναι το γεγονός ότι υπάρχουν σύνθετοι φυσικοί οι οποίοι είναι ψευδοπρώτοι ως προς οποιαδήποτε βάση. Ο μικρότερος τέτοιος αριθμός είναι ο 561. Αυτοί οι ξεχωριστοί αριθμοί καλούνται **απόλυτοι ψευδοπρώτοι** ή **αριθμοί Carmichael** προς τιμήν του R. D. Carmichael που πρώτος ανακάλυψε την ύπαρξή τους. Στο πρώτο του άρθρο για αυτό το θέμα το 1910, ο Carmichael υπέδειξε τέσσερις απόλυτους ψευδοπρώτους, συμπεριλαμβανομένου του 561 που αναφέραμε παραπάνω. Οι υπόλοιποι είναι οι

$$1105 = 5 \cdot 13 \cdot 17 \qquad 2821 = 7 \cdot 13 \cdot 31 \qquad 15841 = 7 \cdot 31 \cdot 73.$$

Δύο χρόνια αργότερα παρουσίασε 11 ακόμα τέτοιους αριθμούς με τρεις πρώτους παράγοντες, ενώ ανακάλυψε και έναν με τέσσερις πρώτους παράγοντες· συγκεκριμένα, τον

$$16046641 = 13 \cdot 37 \cdot 73 \cdot 457.$$

Ας δούμε λίγο τώρα γιατί ο $561 = 3 \cdot 11 \cdot 17$ είναι απόλυτος ψευδοπρώτος. Προσέξτε ότι αν $\gcd(a, 561) = 1$, τότε

$$\gcd(a, 3) = \gcd(a, 11) = \gcd(a, 17) = 1.$$

Εφαρμόζοντας το Θεώρημα 11.1.1 παίρνουμε

$$a^2 \equiv 1 \pmod{3} \qquad a^{10} \equiv 1 \pmod{11} \qquad a^{16} \equiv 1 \pmod{17}$$

και άρα

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

Από τις παραπάνω ισοτιμίες προκύπτει τώρα η ενιαία $a^{560} \equiv 1 \pmod{561}$ για a σχετικά πρώτο με τον 561.

Θα έχετε παρατηρήσει ίσως ότι στα παραδείγματα απόλυτων ψευδοπρώτων που έχουμε δει μέχρι τώρα, όλοι οι αριθμοί έχουν μια κοινή ιδιότητα. Κανένας τους δεν διαιρείται από το τετράγωνο ενός πρώτου. Σε αυτούς τους αριθμούς δίνουμε ένα ξεχωριστό όνομα.

Ορισμός 11.2.4. Αν ένας ακέραιος a έχει την ιδιότητα ότι το μόνο τέλειο τετράγωνο που τον διαιρεί είναι ο 1, τότε ο a καλείται **ελεύθερος τετραγώνων**. Ισοδύναμα, κάθε πρώτος που διαιρεί τον a, εμφανίζεται μόνο μία φορά στην ανάλυση τού a σε πρώτους.

Το 1912 ο Carmichael είκασε ότι υπάρχουν άπειροι αριθμοί Carmichael. Χρειάστηκαν 80 χρόνια για να απαντηθεί αυτή η εικασία. Το 1992 οι Alford, Granville και Pomerance έδειξαν ότι ο Carmichael είχε δίκιο. Δεν είμαστε σε θέση να δούμε την απόδειξη που έδωσαν, μπορούμε όμως να δούμε στο επόμενο θεώρημα έναν τρόπο να βρίσκουμε αριθμούς Carmichael.

Θεώρημα 11.2.5. *Έστω n ένας φυσικός που είναι σύνθετος και ελεύθερος τετραγώνων. Αν για κάθε πρώτο p που διαιρεί τον n, έχουμε ότι $p-1 \mid n-1$, τότε ο n είναι αριθμός Carmichael.*

Απόδειξη. Εξ υποθέσεως έχουμε $n = p_1 p_2 \cdots p_r$, όπου $r \geqslant 2$ και οι p_i είναι διακεκριμένοι πρώτοι. Αν τώρα a είναι ακέραιος σχετικά πρώτος με τον n, τότε $\gcd(a, p_i) = 1$ για $i = 1, 2, \ldots, r$, επομένως το μικρό Θεώρημα του Fermat μας δίνει $a^{p_i - 1} \equiv 1 \pmod{p_i}$. Εφ' όσον $p_i - 1 \mid n - 1$, έπεται ότι υπάρχουν φυσικοί t_i τέτοιοι ώστε $n - 1 = t_i(p_i - 1)$ για $i = 1, 2, \ldots, r$. Συνεπώς, για κάθε τέτοιον i, έχουμε ότι $a^{n-1} = a^{t_i(p_i-1)} \equiv 1 \pmod{p_i}$. Χρησιμοποιώντας είτε το Θεώρημα 10.1.1 είτε το Πόρισμα 2.2.10, παίρνουμε ότι $a^{n-1} \equiv 1 \pmod{n}$, άρα ο n είναι όντως αριθμός Carmichael. ■

11.3 Ασκήσεις

Άσκηση 11.3.1. Να δειχθεί ότι $17 \mid 11^{104} + 1$.

Απόδειξη. Οι 11 και 17 είναι σχετικά πρώτοι. Το Θεώρημα 11.1.1 μας δίνει $11^{16} \equiv 1 \pmod{17}$. Επομένως $11^{96} = (11^{16})^6 \equiv 1 \pmod{17}$. Επίσης $11^2 = 121 \equiv 2 \pmod{17}$, άρα $11^8 \equiv 2^4 \equiv 16 \equiv -1 \pmod{17}$. Συνεπώς $11^{104} = 11^{96} \cdot 11^8 \equiv 1 \cdot (-1) \equiv -1 \pmod{17}$. Προκύπτει λοιπόν ότι $17 \mid 11^{104} + 1$, όπως θέλαμε να δείξουμε. ■

Άσκηση 11.3.2. Να δειχθεί ότι αν $\gcd(a, 35) = 1$, τότε $a^{12} \equiv 1 \pmod{35}$.

Απόδειξη. Εφ' όσον $\gcd(a, 35) = 1$, έχουμε $\gcd(a, 5) = 1$ και $\gcd(a, 7) = 1$. Από το μικρό Θεώρημα του Fermat έχουμε $a^6 \equiv 1 \pmod{7}$ άρα και $a^{12} \equiv 1 \pmod{7}$. Επίσης, $a^4 \equiv 1 \pmod{5}$ που συνεπάγεται ότι $a^{12} \equiv 1 \pmod{5}$. Από το Πόρισμα 2.2.10 (ή το το Θεώρημα 10.1.1), παίρνουμε ότι $a^{12} \equiv 1 \pmod{35}$. ■

Άσκηση 11.3.3. Να δείξετε ότι αν ο p είναι περιττός πρώτος, τότε

(i) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod{p}$,

(ii) $1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$.

Απόδειξη. (i) Εφ' όσον $\gcd(a, p) = 1$ για κάθε φυσικό $a < p$, το μικρό Θεώρημα του Fermat μας δίνει $a^{p-1} \equiv 1 \pmod{p}$ για όλους αυτούς τους a. Άρα

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv \underbrace{1 + 1 + 1 + \ldots + 1}_{p-1} \equiv p - 1 \equiv -1 \pmod{p}.$$

Προσέξτε ότι η συγκεκριμένη σχέση ισχύει και για $p = 2$.

(ii) Από το Πόρισμα 11.1.2 έχουμε ότι για κάθε ακέραιο a, $a^p \equiv a \pmod{p}$. Προκύπτει λοιπόν ότι

$$1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 1 + 2 + 3 + \ldots + p - 1 \equiv p \cdot \left(\frac{p-1}{2}\right) \equiv 0 \pmod{p}.$$

Η τελευταία ισοτιμία είναι συνέπεια του ότι ο p είναι περιττός και άρα ο $\frac{p-1}{2}$ ακέραιος. ■

Άσκηση 11.3.4. Να δείξετε ότι καθένας από τους παρακάτω αριθμούς είναι απόλυτος ψευδοπρώτος:

(i) $1105 = 5 \cdot 13 \cdot 17$,

(ii) $2821 = 7 \cdot 13 \cdot 31$,

(iii) $2465 = 5 \cdot 17 \cdot 29$.

Απόδειξη. Για όλους τους αριθμούς, χρησιμοποιούμε το Θεώρημα 11.2.5.

(i) Ο 1105 είναι σύνθετος και ελεύθερος τετραγώνων. Ακόμα $5-1 = 4 \mid 1104$, $13-1 = 12 \mid 1104$ και $17 - 1 = 16 \mid 1104$.

(ii) Ο 2821 είναι σύνθετος και ελεύθερος τετραγώνων. Επίσης $7-1 = 6 \mid 2820$, $13-1 = 12 \mid 2820$ και $31 - 1 = 30 \mid 2820$.

(ii) Ο 2821 είναι σύνθετος και ελεύθερος τετραγώνων. Επιπλέον $5 - 1 = 4 \mid 2464$, $17 - 1 = 16 \mid 2464$ και $29 - 1 = 28 \mid 2464$. ■

Άσκηση 11.3.5. Να δειχθεί ότι ένας φυσικός της μορφής

$$n = (6k+1)(12k+1)(18k+1)$$

όπου k φυσικός, είναι απόλυτος ψευδοπρώτος αν συμβεί και οι τρεις παράγοντές του να είναι πρώτοι. Επομένως ο $1729 = 7 \cdot 13 \cdot 19$, για παράδειγμα, είναι αριθμός Carmichael.

Απόδειξη. Έστω ότι οι $p_1 = 6k+1$, $p_2 = 12k+1$, $p_3 = 18k+1$ είναι και οι τρεις πρώτοι. Για τον $n-1$ έχουμε ότι

$$n - 1 = (6k+1)(216k^2 + 30k + 1) - 1 = 1296k^3 + 396k^2 + 36k = 36k(36k^2 + 11k + 1).$$

Βλέπουμε λοιπόν ότι $p_1 - 1 = 6k \mid n-1$, $p_2 - 1 = 12k \mid n-1$ και $p_1 - 1 = 18k \mid n-1$. Επίσης, ο $n = p_1p_2p_3$ είναι σύνθετος και ελεύθερος τετραγώνων, άρα όλες οι συνθήκες του Θεωρήματος 11.2.5 ικανοποιούνται. Συνεπώς ο n είναι αριθμός Carmichael. ■

Άσκηση 11.3.6. (∗) Να δειχθεί ότι ένας αριθμός Carmichael είναι αναγκαστικά ελεύθερος τετραγώνων.

Απόδειξη. Έστω n ένας αριθμός Carmichael. Έστω ακόμα ότι υπάρχει p πρώτος που είναι τέτοιος ώστε $n = p^t m$, όπου $\gcd(p, m) = 1$ και $t \geqslant 2$. Δηλαδή, $t = v_p(n)$. Αν $x = b$ είναι λύση του συστήματος ισοτιμιών $x \equiv p^{t-1} + 1 \pmod{p^t}$ και $x \equiv 1 \pmod{m}$, τότε $\gcd(b, p) = 1$ και $\gcd(b, m) = 1$, οπότε $\gcd(b, n) = 1$. Αν ίσχυε ότι $b \equiv 1 \pmod{n}$, τότε θα ίσχυε επίσης ότι $b \equiv 1 \pmod{p^t}$, που είναι άτοπο. Άρα $b \not\equiv 1 \pmod{n}$.

Από την άλλη, έχουμε ότι

$$b^n \equiv (p^{t-1}+1)^n \equiv (p^{t-1})^n + n(p^{t-1})^{n-1} + \ldots + np^{t-1} + 1 \equiv 1 \pmod{p^t},$$

όπου χρησιμοποιούμε το Διωνυμικό Ανάπτυγμα και το γεγονός ότι ο p διαιρεί τον n (άρα ο p^t διαιρεί κάθε όρο εκτός του τελευταίου). Επίσης, $b^n \equiv 1 \pmod{m}$, άρα από το Κινέζικο Θεώρημα Υπολοίπων (ή εναλλακτικά από το Πόρισμα 4.1.3) έχουμε ότι $b^n \equiv 1 \pmod{n}$. Εφ' όσον τώρα $\gcd(b,n) = 1$ και $b \not\equiv 1 \equiv b^n \pmod{n}$, προκύπτει ότι ο n δεν είναι αριθμός Carmichael, κάτι που είναι άτοπο. Καταλήγουμε ότι ο n είναι ελεύθερος τετραγώνων, όπως θέλαμε να δείξουμε. ■

Κεφάλαιο 12

12η Παράδοση

Είδαμε στο προηγούμενο μάθημα το μικρό Θεώρημα του Fermat. Στο σημερινό θα αναφερθούμε σε ένα άλλο θεώρημα που είναι και αυτό μέρος ενός τρίπτυχου θεωρημάτων τα οποία θεωρούνται ορόσημα της στοιχειώδους Θεωρίας Αριθμών. Είναι γνωστό ως το Θεώρημα του Wilson. Το τρίτο και τελευταίο θεώρημα αυτού του τρίπτυχου, που είναι το Θεώρημα του Euler και γενικεύει το Θεώρημα του Fermat, θα το δούμε λίγο αργότερα.

12.1 Το Θεώρημα του Wilson

Στο βιβλίο του Meditationes Algebricae που εξέδωσε το 1770, ο Άγγλος μαθηματικός Edward Waring (1734−1798) ανακοίνωσε αρκετά νέα θεωρήματα. Μεταξύ αυτών και μία ενδιαφέρουσα ιδιότητα των πρώτων την οποία του είχε μεταφέρει ένας μαθητής του ονόματι John Wilson.

Η ιδιότητα έχει ως εξής: αν ο p είναι πρώτος, τότε ο p διαιρεί τον $(p-1)!+1$. Ο Wilson μάλλον το είχε μαντέψει αυτό βάσει αριθμητικών υπολογισμών, πάντως το σίγουρο είναι ότι ούτε αυτός ούτε ο Waring μπορούσαν να το αποδείξουν. Λίγο αργότερα, το 1771, ο Joseph Lagrange το απέδειξε, ενώ παρατήρησε ότι ισχύει επίσης και το αντίστροφο: αν $p \mid (p-1)!+1$, τότε ο p είναι πρώτος. Το δίκαιο μάλλον θα ήταν να είχαμε δώσει στο θεώρημα το όνομα του Leibniz, αφού υπάρχουν ενδείξεις ότι γνώριζε το θεώρημα έναν αιώνα περίπου πριν.

Πριν ξεκινήσουμε την απόδειξη, θα δούμε με ένα παράδειγμα την κεντρική ιδέα. Υπενθυμίζουμε το εξής βασικό από το 9ο μάθημα (Πόρισμα 9.3.2):

Αν οι a, n είναι σχετικά πρώτοι, η ισοτιμία $ax \equiv 1 \pmod{n}$ έχει μοναδική λύση. Αυτή η λύση καλείται ο **πολλαπλασιαστικός αντίστροφος** του $a \bmod n$.

Έστω τώρα $p = 7$. Έχουμε $(7-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$. Αναδιατάσσουμε τους όρους του γινομένου σχηματίζοντας ζευγάρια πολλαπλασιαστικών αντιστρόφων. Συγκεκριμένα, έχουμε $2 \cdot 4 \equiv 1 \pmod{7}$ και $3 \cdot 5 \equiv 1 \pmod{7}$. Επομένως

$$6! \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 6 \equiv -1 \pmod{7}$$

Οι μοναδικοί αριθμοί που δεν σχηματίζουν ζευγάρι είναι ο 1 και ο $p-1 = 6$. Αυτό συμβαίνει γιατί ο πολλαπλασιαστικός αντίστροφος του 1 είναι ο εαυτός του, ενώ το ίδιο συμβαίνει και με τον $p-1 = 6$.

Θεώρημα 12.1.1 (Το Θεώρημα του Wilson). *Αν ο p είναι πρώτος, τότε* $(p-1)! \equiv -1 \pmod{p}$.

Απόδειξη. Αν $p = 2$, τότε $(p-1)! \equiv 1 \equiv -1 \pmod 2$. Ομοίως, αν $p = 3$, τότε $(p-1)! \equiv 2 \equiv -1 \pmod 3$. Επομένως το ζητούμενο ισχύει σε αυτές τις δύο περιπτώσεις και μπορούμε να υποθέσουμε ότι $p > 3$. Από το Πόρισμα 9.3.2 για κάθε ακέραιο a με $1 \leqslant a \leqslant p-1$ υπάρχει αντίστροφος a', $1 \leqslant a' \leqslant p-1$, έτσι ώστε $aa' \equiv 1 \pmod p$.

Ισχυριζόμαστε σε αυτό το σημείο ότι επειδή ο p είναι πρώτος, θα έχουμε $a = a'$, αν και μόνο αν $a = 1$ ή $a = p-1$. Πράγματι, η ισοτιμία $a^2 \equiv 1 \pmod p$ είναι ισοδύναμη με την $(a-1)(a+1) \equiv 0 \pmod p$. Άρα είτε $a - 1 \equiv 0 \pmod p$ και σ' αυτήν την περίπτωση έχουμε $a = 1$ είτε $a + 1 \equiv 0 \pmod p$ οπότε $a = p - 1$.

Μπορούμε τώρα να βάλουμε τους αριθμούς από τον 2 μέχρι τον $p-2$ σε $(p-3)/2$ ζευγάρια πολλαπλασιαστικών αντιστρόφων a, a' με $a \neq a'$ ώστε το γινόμενο των αριθμών σε κάθε ζευγάρι να ισούται με $1 \pmod p$. Άρα θα έχουμε

$$2 \cdot 3 \cdots (p-3) \cdot (p-2) \equiv 1 \pmod p .$$

Πολλαπλασιάζουμε την παραπάνω ισοτιμία με 1 και $p-1$ και παίρνουμε

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-3)(p-2)(p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod p .$$

Η απόδειξη έχει ολοκληρωθεί. ■

Όπως εξηγήσαμε αρχικά, ισχύει και το αντίστροφο του Θεωρήματος 12.1.1.

Θεώρημα 12.1.2. *Αν ο φυσικός $n \geqslant 2$ είναι τέτοιος ώστε $(n-1)! \equiv -1 \pmod n$, τότε ο n είναι πρώτος.*

Απόδειξη. Έστω αντίθετα ότι ο n είναι σύνθετος και ικανοποιεί την $(n-1)! \equiv -1 \pmod n$. Έχουμε τότε ότι $n = ab$ για κάποιους φυσικούς a, b, όπου $1 < a < n$ και $1 < b < n$. Εφ' όσον $a < n$, προκύπτει ότι $a \mid (n-1)!$, αφού ο a εμφανίζεται ως όρος του γινομένου $(n-1)!$. Άρα $a \mid n \mid (n-1)! + 1$. Συνεπώς, ο a διαιρεί τον

$$(n-1)! + 1 - (n-1)! = 1,$$

κάτι που είναι άτοπο, αφού $a > 1$. Καταλήγουμε ότι ο n είναι όντως πρώτος, όπως θέλαμε να δείξουμε. ■

Συνδυαστικά τα Θεωρήματα 12.1.1 και 12.1.2 μας δίνουν ένα από τα ελάχιστα καθολικά κριτήρια πρώτων αριθμών. Επειδή όμως ο $(n-1)!$ αυξάνεται ραγδαία με την αύξηση του n, ως κριτήρια απόφασης αν ένας αριθμός είναι πρώτος, έχουν περισσότερο θεωρητικό παρά πρακτικό ενδιαφέρον.

Ας δούμε τώρα μερικές εφαρμογές του Θεωρήματος του Wilson και του αντιστρόφου του.

Εφαρμογή 12.1.3. Θα δείξουμε τον ακόλουθο «τύπο» για την συνάρτηση μέτρησης πρώτων που αποδίδεται στον Minač:

$$\pi(n) = \sum_{j=2}^{n} \left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor .$$

Αν και φαίνεται τρομακτικός, ο παραπάνω τύπος δεν είναι δύσκολο να δειχθεί. Το μόνο που πρέπει να δείξουμε είναι ότι η συνάρτηση $f(j)$ που λειτουργεί ως όρισμα του αθροίσματος,

είναι «δείκτρια πρώτων», δηλαδή παίρνει την τιμή 1 όταν ο j είναι πρώτος και την τιμή 0 όταν ο j είναι σύνθετος. Σε αυτό θα μας βοηθήσει η Άσκηση 5.3.4 σύμφωνα με την οποία αν ο φυσικός $n > 4$ είναι σύνθετος, τότε $n \mid (n-1)!$.

Αν τώρα ο j είναι πρώτος, τότε το Θεώρημα του Wilson μας δίνει ότι $(j-1)! + 1 = kj$ για κάποιον φυσικό k, οπότε

$$\left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \left\lfloor k - \left\lfloor k - \frac{1}{j} \right\rfloor \right\rfloor = k - (k-1) = 1.$$

Από την άλλη, αν ο $j \geqslant 6$ είναι σύνθετος, τότε η Άσκηση 5.3.4 μας δίνει ότι $(j-1)! = kj$ για κάποιον φυσικό k, οπότε

$$\left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \left\lfloor k + \frac{1}{j} - k \right\rfloor = \left\lfloor \frac{1}{j} \right\rfloor = 0,$$

ενώ για $j = 4$ έχουμε

$$\left\lfloor \frac{3!+1}{4} - \left\lfloor \frac{3!}{4} \right\rfloor \right\rfloor = 0.$$

Σε κάθε περίπτωση έχουμε δείξει ότι $f(j) = 1$, αν ο j είναι πρώτος και $f(j) = 0$, αν ο j είναι σύνθετος, οπότε η απόδειξη είναι πλήρης. ■

Ως δεύτερη εφαρμογή του Θεωρήματος του Wilson, θα εξετάσουμε μια ειδική περίπτωση τετραγωνικής ισοτιμίας. Με τον όρο τετραγωνική ισοτιμία (θα έχουμε περισσότερα να πούμε γι' αυτές στα τελευταία μαθήματα) εννοούμε μία ισοτιμία της μορφής $ax^2+bx+c \equiv 0 \pmod{n}$, όπου $a \not\equiv 0 \pmod{n}$.

Εφαρμογή 12.1.4. Θα δείξουμε ότι η τετραγωνική ισοτιμία $x^2 + 1 \equiv 0 \pmod{p}$, όπου p είναι ένας περιττός πρώτος, έχει λύση, αν και μόνο αν $p \equiv 1 \pmod{4}$.

Έστω a μία λύση της $x^2 + 1 \equiv 0 \pmod{p}$ έτσι ώστε $a^2 \equiv -1 \pmod{p}$. Εφ' όσον $p \nmid a$, το μικρό Θεώρημα του Fermat μας δίνει

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Συμπεραίνουμε ότι ο p δεν είναι της μορφής $4k + 3$, αφού διαφορετικά θα είχαμε

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1,$$

άρα και $1 \equiv -1 \pmod{p}$, δηλαδή $p = 2$, ενώ υποθέτουμε ότι ο p είναι περιττός. Άρα $p = 4k+1$ για κάποιον φυσικό k, που σημαίνει ότι $p \equiv 1 \pmod{4}$.

Θα δείξουμε τώρα το αντίστροφο, δηλαδή ότι αν $p \equiv 1 \pmod{4}$, τότε η τετραγωνική ισοτιμία $x^2 + 1 \equiv 0 \pmod{p}$ έχει λύση. Στο γινόμενο

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)$$

έχουμε τις ισοτιμίες

$$\begin{aligned} p - 1 &\equiv -1 \pmod{p} \\ p - 2 &\equiv -2 \pmod{p} \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p}. \end{aligned}$$

Αναδιατάσσοντας τους όρους, παίρνουμε

$$\begin{aligned}(p-1)! &\equiv 1\cdot(-1)\cdot 2\cdot(-2)\cdots\frac{p-1}{2}\cdot\left(-\frac{p-1}{2}\right) \pmod p\\ &\equiv (-1)^{(p-1)/2}\left(1\cdot 2\cdots\frac{p-1}{2}\right)^2 \pmod p,\end{aligned}$$

αφού ο αριθμός των αρνητικών προσήμων είναι $(p-1)/2$. Χρησιμοποιούμε τώρα το Θεώρημα του Wilson, που μας δίνει ότι $(p-1)!\equiv -1 \pmod p$, για να γράψουμε

$$-1\equiv (-1)^{(p-1)/2}\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p.$$

Υποθέτουμε όμως ότι ο p είναι της μορφής $4k+1$, άρα $(-1)^{(p-1)/2}=1$. Έχουμε επομένως ότι

$$-1\equiv\left[\left(\frac{p-1}{2}\right)!\right]^2,$$

από το οποίο προκύπτει ότι ο $[(p-1)/2]!$ ικανοποιεί την ισοτιμία $x^2+1\equiv 0 \pmod p$. ■

Παράδειγμα 12.1.5. Για να δούμε με ένα συγκεκριμένο παράδειγμα ότι αυτό που κάναμε στην παραπάνω εφαρμογή είναι όντως σωστό, θεωρούμε τον $p=13$ που είναι πρώτος της μορφής $4k+1$. Έχουμε ότι $(p-1)/2=6$ και

$$6!=720\equiv 5 \pmod{13}.$$

Έχουμε τώρα ότι

$$5^2+1=26\equiv 0 \pmod{13},$$

όπως είχαμε προβλέψει.

12.2 Ασκήσεις

Άσκηση 12.2.1. Βρείτε το υπόλοιπο της διαίρεσης του 15! με τον 17.

Απόδειξη. Από το Θεώρημα του Wilson έχουμε $16!\equiv -1\equiv 16 \pmod{17}$. Είτε πολλαπλασιάζοντας με 16 και τα δύο μέλη της ισοτιμίας (αφού ο 16 είναι ο πολλαπλασιαστικός αντίστροφος του εαυτού του) είτε παρατηρώντας ότι $\gcd(16,17)=1$ και άρα ο παράγοντας 16 μπορεί να απλοποιηθεί, παίρνουμε $15!\equiv 1 \pmod{17}$. Άρα το υπόλοιπο της διαίρεσης είναι ο 1. ■

Άσκηση 12.2.2. Ομαδοποιήστε τους αριθμούς $2,3,4,\ldots,21$ σε ζευγάρια a, b έτσι ώστε $ab\equiv 1 \pmod{23}$.

Λύση. Παρατηρούμε τα εξής:

$$\begin{aligned}2\cdot 12=3\cdot 8=4\cdot 6=24&\equiv 1 \pmod{23}\\ 5\cdot 14=7\cdot 10=70&\equiv 1 \pmod{23}\\ 9\cdot 18=162&\equiv 1 \pmod{23}\\ 11\cdot 21=231&\equiv 1 \pmod{23}\\ 13\cdot 16=208&\equiv 1 \pmod{23}\\ 15\cdot 20=300&\equiv 1 \pmod{23}\\ 17\cdot 19=323&\equiv 1 \pmod{23}.\end{aligned}$$

Άρα τα

$$\{\{2,12\},\{3,8\},\{4,6\},\{5,14\},\{7,10\},\{9,18\},\{11,21\},\{13,16\},\{15,20\},\{19,17\}\}$$

είναι τα ζεύγη πολλαπλασιαστικών αντιστρόφων που ψάχνουμε. ■

Άσκηση 12.2.3. Δείξτε ότι υπάρχουν άπειροι σύνθετοι της μορφής $n! + 1$.

Σημείωση: Είναι ανοιχτό πρόβλημα αν υπάρχουν άπειρες τιμές του n για τις οποίες ο $n! + 1$ είναι πρώτος. Πρώτοι αυτής της μορφής καλούνται «παραγοντικοί πρώτοι». Ο $150209! + 1$ είναι ο μεγαλύτερος παραγοντικός πρώτος που έχουμε ανακαλύψει μέχρι σήμερα.

Απόδειξη. Το Θεώρημα του Wilson μας δίνει ότι αν ο p είναι πρώτος, τότε $p \mid (p-1)! + 1$. Για $p > 3$ όμως έχουμε $(p-2)! > 1$, δηλαδή $(p-1)! > p - 1$ και άρα $(p-1)! + 1 > p$. Προκύπτει λοιπόν ότι για $p > 3$, ο p είναι γνήσιος διαιρέτης του $(p-1)! + 1$. Συμπεραίνουμε ότι ο $(p-1)! + 1$ είναι σύνθετος για κάθε πρώτο $p \geqslant 5$. ■

Άσκηση 12.2.4. Χρησιμοποιήστε την Άσκηση 5.3.4 για να δώσετε μια διαφορετική απόδειξη του Θεωρήματος 12.1.2.

Απόδειξη. Χρησιμοποιούμε αντιθετοαντιστροφή για να δείξουμε το ζητούμενο, οπότε αρκεί να δείξουμε ότι αν ο φυσικός n είναι σύνθετος, τότε $(n-1)! \not\equiv -1 \pmod{n}$. Για $n = 4$ έχουμε $3! = 6 \not\equiv -1 \pmod{4}$, ενώ για $n > 4$ η Άσκηση 5.3.4 μας εξασφαλίζει ότι

$$(n-1)! \equiv 0 \not\equiv -1 \pmod{n},$$

όπως θέλαμε. ■

Άσκηση 12.2.5. Να αποδειχθεί η εξής γενίκευση του Θεωρήματος του Wilson η οποία οφείλεται στον Elston (1957): αν p πρώτος και $0 \leqslant k \leqslant p-1$, τότε

$$k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}.$$

Απόδειξη. Παρατηρούμε αρχικά ότι $(p-1)! = (p-k-1)!(p-k)\cdots(p-1)$. Έχουμε ακόμα ότι

$$\begin{aligned} p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \\ &\vdots \\ p-k &\equiv -k \pmod{p}. \end{aligned}$$

Πολλαπλασιάζουμε τις ισοτιμίες και παίρνουμε $(p-k)\cdots(p-1) \equiv (-1)^k k! \pmod{p}$. Προκύπτει λοιπόν ότι

$$(p-1)! = (p-k-1)!(p-k)\cdots(p-1) \equiv (p-k-1)!(-1)^k k! \pmod{p}.$$

Από το Θεώρημα του Wilson όμως γνωρίζουμε ότι $(p-1)! \equiv -1 \pmod{p}$, άρα

$$(p-k-1)!(-1)^k k! \equiv -1 \pmod{p}.$$

Πολλαπλασιάζοντας με $(-1)^k$, παίρνουμε

$$(p-k-1)!k! \equiv (-1)^{k+1} \pmod{p},$$

που είναι ακριβώς η σχέση που θέλαμε να δείξουμε. ■

Άσκηση 12.2.6. $(*)$ Έστω p πρώτος και n φυσικός. Δείξτε ότι

$$\frac{(np)!}{n!p^n} \equiv (-1)^n \pmod{p}.$$

Απόδειξη. Κάνουμε την εξής αρχική παρατήρηση: αν ο a είναι φυσικός και $a \equiv 1 \pmod{p}$, τότε από το Θεώρημα του Wilson έχουμε ότι

$$a(a+1)\cdots[a+(p-2)] \equiv (p-1)! \equiv -1 \pmod{p}.$$

Με άλλα λόγια, το γινόμενο των $p-1$ ακεραίων μεταξύ δύο διαδοχικών πολλαπλασίων του p είναι ισότιμο με $-1 \pmod{p}$. Συμπεραίνουμε ότι

$$\begin{aligned}
\frac{(np)!}{n!p^n} &= \frac{(np)!}{p \cdot 2p \cdot 3p \cdots (np)} \\
&= \prod_{r=1}^{n} [(r-1)p+1] \cdots [(r-1)p+(p-1)] \\
&\equiv \prod_{r=1}^{n} (p-1)! \pmod{p} \\
&\equiv \prod_{r=1}^{n} (-1) \pmod{p} \\
&\equiv (-1)^n \pmod{p},
\end{aligned}$$

όπως θέλαμε να δείξουμε. ■

Κεφάλαιο 13

13η Παράδοση

Στο σημερινό μάθημα θα κάνουμε μια εισαγωγή στις αριθμητικές συναρτήσεις. Θα δούμε τις συναρτήσεις σ και τ, τις καλούμενες αντίστοιχα «άθροισμα θετικών διαιρετών» και «πλήθος θετικών διαιρετών», και κάποιες βασικές ιδιότητές τους.

13.1 Οι συναρτήσεις τ και σ

Με τον όρο *αριθμητική συνάρτηση* (ή *αριθμοθεωρητική συνάρτηση*) εννοούμε απλώς μία συνάρτηση με πεδίο ορισμού τους φυσικούς. Συνήθως το πεδίο τιμών είναι οι ίδιοι οι φυσικοί, αλλά μπορεί σε κάποιες περιπτώσεις να είναι οι ακέραιοι ή ακόμα και οι πραγματικοί ή οι μιγαδικοί αριθμοί.

Ορισμός 13.1.1. Δοθέντος φυσικού n, συμβολίζουμε με $\tau(n)$ το πλήθος των θετικών διαιρετών του n και με $\sigma(n)$ το άθροισμα αυτών των θετικών διαιρετών.

Αν έχουμε $n = 12$ για παράδειγμα, τότε επειδή οι θετικοί διαιρέτες του 12 είναι οι $1, 2, 3, 4, 6, 12$, βρίσκουμε ότι

$$\tau(12) = 6 \qquad \text{και} \qquad \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$

Μερικές ακόμα τιμές των συναρτήσεων τ και σ φαίνονται στον Πίνακα 13.1.1. Παρατηρούμε ότι $\tau(n) = 2$ αν και μόνο αν ο n είναι πρώτος. Επίσης, $\sigma(n) = n+1$. αν και μόνο αν ο n είναι πρώτος.

Πίνακας 13.1.1: Οι αρχικές τιμές των συναρτήσεων τ και σ

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39

Πριν μελετήσουμε αναλυτικότερα τις συναρτήσεις τ και σ, εξηγούμε έναν εύχρηστο συμβολισμό ο οποίος θα μας φανεί χρήσιμος και αργότερα. Συγκεκριμένα, το

$$\sum_{d|n} f(d)$$

συμβολίζει ένα άθροισμα που εκτείνεται στους διαιρέτες του n (και μόνο σ' αυτούς). Έχουμε για παράδειγμα

$$\sum_{d|20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20).$$

Με αυτόν τον συμβολισμό λοιπόν έχουμε ότι

$$\tau(n) = \sum_{d|n} 1 \qquad \text{και} \qquad \sigma(n) = \sum_{d|n} d.$$

Στο επόμενο θεώρημα εξηγούμε αναλυτικά την μορφή των διαιρετών ενός φυσικού n, εάν μας δίνεται η κανονική μορφή του n.

Θεώρημα 13.1.2. *Αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού $n > 1$, τότε οι θετικοί διαιρέτες του n είναι ακριβώς εκείνοι οι φυσικοί d της μορφής*

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

όπου $0 \leqslant a_i \leqslant k_i$ για $i = 1, 2, \ldots, r$.

Απόδειξη. Για $a_1 = a_2 = \cdots = a_r = 0$ έχουμε $d = 1$, ενώ για $a_1 = k_1, a_2 = k_2, \ldots, a_r = k_r$ έχουμε $d = n$. Αν τώρα ο d είναι γνήσιος διαιρέτης του n, τότε $n = dd'$ και $d > 1$, $d' > 1$. Γράφουμε και τον d και τον d' ως γινόμενα (όχι απαραίτητα διακεκριμένων) πρώτων:

$$d = q_1 q_2 \cdots q_s \qquad d' = t_1 t_2 \cdots t_u.$$

Έχουμε τότε ότι οι

$$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 q_2 \cdots q_s t_1 t_2 \cdots t_u$$

είναι και οι δύο αναλύσεις του n ως γινομένου πρώτων. Από το Θεμελιώδες Θεώρημα της Αριθμητικής κάθε πρώτος q_i είναι ένας από τους p_j. Μαζεύοντας τώρα ίδιους παράγοντες σε μία ενιαία δύναμη, παίρνουμε

$$d = q_1 q_2 \cdots q_s = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

όπου έχουμε επιτρέψει το ενδεχόμενο $a_i = 0$ για κάποιους δείκτες i.

Αντίστροφα, είναι σχεδόν προφανές ότι κάθε αριθμός της μορφής $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, με $0 \leqslant a_i \leqslant k_i$, είναι διαιρέτης του n, αφού

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \left(p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r} \right) = dd'$$

με $d' = p_1^{k_1 - a_1} p_2^{k_2 - a_2} \cdots p_r^{k_r - a_r}$ και $k_i - a_i \geqslant 0$ για κάθε i. Επομένως $d' > 0$ και άρα $d \mid n$. ■

Στο επόμενο θεώρημα θα δούμε πώς μπορούμε να χρησιμοποιήσουμε αυτό που μόλις δείξαμε, για να βρούμε τύπους για τις συναρτήσεις τ και σ.

Θεώρημα 13.1.3. *Αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού $n > 1$, τότε*

(i) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$, *και*

(ii) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}.$

Απόδειξη. (i) Σύμφωνα με το Θεώρημα 13.1.2, οι θετικοί διαιρέτες του n είναι ακριβώς εκείνοι οι φυσικοί

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

όπου $0 \leqslant a_i \leqslant k_i$ για $i = 1, 2, \ldots, r$. Υπάρχουν k_1+1 επιλογές για τον εκθέτη a_1, k_2+1 επιλογές για τον εκθέτη a_2, ... και $k_r + 1$ επιλογές για τον εκθέτη a_r. Επομένως, υπάρχουν

$$(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

θετικοί διαιρέτες του n.

(ii) Θεωρούμε το γινόμενο

$$\left(1 + p_1 + p_1^2 + \ldots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}\right) \cdots \left(1 + p_r + p_r^2 + \ldots + p_r^{k_r}\right)$$

και παρατηρούμε ότι κάθε διαιρέτης του n εμφανίζεται ακριβώς μία φορά στο ανάπτυγμα αυτού του γινομένου. Επομένως

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \ldots + p_1^{k_1}\right) \cdots \left(1 + p_r + p_r^2 + \ldots + p_r^{k_r}\right).$$

Για κάθε δείκτη i με $1 \leqslant i \leqslant r$, το $1 + p_i + p_i^2 + \ldots + p_i^{k_i}$ είναι άθροισμα όρων γεωμετρικής σειράς, άρα

$$1 + p_i + p_i^2 + \ldots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

Συμπεραίνουμε ότι

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1},$$

όπως θέλαμε να δείξουμε. ■

Το ανάλογο που εξηγήσαμε πριν για τον συμβολισμό αθροισμάτων, ισχύει και για τα γινόμενα. Έχουμε για παράδειγμα ότι

$$\prod_{d=1}^{5} f(d) = f(1)f(2)f(3)f(4)f(5), \quad \prod_{d|9} f(d) = f(1)f(3)f(9), \quad \prod_{\substack{p|30 \\ p \text{ πρώτος}}} f(p) = f(2)f(3)f(5).$$

Με αυτές τις εξηγήσεις μπορούμε να αναδιατυπώσουμε το Θεώρημα 13.1.3 ως εξής:

Αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού $n > 1$, τότε

$$\tau(n) = \prod_{i=1}^{r} (k_i + 1) \qquad \text{και} \qquad \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

Παράδειγμα 13.1.4. Ο φυσικός $180 = 2^2 \cdot 3^2 \cdot 5$ έχει

$$\tau(180) = (2 + 1)(2 + 1)(1 + 1) = 18$$

θετικούς διαιρέτες. Οι διαιρέτες αυτοί έχουν την μορφή

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3},$$

όπου $a_1 \in \{0,1,2\}$, $a_2 \in \{0,1,2\}$ και $a_3 \in \{0,1\}$. Συγκεκριμένα, οι θετικοί διαιρέτες του 180 είναι οι

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 9,\ 10,\ 12,\ 15,\ 18,\ 20,\ 30,\ 36,\ 45,\ 60,\ 90,\ 180.$$

Παρατηρήστε ότι καθένας τους αντιστοιχεί σε μία επιλογή των a_1, a_2, a_3. Το δε άθροισμα των θετικών διαιρετών είναι

$$\sigma(180) = \frac{2^3-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546.$$

Κάνουμε ξεχωριστή μνεία στην εξής απόρροια του Θεωρήματος 13.1.3.

Πόρισμα 13.1.5. *Για έναν φυσικό n έχουμε ότι ο $\tau(n)$ είναι περιττός, αν και μόνο αν ο n είναι τέλειο τετράγωνο.*

Απόδειξη. Για $n = 1$ το ζητούμενο ισχύει προφανώς, αφού $1 = 1^2$ και $\tau(1) = 1$. Αν $n > 1$ και $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του n, τότε ξέρουμε από το Θεώρημα 13.1.3 ότι $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$.

Αν ο $\tau(n)$ είναι περιττός, τότε κάθε όρος $k_i + 1$ είναι αναγκαστικά περιττός, δηλαδή $k_i = 2a_i$ για κάποιον a_i. Επομένως

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = (p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})^2$$

και άρα ο n είναι τέλειο τετράγωνο.

Αντίστροφα, αν $n = m^2$ για κάποιον φυσικό m, τότε ο εκθέτης k_i κάθε πρώτου p_i που εμφανίζεται στην κανονική μορφή του n είναι άρτιος. (Συγκεκριμένα, αν ο p_i εμφανίζεται στην κανονική μορφή του m στην δύναμη b_i, τότε ο p_i εμφανίζεται στην κανονική μορφή του n στην δύναμη $2b_i$.) Προκύπτει λοιπόν ότι ο $k_i + 1$ είναι περιττός και άρα ο $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$ είναι επίσης περιττός. ■

Ας δούμε τώρα και μία εφαρμογή.

Εφαρμογή 13.1.6. Θα δείξουμε ότι το γινόμενο όλων των θετικών διαιρετών του φυσικού $n > 1$ ισούται με $n^{\tau(n)/2}$, δηλαδή

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}.$$

Έστω d θετικός διαιρέτης του n, έτσι ώστε $n = dd'$ για κάποιον d'. Προσέξτε ότι ο d' είναι επίσης διαιρέτης του n. Καθώς ο d διατρέχει τους θετικούς διαιρέτες του n, προκύπτουν $\tau(n)$ τέτοιες εξισώσεις τις οποίες μπορούμε να πολλαπλασιάσουμε μεταξύ τους και να πάρουμε

$$n^{\tau(n)} = \prod_{d|n} d \cdot \prod_{d'|n} d'.$$

Παρατηρούμε τώρα ότι όταν ο d διατρέχει τους θετικούς διαιρέτες του n, το ίδιο κάνει και ο d'. Επομένως

$$\prod_{d|n} d = \prod_{d'|n} d'$$

και άρα

$$n^{\tau(n)} = \left(\prod_{d|n} d \right)^2$$

που είναι ισοδύναμο με αυτό που θέλαμε να δείξουμε. ■

13.2 Ασκήσεις

Άσκηση 13.2.1. Δείξτε ότι για $n = 3655$ και $n = 4503$ ισχύει ότι

$$\tau(n) = \tau(n+1) = \tau(n+2) = \tau(n+3),$$

ενώ για $n = 14$, $n = 206$ και $n = 957$ ισχύει ότι

$$\sigma(n) = \sigma(n+1).$$

Απόδειξη. Οι αριθμοί $3655, 3666, 3657, 3658$ όπως και οι $4503, 4504, 4505, 4506$ είναι όλοι είτε της μορφής $p \cdot q \cdot r$ είτε της $p^3 \cdot q$. Προκύπτει λοιπόν ότι, αν ο n είναι ένας από αυτούς τους αριθμούς, τότε $\tau(n) = 2 \cdot 2 \cdot 2 = 8 = 4 \cdot 2$. Συγκεκριμένα, $3655 = 5 \cdot 17 \cdot 43$, $3656 = 2^3 \cdot 357$, $3657 = 3 \cdot 23 \cdot 53$, $3658 = 2 \cdot 31 \cdot 59$ και $4503 = 3 \cdot 19 \cdot 79$, $4504 = 2^3 \cdot 563$, $4505 = 5 \cdot 17 \cdot 53$, $4506 = 2 \cdot 3 \cdot 751$.

Έχουμε $\sigma(14) = 3 \cdot 8 = 24 = 4 \cdot 6 = \sigma(15)$, $\sigma(206) = 3 \cdot 104 = 312 = 13 \cdot 24 = \sigma(207)$ και $\sigma(957) = 4 \cdot 12 \cdot 30 = 1440 = 3 \cdot 480 = \sigma(958)$. ■

Άσκηση 13.2.2. Δείξτε ότι ο $n^{\tau(n)/2}$ είναι πάντα φυσικός, όπου n φυσικός και $n > 1$, χωρίς να χρησιμοποιήσετε την ισότητα που δείξαμε στην Εφαρμογή 13.1.6.

Σημείωση: Το νόημα αυτής της άσκησης είναι το εξής: στην ισότητα που δείξαμε στην Εφαρμογή 13.1.6, ο $\prod_{d|n} d$ είναι σίγουρα φυσικός, αλλά δεν είναι εντελώς προφανές γιατί είναι φυσικός και ο $n^{\tau(n)/2}$.

Απόδειξη. Έστω φυσικός $n > 1$. Εάν ο $\tau(n)$ είναι άρτιος, τότε ο $\tau(n)/2$ είναι φυσικός και άρα ο $n^{\tau(n)/2}$ είναι επίσης φυσικός. Από την άλλη, αν ο $\tau(n)$ είναι περιττός, τότε ο n είναι τέλειο τετράγωνο σύμφωνα με το Πόρισμα 13.1.5, δηλαδή $n = m^2$ για κάποιον φυσικό m. Προκύπτει τότε ότι

$$n^{\frac{\tau(n)}{2}} = (m^2)^{\frac{\tau(n)}{2}} = m^{\tau(n)},$$

που είναι φυσικός. ■

Άσκηση 13.2.3. Να αποδειχθεί ότι για κάθε φυσικό n ισχύει ότι

$$\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}.$$

Απόδειξη. Παρατηρούμε ότι ο d είναι διαιρέτης του φυσικού n, αν και μόνο αν ο n/d είναι διαιρέτης του n, αφού $d \cdot \frac{n}{d} = n$. Επομένως, αν $\{d_1, d_2, \ldots, d_k\}$ είναι το σύνολο διαιρετών του n, τότε

$$\{d_1, d_2, \ldots, d_k\} = \left\{ \frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_k} \right\}$$

άρα και

$$\sigma(n) = \sum_{i=1}^{k} d_i = \sum_{i=1}^{k} \frac{n}{d_i} = n \sum_{i=1}^{k} \frac{1}{d_i}.$$

Συμπεραίνουμε ότι

$$\frac{\sigma(n)}{n} = \sum_{i=1}^{k} \frac{1}{d_i} = \sum_{d|n} \frac{1}{d},$$

που ήταν το ζητούμενο. ■

Άσκηση 13.2.4. Να αποδειχθεί ότι για κάθε φυσικό n ισχύει η ανισότητα $\tau(n) \leqslant 2\sqrt{n}$.

Υπόδειξη: Αν $d \mid n$, τότε ένας εκ των d, n/d είναι $\leqslant \sqrt{n}$.

Απόδειξη. Ας υποθέσουμε αρχικά ότι ο n δεν είναι τέλειο τετράγωνο. Τότε για κάθε διαιρέτη του n που είναι μικρότερος του $\sqrt{n}$, υπάρχει ένας και μόνο ένας «συμπληρωματικός» διαιρέτης του n που είναι μεγαλύτερος του $\sqrt{n}$ (συγκεκριμένα, ο συμπληρωματικός αυτός διαιρέτης είναι ο n/d). Προκύπτει λοιπόν ότι ο αριθμός των διαιρετών του n είναι το διπλάσιο του αριθμού των διαιρετών του n που είναι μικρότεροι του $\sqrt{n}$. Όμως ο αριθμός των διαιρετών του n που είναι μικρότεροι του $\sqrt{n}$ είναι προφανώς το πολύ $\sqrt{n}$, άρα $\tau(n) \leqslant 2\sqrt{n}$.

Το ίδιο επιχείρημα δουλεύει και στην περίπτωση που ο n είναι τέλειο τετράγωνο· με την διαφορά ότι εδώ υπάρχει ένας διαιρέτης που δεν σχηματίζει ζευγάρι με διαιρέτη διαφορετικό του εαυτού του. Ο ξεχωριστός αυτός διαιρέτης είναι ο $\sqrt{n}$. Επιχειρηματολογώντας όπως και πιο πάνω, βλέπουμε ότι σε αυτήν την περίπτωση ισχύει το ελαφρώς ισχυρότερο φράγμα $\tau(n) \leqslant 2\sqrt{n} - 1$. ■

Άσκηση 13.2.5. Δίνεται ότι ο φυσικός n είναι τέτοιος ώστε ο $m = n^2 - 9$ έχει 6 θετικούς διαιρέτες. Να δείξετε ότι $\gcd(n-3, n+3) = 1$.

Απόδειξη. Υπενθυμίζουμε ότι αν $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού m, τότε $\tau(m) = (k_1 + 1) \cdots (k_r + 1)$. Επειδή

$$\tau(m) = 6 = 1 \cdot 6 = 2 \cdot 3$$

είναι οι μόνες δύο παραγοντοποιήσεις του 6, βλέπουμε ότι είτε $m = p^5$ είτε $m = p^2 q$, όπου p, q πρώτοι.

Εξετάζουμε την περίπτωση $m = p^5$ αρχικά. Εφ' όσον $n - 3 < n + 3$, ενώ παράλληλα $m = (n-3)(n+3)$, έχουμε αναγκαστικά $n - 3 \leqslant \sqrt{p^5} \leqslant n + 3$. Προκύπτει επομένως ότι $n - 3 \leqslant p^2$ και $p^3 \leqslant n + 3$. Άρα

$$n + 3 \geqslant p^3 = p \cdot p^2 \geqslant p \cdot (n-3) \geqslant 2(n-3) = 2n - 6$$

η οποία συνεπάγεται την $n \leqslant 9$. Μπορούμε τώρα να απορρίψουμε την περίπτωση $m = p^5$ με έλεγχο των τιμών $n \leqslant 9$ (δείτε τον Πίνακα 13.2.1).

Συμπεραίνουμε ότι $m = p^2 q$, όπου p, q διακεκριμένοι πρώτοι. Προσέξτε ότι δεν κάνουμε καμία υπόθεση ποιος από τους p, q είναι μεγαλύτερος του άλλου. Η μόνη περίπτωση να μην ισχύει η $\gcd(n-3, n+3) = 1$ είναι να έχουμε $n + 3 = pq$ και $n - 3 = p$. Σε αυτήν την περίπτωση όμως θα ισχύει

$$n + 3 = pq \geqslant 2p = 2n - 6,$$

Πίνακας 13.2.1: Η $\tau(m)$ για $n \leqslant 9$

n	4	5	6	7	8	9
m	7	16	27	40	55	72
$\tau(m)$	2	5	4	8	4	12

δηλαδή $n \leqslant 9$. Με βάση πάλι τον Πίνακα 13.2.1, δεν υπάρχει $n \leqslant 9$ ώστε $\tau(m) = 6$. Άρα όντως $\gcd(n-3, n+3) = 1$, όπως θέλαμε να δείξουμε. ■

Σημείωση: Δεν είναι εντελώς προφανές ότι υπάρχουν φυσικοί n τέτοιοι ώστε ο $m = n^2 - 9$ να έχει 6 ακριβώς διαιρέτες. Υπάρχουν όντως όμως τέτοιοι n και με χρήση ενός υπολογιστικού προγράμματος μπορούμε να βρούμε παραδείγματα. Για $n \leqslant 100$ οι τιμές για τις οποίες $\tau(m) = 6$ είναι οι $n = 22, 28, 46$.

Άσκηση 13.2.6. Να δείξετε ότι αν ο n είναι φυσικός, τότε ο $\sigma(n)$ είναι περιττός αν και μόνο αν ο n είναι είτε τέλειο τετράγωνο είτε το διπλάσιο ενός τέλειου τετραγώνου.

Υπόδειξη: Αν ο p είναι περιττός πρώτος, τότε ο $1 + p + p^2 + \ldots + p^k$ είναι περιττός, μόνο όταν ο k είναι άρτιος.

Απόδειξη. Έστω $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ η κανονική μορφή του φυσικού n.

Υποθέτουμε αρχικά ότι ο

$$\sigma(n) = \prod_{i=1}^{r} \left(1 + p_i + p_i^2 + \ldots + p_i^{k_i}\right)$$

είναι περιττός. Προκύπτει τότε ότι κάθε όρος $1 + p_i + p_i^2 + \ldots + p_i^{k_i}$ είναι επίσης περιττός, επομένως (σύμφωνα με την υπόδειξη) αν ο p_i είναι περιττός, τότε $k_i = 2a_i$. Συμπεραίνουμε ότι αν ο n είναι περιττός, τότε $n = t^2$ όπου $t = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Σε περίπτωση που ο n είναι άρτιος και $v_2(n) = b$, έχουμε $n = \left(2^{b/2} p_2^{a_2} \cdots p_r^{a_r}\right)^2$, αν ο b είναι άρτιος και $n = 2\left(2^{(b-1)/2} p_2^{a_2} \cdots p_r^{a_r}\right)^2$, αν ο b είναι περιττός.

Για το αντίστροφο, παρατηρούμε αρχικά ότι ο $\sigma(2^a)$ είναι πάντα περιττός για $a \geqslant 0$. Αν $n = t^2$ με $t = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, τότε $n = p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r}$ και έχουμε ότι ο $\sigma(p_i^{2a_i})$ είναι περιττός για κάθε πρώτο p_i. Εφ' όσον ο $\sigma(n)$ είναι το γινόμενο των $\sigma(p_i^{2a_i})$, συμπεραίνουμε ότι ο $\sigma(n)$ είναι περιττός. Αν $n = 2t^2$ για κάποιον φυσικό t, τότε $n = 2^a p_2^{2a_2} \cdots p_r^{2a_r}$ για κάποιον φυσικό a και περιττούς πρώτους $p_2, \ldots, p_r$. Ο $\sigma(2^a)$ είναι περιττός σύμφωνα με την αρχική μας παρατήρηση, όπως περιττοί είναι όλοι οι $\sigma(p_i^{2a_i})$ από τις εξηγήσεις που δώσαμε στην πρώτη παράγραφο. Εφ' όσον ο $\sigma(n)$ είναι το γινόμενο των $\sigma(p_i^{2a_i})$ με τον $\sigma(2^a)$ και κάθε όρος του γινομένου είναι περιττός, ο $\sigma(n)$ είναι περιττός. ■

Άσκηση 13.2.7. Να δείξετε τις παρακάτω προτάσεις:

(i) Αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού $n > 1$, τότε

$$1 > \frac{n}{\sigma(n)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

(ii) Για κάθε φυσικό n ισχύει ότι

$$\frac{\sigma(n!)}{n!} \geqslant 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}.$$

Υπόδειξη: Χρησιμοποιήστε την Άσκηση 13.2.3.

Σχόλιο: Εφ' όσον η αρμονική σειρά αποκλίνει, ένα πόρισμα αυτής της άσκησης είναι ότι $\limsup_{m\to\infty} \sigma(m)/m = \infty$.

(iii) Αν ο φυσικός $n > 1$ είναι σύνθετος, τότε $\sigma(n) > n + \sqrt{n}$.

Υπόδειξη: Έστω d διαιρέτης του n, όπου $1 < d < n$ έτσι ώστε $1 < n/d < n$. Αν $d \leqslant \sqrt{n}$, τότε $n/d \geqslant \sqrt{n}$.

Απόδειξη. (i) Εφ' όσον $n > 1$, οι 1 και n είναι διακεκριμένοι διαιρέτες του n. Επομένως $\sigma(n) \geqslant n + 1$ και άρα

$$\frac{n}{\sigma(n)} \leqslant \frac{n}{n+1} < 1.$$

Για την δεύτερη ανισότητα, παρατηρούμε ότι αν ο p είναι πρώτος και ο a είναι φυσικός, τότε

$$\frac{p^a}{\sigma(p^a)} = \frac{p^a}{\frac{p^{a+1}-1}{p-1}} = \frac{p^{a+1}-p^a}{p^{a+1}-1} = \frac{p-1}{p-p^{-a}} > \frac{p-1}{p} = 1 - \frac{1}{p}.$$

Συμπεραίνουμε ότι

$$\frac{n}{\sigma(n)} = \prod_{i=1}^{r} \frac{p_i^{k_i}}{\sigma(p_i^{k_i})} > \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right),$$

που είναι η ανισότητα που θέλαμε να δείξουμε.

(ii) Χρησιμοποιούμε αυτό που δείξαμε στην Άσκηση 13.2.3 για να γράψουμε

$$\frac{\sigma(n!)}{n!} = \sum_{d|n!} \frac{1}{d} \geqslant 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n},$$

όπου η ανισότητα προκύπτει από το γεγονός ότι κάθε φυσικός i με $1 \leqslant i \leqslant n$ είναι διαιρέτης του $n!$.

(iii) Εξ υποθέσεως ο n είναι σύνθετος, άρα υπάρχουν φυσικοί d, d' τέτοιοι ώστε $n = dd'$ και $1 < d, d' < n$. Τουλάχιστον ένας εκ των d, d' θα πρέπει να είναι μεγαλύτερος ή ίσος του $\sqrt{n}$, διαφορετικά θα είχαμε $n = dd' < \sqrt{n}\sqrt{n} = n$, που είναι άτοπο. Αν $d \geqslant \sqrt{n}$ για παράδειγμα, τότε $\sigma(n) \geqslant n + d \geqslant n + \sqrt{n}$. Για να δικαιολογήσουμε την πρώτη ανισότητα χρησιμοποιούμε ότι $d < n$ και άρα οι d, n είναι διακεκριμένοι διαιρέτες του n. ■

Άσκηση 13.2.8. $(*)$ Να δείξετε ότι αν $24 \mid n$ όπου $n > 1$ φυσικός, τότε $24 \mid \sigma(n-1)$.

Υπόδειξη: Δείξτε ότι αν $d \mid n-1$, τότε $24 \mid d^2 - 1$ και ότι ο $n-1$ δεν είναι τέλειο τετράγωνο, άρα οι διαιρέτες του «ζευγαριάζουν».

Απόδειξη. Θα δείξουμε πρώτα ότι αν ο d είναι ένας διαιρέτης του $n-1$, τότε $24 \mid d^2 - 1$. Παρατηρούμε ότι ο d δεν είναι πολλαπλάσιο του 3 (αν $3 \mid d$, τότε $3 \mid n-1$ και αφού $3 \mid n$, παίρνουμε $3 \mid 1$, που είναι άτοπο). Άρα $d \equiv 1, 2 \pmod 3$ και έτσι $d^2 \equiv 1 \pmod 3$. Εφ' όσον ο n είναι άρτιος, ο $n-1$ είναι περιττός, άρα και ο d είναι περιττός. Από το Παράδειγμα 2.1.3

γνωρίζουμε ότι $d^2 \equiv 1 \pmod 8$. Έχουμε λοιπόν ότι $3 \mid d^2-1$ και $8 \mid d^2-1$. Επειδή $\gcd(3,8)=1$, παίρνουμε $24 \mid d^2-1$, όπως θέλαμε.

Ισχυριζόμαστε τώρα ότι ο $n-1$ δεν είναι τέλειο τετράγωνο. Αυτό ισχύει γιατί $n-1 \equiv -1 \pmod{24}$ άρα και $n-1 \equiv -1 \pmod 4$, δηλαδή $n-1 \equiv 3 \pmod 4$. Γνωρίζουμε όμως ότι ένα τέλειο τετράγωνο είναι $\equiv 0,1 \pmod 4$, άρα όντως ο $n-1$ δεν είναι τέλειο τετράγωνο. Συμπεραίνουμε ότι οι διαιρέτες του $n-1$ μπαίνουν σε ζευγάρια συμπληρωματικών διαιρετών d, $(n-1)/d$. Όμως

$$d + \frac{n-1}{d} = \frac{(d^2-1)+n}{d}.$$

Ο αριθμητής αυτού του κλάσματος είναι πολλαπλάσιο του 24, γιατί και ο n είναι πολλαπλάσιο του 24 (εξ υποθέσεως) και ο d^2-1 είναι πολλαπλάσιο του 24, όπως δείξαμε στην πρώτη παράγραφο. Άρα

$$d + \frac{n-1}{d} = \frac{24m}{d}$$

για κάποιον φυσικό m. Επίσης, $\gcd(d,24)=1$ άρα $d \mid m$. Καταλήγουμε λοιπόν ότι ο 24 διαιρεί τον $d+(n-1)/d$. Έχουμε τελικά ότι ο

$$\sigma(n-1) = \sum_{\substack{d \mid n-1 \\ d<\sqrt{n}}} \left(d + \frac{n-1}{d} \right)$$

είναι πολλαπλάσιο του 24 ως άθροισμα πολλαπλασίων του 24. ■

Κεφάλαιο 14

14η Παράδοση

Στο σημερινό μάθημα συνεχίζουμε την μελέτη των αριθμητικών συναρτήσεων. Η κεντρική έννοια την οποία θα μελετήσουμε είναι αυτή της πολλαπλασιαστικής συνάρτησης. Θα δούμε κάποια βασικά θεωρήματα που τις αφορούν και μερικές ακόμα συναφείς έννοιες.

14.1 Πολλαπλασιαστικές συναρτήσεις

Στο προηγούμενο μάθημα μιλήσαμε για τις συναρτήσεις τ και σ. Παρατηρήστε ότι για τις δύο αυτές συναρτήσεις ισχύουν (για παράδειγμα) τα εξής:

$$\tau(2 \cdot 6) = \tau(12) = 6 \neq 2 \cdot 4 = \tau(2) \cdot \tau(6)$$

και

$$\sigma(2 \cdot 6) = \sigma(12) = 28 \neq 3 \cdot 12 = \sigma(2) \cdot \sigma(6).$$

Βλέπουμε δηλαδή ότι για τις συναρτήσεις τ και σ δεν ισχύει ότι $f(mn) = f(m)f(n)$ για κάθε δύο φυσικούς m, n. Ισχύει όμως η ισότητα, αν απαιτήσουμε επιπλέον οι m, n να είναι σχετικά πρώτοι. Την ιδιότητα αυτήν την απολαμβάνουν οι περισσότερες «καλές» αριθμητικές συναρτήσεις και γι' αυτόν τον λόγο της δίνουμε ξεχωριστό όνομα.

Ορισμός 14.1.1. Μία αριθμητική συνάρτηση f καλείται **πολλαπλασιαστική**, αν

$$f(mn) = f(m)f(n)$$

για κάθε δύο φυσικούς m, n με $\gcd(m, n) = 1$.

Σε περίπτωση που έχουμε $f(mn) = f(m)f(n)$ για κάθε δύο (όχι απαραίτητα σχετικά πρώτους) φυσικούς m, n, τότε η συνάρτηση f καλείται **πλήρως πολλαπλασιαστική**.

Παραδείγματα πολλαπλασιαστικών συναρτήσεων υπάρχουν πολλά. Θα δείξουμε στην συνέχεια ότι οι συναρτήσεις τ και σ είναι πολλαπλασιαστικές, όπως πολλαπλασιαστικές είναι οι συναρτήσεις ϕ του Euler και μ του Möbius, στις οποίες θα αναφερθούμε αργότερα.

Παραδείγματα πλήρως πολλαπλασιαστικών συναρτήσεων είναι οι συναρτήσεις $f(n) = n^k$, όπου k σταθερός πραγματικός, και η ειδική περίπτωση της προηγούμενης συνάρτησης $g(n) = 1$. Μη τετριμμένα παραδείγματα είναι η συνάρτηση «λάμδα» του Liouville καθώς και τα σύμβολα του Legendre και του Jacobi στα οποία θα αναφερθούμε στα μαθήματα για τις τετραγωνικές ισοτιμίες. Είναι σαφές ότι μία πλήρως πολλαπλασιαστική συνάρτηση είναι αυτόματα και πολλαπλασιαστική. Όπως είδαμε πριν όμως, το αντίστροφο δεν ισχύει.

Θέλουμε τώρα να διατυπώσουμε μερικές αρχικές παρατηρήσεις σε ό,τι αφορά τις πολλαπλασιαστικές συναρτήσεις.

- Μία πρώτη τέτοια παρατήρηση είναι ότι με βάση τον Ορισμό 14.1.1 και ένα εύκολο επαγωγικό επιχείρημα, αν οι φυσικοί $n_1, n_2, \ldots, n_r$ είναι σχετικά πρώτοι ανά δύο, τότε

$$f(n_1 n_2 \cdots n_r) = f(n_1) f(n_2) \cdots f(n_r).$$

  Άμεση συνέπεια αυτού είναι ότι αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού $n > 1$, τότε

$$f(n) = f(p_1^{k_1}) f(p_2^{k_2}) \cdots f(p_r^{k_r}). \tag{14.1.1}$$

  Επομένως μια πολλαπλασιαστική συνάρτηση *προσδιορίζεται πλήρως από τις τιμές που παίρνει σε δυνάμεις πρώτων.*

- Μία δεύτερη παρατήρηση είναι ότι αν η πολλαπλασιαστική συνάρτηση f δεν είναι ταυτοτικά ίση με 0, τότε $f(1) = 1$. Για να το δούμε αυτό, παρατηρούμε ότι εφ' όσον η f δεν είναι ταυτοτικά ίση με 0, υπάρχει φυσικός n_0 τέτοιος ώστε $f(n_0) \neq 0$. Προκύπτει λοιπόν ότι

$$f(n_0) = f(n_0 \cdot 1) = f(n_0) \cdot f(1), \tag{14.1.2}$$

  όπου για την δεύτερη ισότητα χρησιμοποιούμε ότι ο 1 είναι σχετικά πρώτος με οποιονδήποτε φυσικό. Επειδή $f(n_0) \neq 0$, ο $f(n_0)$ μπορεί να απλοποιηθεί στην (14.1.2), οπότε και παίρνουμε $f(1) = 1$, όπως ισχυριστήκαμε.

Συνεχίζουμε τώρα με ένα γενικό αποτέλεσμα το οποίο θα χρησιμοποιήσουμε σε λίγο για να δούμε έναν κανονικό τρόπο κατασκευής πολλαπλασιαστικών συναρτήσεων.

Λήμμα 14.1.2. *Αν $\gcd(m, n) = 1$, τότε το σύνολο των θετικών διαιρετών του mn αποτελείται από τα γινόμενα $d_1 d_2$, όπου $d_1 \mid m$, $d_2 \mid n$ και $\gcd(d_1, d_2) = 1$. Ακόμα, τα γινόμενα αυτά είναι όλα διακεκριμένα.*

Απόδειξη. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $m > 1$ και $n > 1$. Έστω $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ και $n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$ οι κανονικές μορφές των φυσικών m και n. Εφ' όσον οι m, n είναι σχετικά πρώτοι, οι $p_1, \ldots, p_r, q_1, \ldots, q_s$ είναι διακεκριμένοι. Επομένως η κανονική μορφή του mn είναι η

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}.$$

Προκύπτει τώρα ότι ένας διαιρέτης d του mn γράφεται με μοναδικό τρόπο ως

$$d = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s},$$

όπου $0 \leqslant a_i \leqslant k_i$ και $0 \leqslant b_i \leqslant j_i$. Έχουμε λοιπόν ότι $d = d_1 d_2$, όπου ο $d_1 = p_1^{a_1} \cdots p_r^{a_r}$ διαιρεί τον m και ο $d_2 = q_1^{b_1} \cdots q_s^{b_s}$ διαιρεί τον n. Όμως κανένας πρώτος p_i δεν ταυτίζεται με κάποιον q_j, άρα $\gcd(d_1, d_2) = 1$. ■

Το επόμενο θεώρημα είναι κεντρικό.

Θεώρημα 14.1.3. *Αν η f είναι πολλαπλασιαστική συνάρτηση και η F ορίζεται ως*

$$F(n) = \sum_{d \mid n} f(d),$$

τότε η F είναι επίσης πολλαπλασιαστική.

Απόδειξη. Έστω m, n σχετικά πρώτοι φυσικοί. Τότε

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2).$$

Για να δικαιολογήσουμε την δεύτερη ισότητα, επικαλούμαστε το Λήμμα 14.1.2 σύμφωνα με το οποίο οι διαιρέτες του mn είναι σε $1-1$ αντιστοιχία με τα ζεύγη (d_1, d_2), όπου $d_1 \mid m$ και $d_2 \mid n$. Από τον Ορισμό 14.1.1 και δεδομένου ότι $\gcd(d_1, d_2) = 1$, έχουμε

$$f(d_1 d_2) = f(d_1) f(d_2)$$

και άρα προκύπτει ότι

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) = \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) = F(m) F(n), \tag{14.1.3}$$

όπως θέλαμε να δείξουμε. ■

Σε περίπτωση που δεν είναι εντελώς σαφές γιατί ισχύει η δεύτερη ισότητα στην (14.1.3), βλέπουμε τι συμβαίνει με ένα συγκεκριμένο παράδειγμα.

Για $m = 8$ και $n = 3$ έχουμε

$$\begin{aligned}
F(8 \cdot 3) &= \sum_{d|24} f(d) \\
&= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24) \\
&= f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(2 \cdot 3) + f(8 \cdot 1) + f(4 \cdot 3) + f(8 \cdot 3) \\
&= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(2)f(3) + f(8)f(1) \\
&\quad + f(4)f(3) + f(8)f(3) \\
&= [f(1) + f(2) + f(4) + f(8)][f(1) + f(3)] \\
&= \sum_{d|8} f(d) \cdot \sum_{d|3} f(d) \\
&= F(8) \cdot F(3)
\end{aligned}$$

Είμαστε τώρα σε θέση να αποδείξουμε εύκολα ότι οι συναρτήσεις τ, σ είναι πολλαπλασιαστικές.

Πόρισμα 14.1.4. *Οι τ και σ είναι πολλαπλασιαστικές συναρτήσεις.*

Απόδειξη. Όπως έχουμε ήδη αναφέρει, οι συναρτήσεις $f(n) = 1$, $g(n) = n$ για κάθε n φυσικό αντίστοιχα, είναι πολλαπλασιαστικές. Έχουμε τώρα ότι

$$\tau(n) = \sum_{d|n} 1 \qquad \text{και} \qquad \sigma(n) = \sum_{d|n} d,$$

οπότε το ζητούμενο προκύπτει με απλή εφαρμογή του Θεωρήματος 14.1.3. ■

Κατ' αναλογία με την έννοια της πολλαπλασιαστικής συνάρτησης, υπάρχει η έννοια της προσθετικής συνάρτησης.

Ορισμός 14.1.5. Μία αριθμητική συνάρτηση f καλείται **προσθετική**, αν

$$f(mn) = f(m) + f(n)$$

για κάθε δύο φυσικούς m, n με $\gcd(m, n) = 1$.

Επίσης ανάλογα, σε περίπτωση που έχουμε $f(mn) = f(m)+f(n)$ για κάθε δύο (όχι απαραίτητα σχετικά πρώτους) φυσικούς m, n, τότε η συνάρτηση f καλείται **πλήρως προσθετική**.

Το κανονικό παράδειγμα προσθετικής συνάρτησης είναι η συνάρτηση $\omega(n)$ η οποία ορίζεται ως το πλήθος των διακεκριμένων πρώτων που διαιρούν τον n. Δηλαδή, αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού n, τότε εξ ορισμού $\omega(n) = r$. Έχουμε για παράδειγμα ότι $\omega(n) = 1$, αν και μόνο αν ο n είναι δύναμη πρώτου.

Το δε κανονικό παράδειγμα πλήρως προσθετικής συνάρτησης είναι η συνάρτηση $\Omega(n)$ η οποία ορίζεται ως το πλήθος όλων των πρώτων που διαιρούν τον n. Δηλαδή, αν $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού n, τότε εξ ορισμού $\Omega(n) = k_1 + k_2 + \ldots + k_r$. Πλήρως προσθετική είναι φυσικά και η συνάρτηση $f(n) = \log n$, ο περιορισμός δηλαδή της συνήθους συνάρτησης «λογάριθμος» στους φυσικούς. Οι πρώτες τιμές των συναρτήσεων ω και Ω φαίνονται στον Πίνακα 14.1.1.

Πίνακας 14.1.1: Οι αρχικές τιμές των συναρτήσεων ω και Ω

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\omega(n)$	0	1	1	1	1	2	1	1	1	2	1	2	1	2	2	1	1	2
$\Omega(n)$	0	1	1	2	1	2	1	3	2	2	1	3	1	2	2	4	1	3

Αν και δεν θα επιμείνουμε στις (πλήρως) προσθετικές συναρτήσεις, σημειώνουμε ότι αν η f είναι μία πλήρως προσθετική συνάρτηση τότε η f είναι αυτόματα προσθετική. Επίσης, είναι εύκολη απόρροια των ορισμών ότι αν η f είναι προσθετική, τότε $f(1) = 0$. Παρατηρήστε (ή δείτε το ως άσκηση, αν προτιμάτε) ότι για τις συναρτήσεις «ωμέγα» που ορίσαμε παραπάνω ισχύει ότι $\omega(n) = \Omega(n)$ αν και μόνο αν ο n είναι ελεύθερος τετραγώνων. Τέλος, αν $f(n)$ είναι μία (πλήρως) προσθετική συνάρτηση και $a > 0$ ένας σταθερός πραγματικός, τότε η $a^{f(n)}$ είναι (πλήρως) πολλαπλασιαστική. Η δε $\log g(n)$ είναι (πλήρως) προσθετική, εφ' όσον η $g(n)$ είναι (πλήρως) πολλαπλασιαστική.

Ας δούμε τώρα μερικές εφαρμογές.

Εφαρμογή 14.1.6. Θα δείξουμε ότι

$$\left(\frac{1}{2}\right)^{\omega(n)} \tau(n)^2 < F(n) \leqslant \left(\frac{3}{4}\right)^{\omega(n)} \tau(n)^2, \tag{14.1.4}$$

όπου $F(n) = \sum_{d|n} \tau(d)$.

Παρατηρούμε αρχικά ότι η $F(n)$ είναι αθροιστική συνάρτηση της πολλαπλασιαστικής συνάρτησης τ, άρα και η ίδια πολλαπλασιαστική, χάριν του Θεωρήματος 14.1.3.

Για n δύναμη πρώτου, έχουμε $n = p^a$, οπότε

$$F(p^a) = \sum_{d|p^a} \tau(d) = \sum_{i=0}^{a} \tau(p^i) = \sum_{i=0}^{a} (i+1) = \frac{(a+1)(a+2)}{2} = \frac{a^2+3a+2}{2}.$$

Βλέπουμε τώρα ότι

$$\frac{1}{2}\tau(p^a)^2 = \frac{(a+1)^2}{2} = \frac{a^2+2a+1}{2} < F(p^a) = \frac{a^2+3a+2}{2} \leqslant \frac{3(a+1)^2}{4} = \frac{3}{4}\tau(p^a)^2.$$

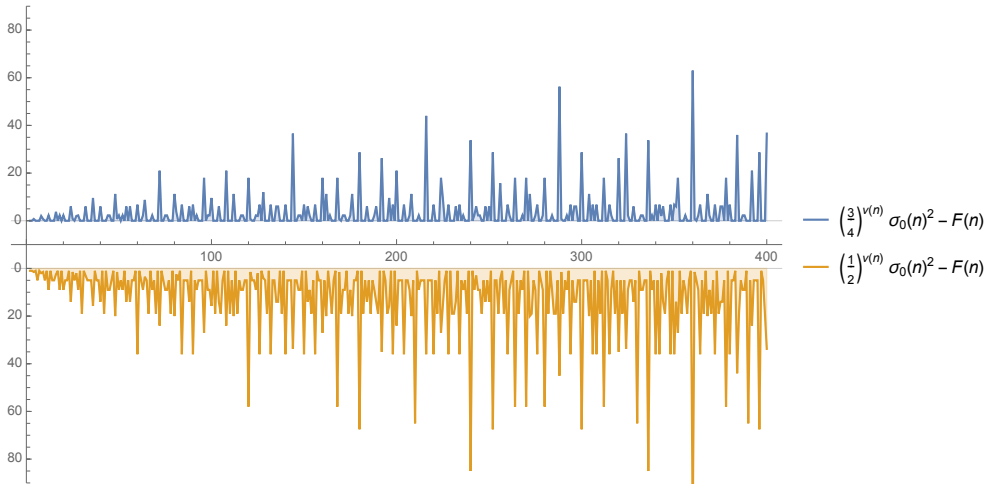
Αν τώρα $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού n, τότε

$$\prod_{i=1}^{r}\left(\frac{1}{2}\tau(p_i^{k_i})^2\right) < F(n) \leqslant \prod_{i=1}^{r}\left(\frac{3}{4}\tau(p_i^{k_i})^2\right),$$

δηλαδή

$$\left(\frac{1}{2}\right)^r \tau(n)^2 < F(n) \leqslant \left(\frac{3}{4}\right)^r \tau(n)^2.$$

Το ζητούμενο έχει δειχθεί εφ' όσον $\omega(n) = r$. ■



Σχήμα 14.1: Οι διαφορές που ορίζουν οι συναρτήσεις στην (14.1.4)

Παρατηρήστε ότι οι σταθερές $c_1 = 1/2$ και $c_2 = 3/4$ στην ανισότητα (14.1.4) είναι οι καλύτερες δυνατές. Συγκεκριμένα, η δεξιά ανισότητα είναι ισότητα για n ελεύθερο τετραγώνων, ενώ η $c_1 = 1/2$ στην αριστερή ανισότητα είναι αδύνατο να βελτιωθεί, αφού

$$\inf\left\{\frac{a^2+3a+2}{2(a+1)^2} : a \in \mathbb{N}\right\} = \frac{1}{2}.$$

Οι παρατηρήσεις αυτές αποτυπώνονται και στο Σχήμα 14.1.

Στην επόμενη εφαρμογή δίνουμε μία ικανή και αναγκαία συνθήκη ώστε να είναι μία αριθμητική συνάρτηση πολλαπλασιαστική.

Εφαρμογή 14.1.7. Θα δείξουμε ότι μία αριθμητική συνάρτηση f τέτοια ώστε $f(1) = 1$, είναι πολλαπλασιαστική, αν και μόνο αν για κάθε δύο φυσικούς m, n ισχύει ότι

$$f(\gcd(m,n))f(\operatorname{lcm}(m,n)) = f(m)f(n). \tag{14.1.5}$$

Έστω $m = p_1^{j_1}\cdots p_r^{j_r}$ και $n = p_1^{k_1}\cdots p_r^{k_r}$ φυσικοί, όπου κάποιοι από τους j_i, k_i ενδέχεται να είναι 0. Τότε

$$\gcd(m,n) = p_1^{\min\{j_1,k_1\}}\cdots p_r^{\min\{j_r,k_r\}}$$

και

$$\operatorname{lcm}(m,n) = p_1^{\max\{j_1,k_1\}} \cdots p_r^{\max\{j_r,k_r\}}$$

σύμφωνα με τις εξηγήσεις που είχαμε δώσει στις παραγράφους πριν την Εφαρμογή 4.2.4.

Αν τώρα η f είναι πολλαπλασιαστική, τότε

$$f(\gcd(m,n))f(\operatorname{lcm}(m,n)) = f(p_1^{\min\{j_1,k_1\}}) \cdots f(p_r^{\min\{j_r,k_r\}}) \cdot f(p_1^{\max\{j_1,k_1\}}) \cdots f(p_r^{\max\{j_r,k_r\}}).$$

Έστω ℓ φυσικός τέτοιος ώστε $1 \leqslant \ell \leqslant r$. Εξετάζουμε τι συμβαίνει με τον παράγοντα p_ℓ και τον εκθέτη του. Στο αριστερό μέλος της (14.1.5) η συνεισφορά του p_ℓ είναι

$$f(p_\ell^{\min\{j_\ell,k_\ell\}})f(p_\ell^{\max\{j_\ell,k_\ell\}}),$$

ενώ στο δεξί μέλος της (14.1.5) η συνεισφορά του p_ℓ είναι

$$f(p_\ell^{j_\ell})f(p_\ell^{k_\ell}).$$

Οι δύο αυτές ποσότητες είναι ίσες, άρα η f ικανοποιεί την (14.1.5).

Αντίστροφα, αν οι φυσικοί m, n είναι σχετικά πρώτοι και η f ικανοποιεί την (14.1.5), τότε $\operatorname{lcm}(m,n) = mn$ από το Θεώρημα 3.2.2. Επομένως

$$f(mn) = 1 \cdot f(mn) = f(1) \cdot f(mn) = f(\gcd(m,n))f(\operatorname{lcm}(m,n)) = f(m)f(n)$$

και άρα η f είναι πολλαπλασιαστική, όπως ακριβώς είχαμε ισχυριστεί. ■

14.2 Ασκήσεις

Άσκηση 14.2.1. Έστω g η αριθμητική συνάρτηση η οποία, για κάθε φυσικό n, ορίζεται από τον τύπο

$$g(n) = \begin{cases} 2 & \text{αν } n \equiv 0 \pmod 3, \\ 1 & \text{αν } n \equiv 1 \pmod 3, \\ 3 & \text{αν } n \equiv 2 \pmod 3. \end{cases}$$

Είναι η g πολλαπλασιαστική συνάρτηση;

Λύση. Όχι. Έχουμε για παράδειγμα $g(6) = 2 \neq 3 \cdot 2 = g(2) \cdot g(3)$. ■

Άσκηση 14.2.2. Μία συνάρτηση f καλείται *ισχυρά πολλαπλασιαστική* αν είναι πολλαπλασιαστική και επιπλέον ισχύει ότι $f(p^a) = f(p)$ για κάθε πρώτο p και κάθε φυσικό a. Ποιες από τις παρακάτω συναρτήσεις

$$\gamma(n) = \prod_{p|n} p, \qquad \sigma_2(n) = \sum_{d|n} d^2, \qquad g(n) = 2^{\omega(n)}$$

είναι ισχυρά πολλαπλασιαστικές;

Λύση. Η συνάρτηση $\sigma_2(n)$ *είναι* πολλαπλασιαστική (γιατί;), αλλά $\sigma_2(3) = 1^2 + 3^2 = 10$, ενώ $\sigma_2(3^2) = 1^2 + 3^2 + 9^2 = 91$. Επομένως η $\sigma_2(n)$ δεν είναι ισχυρά πολλαπλασιαστική.

Εξετάζουμε τώρα την συνάρτηση $\gamma(n)$. Έχουμε αρχικά ότι αν $\gcd(m,n) = 1$, τότε το σύνολο των πρώτων που διαιρούν τον mn είναι η ξένη ένωση του συνόλου των πρώτων που διαιρούν

τον m και του συνόλου των πρώτων που διαιρούν τον n. Αυτό ισχύει γιατί αν $p \mid mn$, τότε $p \mid m$ ή $p \mid n$ από το Θεώρημα 4.1.2 και εφ' όσον οι m, n είναι σχετικά πρώτοι, συμβαίνει ακριβώς ένα από τα δύο.

Επομένως

$$\gamma(mn) = \prod_{p|mn} p = \prod_{p|m} p \cdot \prod_{p|n} p = \gamma(m) \cdot \gamma(n)$$

και άρα η γ είναι πολλαπλασιαστική. Το ότι η γ είναι ισχυρά πολλαπλασιαστική φαίνεται άμεσα. Το γινόμενο όλων των πρώτων που διαιρούν μία δύναμη πρώτου p^a, ισούται με $p = \gamma(p)$, εφ' όσον ο μόνος πρώτος που διαιρεί τον p^a είναι ο πρώτος p.

Για την συνάρτηση $g(n) = 2^{\omega(n)}$ μπορούμε να πούμε ότι είναι πολλαπλασιαστική, εφ' όσον η $\omega(n)$ είναι αθροιστική και σύμφωνα με τις παρατηρήσεις της τελευταίας παραγράφου πριν από την Εφαρμογή 14.1.6. Ισχύει δε ότι $g(p^a) = 2^1 = g(p)$, αφού $\omega(p^a) = \omega(p) = 1$ για κάθε πρώτο p και κάθε φυσικό a. ■

Άσκηση 14.2.3. Έστω f αριθμητική συνάρτηση η οποία είναι ταυτόχρονα πλήρως πολλαπλασιαστική και ισχυρά πολλαπλασιαστική. Ισχύει ότι το σύνολο $f(\mathbb{N}) = \{f(n) : n \in \mathbb{N}\}$ έχει το πολύ δύο στοιχεία;

Λύση. Ναι. Αν p πρώτος και k φυσικός, τότε

$$f(p) = f(p^k) = (f(p))^k,$$

όπου για την πρώτη ισότητα χρησιμοποιούμε ότι η f είναι ισχυρά πολλαπλασιαστική και για την δεύτερη ότι είναι πλήρως πολλαπλασιαστική.

Προκύπτει λοιπόν ότι αν $f(p) \neq 0$ και $k = 2$, τότε $f(p) = 1$ και άρα $f(p) \in \{0, 1\}$ για κάθε πρώτο p. Παρατηρήστε τώρα ότι η τιμή της f σε έναν φυσικό προσδιορίζεται πλήρως από τις τιμές $f(p)$. Είμαστε σε θέση επομένως να συμπεράνουμε ότι $\{f(n) : n \in \mathbb{N}\} \subseteq \{0, 1\}$, όπως θέλαμε να δείξουμε. ■

Άσκηση 14.2.4. Να αποδείξετε ότι το γινόμενο και το πηλίκο (όταν αυτό ορίζεται) δύο πολλαπλασιαστικών συναρτήσεων είναι πολλαπλασιαστικές συναρτήσεις.

Απόδειξη. Έστω f, g πολλαπλασιαστικές συναρτήσεις και m, n φυσικοί τέτοιοι ώστε $\gcd(m, n) = 1$. Έχουμε τότε

$$\begin{aligned}(f \cdot g)(mn) = f(mn)g(mn) &= [f(m)f(n)] \cdot [g(m)g(n)] \\ &= [f(m)g(m)] \cdot [f(n)g(n)] \\ &= (f \cdot g)(m) \cdot (f \cdot g)(n),\end{aligned}$$

επομένως η $f \cdot g$ είναι όντως πολλαπλασιαστική. Με εντελώς ανάλογο τρόπο, δείχνουμε ότι η f/g είναι επίσης πολλαπλασιαστική συνάρτηση. Αρκεί να υποθέσουμε ότι το πηλίκο είναι καλώς ορισμένη συνάρτηση, δηλαδή $g(n) \neq 0$ για κάθε φυσικό n. ■

Άσκηση 14.2.5. Έστω f πολλαπλασιαστική συνάρτηση και k φυσικός τέτοιος ώστε $f(k) \neq 0$. Να αποδείξετε ότι η αριθμητική συνάρτηση g που ορίζεται από τον τύπο

$$g(n) = \frac{f(kn)}{f(k)},$$

όπου n φυσικός, είναι επίσης πολλαπλασιαστική.

Υπόδειξη: Χρησιμοποιήστε αυτό που δείξαμε στην Εφαρμογή 14.1.7.

Απόδειξη. Έστω m, n σχετικά πρώτοι φυσικοί. Χρησιμοποιούμε αυτό που δείξαμε στην Εφαρμογή 14.1.7 και το δεδομένο ότι η f είναι πολλαπλασιαστική, για να γράψουμε

$$f(km)f(kn) = f(\gcd(km, kn))f(\operatorname{lcm}(km, kn)). \tag{14.2.1}$$

Παρατηρούμε τώρα ότι

$$f(\gcd(km, kn)) = f(k\gcd(m, n)) = f(k),$$

όπου η πρώτη ισότητα είναι πόρισμα του Θεωρήματος 3.1.4, ενώ η δεύτερη προκύπτει από την υπόθεση ότι οι m, n είναι σχετικά πρώτοι.

Έχουμε ακόμα το εξής:

$$\operatorname{lcm}(km, kn) = \frac{km \cdot kn}{\gcd(km, kn)} = \frac{k^2mn}{k} = kmn,$$

όπου στην πρώτη ισότητα έχουμε χρησιμοποιήσει το Θεώρημα 3.2.2. Η (14.2.1) επομένως ξαναγράφεται ως

$$f(km)f(kn) = f(k)f(kmn).$$

Συμπεραίνουμε λοιπόν ότι

$$g(m) \cdot g(n) = \frac{f(km)}{f(k)} \cdot \frac{f(kn)}{f(k)} = \frac{f(kmn)}{f(k)} = g(mn),$$

που σημαίνει ότι η g είναι πολλαπλασιαστική. ■

Άσκηση 14.2.6. Να δειχθεί ότι για κάθε φυσικό n ισχύει η ισότητα $\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d)\right)^2$.

Υπόδειξη: Δείξτε ότι και η συνάρτηση του δεξιού μέλους και αυτή του αριστερού είναι πολλαπλασιαστικές συναρτήσεις. Η Άσκηση 1.3.3 είναι σχετική.

Απόδειξη. Θεωρούμε πρώτα την συνάρτηση $f(n) = \sum_{d|n} \tau(d)^3$. Έχουμε αρχικά ότι η $\tau(n)^3$ είναι πολλαπλασιαστική συνάρτηση ως γινόμενο πολλαπλασιαστικών συναρτήσεων. Συγκεκριμένα, η $\tau(n)$ είναι πολλαπλασιαστική από το Πόρισμα 14.1.4, ενώ η $\tau(n)^3$ είναι πολλαπλασιαστική από την Άσκηση 14.2.4. Η δε $f(n)$ είναι πολλαπλασιαστική επειδή είναι αθροιστική συνάρτηση πολλαπλασιαστικής συνάρτησης.

Με παρόμοιο επιχείρημα, δείχνουμε ότι η $g(n) = \left(\sum_{d|n} \tau(d)\right)^2$ είναι πολλαπλασιαστική συνάρτηση. Όπως εξηγήσαμε, η $\tau(n)$ είναι πολλαπλασιαστική, ενώ η $\sum_{d|n} \tau(d)$ είναι αθροιστική συνάρτηση πολλαπλασιαστικής συνάρτησης, άρα και η ίδια πολλαπλασιαστική. Προκύπτει τώρα ότι η $g(n)$ είναι πολλαπλασιαστική ως γινόμενο δύο πολλαπλασιαστικών συναρτήσεων.

Με αυτές τις εξηγήσεις, είναι σαφές το εξής: για να δείξουμε την ισότητα μεταξύ των δύο συναρτήσεων, αρκεί να δείξουμε ότι οι συναρτήσεις συμφωνούν σε δυνάμεις πρώτων. Έστω τώρα p πρώτος και a φυσικός.

Έχουμε αρχικά ότι

$$f(p^a) = \sum_{d|p^a} \tau(d)^3 = \sum_{i=0}^{a} \tau(p^i)^3 = \sum_{i=0}^{a} (i+1)^3 = \sum_{j=1}^{a+1} j^3.$$

Επίσης,

$$g(p^a) = \left(\sum_{d|p^a} \tau(d)\right)^2 = \left(\sum_{i=0}^{a} \tau(p^i)\right)^2 = \left(\sum_{i=0}^{a} (i+1)\right)^2 = \left[\frac{(a+1)(a+2)}{2}\right]^2.$$

Προκύπτει τώρα ότι $f(p^a) = g(p^a)$ από την Άσκηση 1.3.3 θέτοντας $n = a+1$. Εφ' όσον οι p και a ήταν τυχαίοι, συμπεραίνουμε ότι οι f, g συμφωνούν σε δυνάμεις πρώτων. Έπεται από αυτό ότι, εφ' όσον οι f, g είναι πολλαπλασιαστικές συναρτήσεις, θα έχουμε $f(n) = g(n)$ για κάθε φυσικό n και άρα το ζητούμενο έχει δειχθεί. ■

Άσκηση 14.2.7. $(*)$ Έστω $f : \mathbb{N} \to \mathbb{N}$ μία γνησίως αύξουσα συνάρτηση τέτοια ώστε $f(2) = 2$ και $f(mn) = f(m)f(n)$ για κάθε δύο φυσικούς m, n που είναι σχετικά πρώτοι. Να δειχθεί ότι η f είναι η ταυτοτική συνάρτηση, δηλαδή $f(n) = n$ για κάθε φυσικό n.

Υπόδειξη: Παρατηρήστε αρχικά ότι μία γνησίως αύξουσα αριθμητική συνάρτηση ικανοποιεί την $f(n+b) \geqslant f(n) + b$ για κάθε ακέραιο $b \geqslant 0$. Δείξτε τώρα ότι $f(3) = 3$ (θέλει λίγη δουλειά αυτό) και εργαστείτε επαγωγικά για να δείξετε ότι $f(2^n+1) = 2^n+1$ για κάθε φυσικό n. Τέλος, παρατηρήστε ότι αν $f(k) = k$ για κάποιον φυσικό k, τότε η μονοτονία της f εξαναγκάζει την $f(m) = m$ για κάθε φυσικό $m \leqslant k$. Το ζητούμενο έπεται από το γεγονός ότι ο k μπορεί να γίνει όσο μεγάλος θέλουμε.

Σημείωση: Η άσκηση αυτή είναι ειδική περίπτωση ενός πολύ γενικότερου θεωρήματος το οποίο οφείλεται (μαντέψτε) στον Erdős. Σύμφωνα με αυτό το θεώρημα, αν η f είναι μία αύξουσα πολλαπλασιαστική αριθμητική συνάρτηση, τότε υπάρχει σταθερά α τέτοια ώστε $f(n) = n^\alpha$ για κάθε φυσικό n. Με άλλα λόγια, μόνο οι «τετριμμένες» (ή προφανείς) πολλαπλασιαστικές συναρτήσεις είναι αύξουσες.

Απόδειξη. Ξεκινούμε με την εξής απλή παρατήρηση: μία γνησίως αύξουσα αριθμητική συνάρτηση f ικανοποιεί την ανισότητα $f(n) \geqslant n$ για κάθε n φυσικό. Εργαζόμαστε επαγωγικά για να το δείξουμε αυτό. Εφ' όσον η f δεν είναι ταυτοτικά ίση με 0, έχουμε $f(1) = 1$ που μας δίνει την βάση της επαγωγής. Αν τώρα ισχύει ότι $f(n) \geqslant n$, τότε $f(n+1) > f(n) \geqslant n$ και άρα $f(n+1) \geqslant n+1$. Η επαγωγή είναι πλήρης. Συμπεραίνουμε ότι η συνάρτηση f που μας δίνεται στην εκφώνηση της άσκησης, ικανοποιεί την $f(n) \geqslant n$. Με εντελώς παρόμοιο επιχείρημα δείχνουμε ότι $f(n+b) \geqslant f(n) + b$ για κάθε φυσικό b.

Ορίζουμε τώρα τον μη αρνητικό ακέραιο k από την σχέση $f(3) = k+3$ και χρησιμοποιούμε ότι η f είναι γνήσια αύξουσα και πολλαπλασιαστική για να γράψουμε διαδοχικά τις εξής σχέσεις:

$$\begin{aligned}
f(6) &= f(2)f(3) = 6 + 2k, \\
f(5) &\leqslant 5 + 2k, \\
f(10) &= f(2)f(5) \leqslant 10 + 4k, \\
f(9) &\leqslant 9 + 4k, \\
f(18) &= f(2)f(9) \leqslant 18 + 8k, \\
f(15) &\leqslant 15 + 8k.
\end{aligned} \tag{14.2.2}$$

Από την άλλη, έχουμε $f(3) = k+3$ και άρα $f(5) \geqslant 5 + k$. Επομένως

$$f(15) = f(3)f(5) \geqslant 15 + 8k + k^2. \tag{14.2.3}$$

Από τις (14.2.2) και (14.2.3) βλέπουμε ότι $k = 0$ και άρα $f(3) = f(2^1 + 1) = 3$.

Θα δείξουμε τώρα επαγωγικά ότι για κάθε φυσικό n έχουμε

$$f(2^n + 1) = 2^n + 1. \tag{14.2.4}$$

Έχουμε ήδη δείξει ότι $f(3) = f(2^1 + 1) = 3$, επομένως η βάση της επαγωγής μας ισχύει. Ας υποθέσουμε τώρα ότι η (14.2.4) ισχύει για $n = r$. Τότε

$$f(2^{r+1} + 2) = f(2)f(2^r + 1) = 2(2^r + 1) = 2^{r+1} + 2$$

Εφ' όσον η f είναι γνησίως αύξουσα, έχουμε

$$2^{r+1} + 1 \leqslant f(2^{r+1} + 1) < f(2^{r+1} + 2) = 2^{r+1} + 2,$$

όπου η πρώτη ανισότητα ισχύει από αυτό που δείξαμε στην πρώτη παράγραφο. Συμπεραίνουμε ότι $f(2^{r+1} + 1) = 2^{r+1} + 1$, οπότε η επαγωγή μας έχει ολοκληρωθεί.

Επειδή εξ υποθέσεως η f είναι γνησίως μονότονη, προκύπτει εύκολα ότι αν $f(k) = k$ για κάποιον φυσικό k, τότε $f(m) = m$ για κάθε φυσικό $m \leqslant k$. Το $k = k(n) = 2^n + 1$ μπορεί όμως να γίνει όσο μεγάλο θέλουμε, επομένως έχουμε δείξει το ζητούμενο. ■

Κεφάλαιο 15

15η Παράδοση

Στο σημερινό μάθημα θα εισαγάγουμε μία ξεχωριστή πολλαπλασιαστική συνάρτηση, την συνάρτηση μ του Möbius. Θα δούμε διάφορα παραδείγματα και εφαρμογές και θα αναφερθούμε στον τύπο αντιστροφής του Möbius.

15.1 Η συνάρτηση μ του Möbius

Ξεκινούμε με τον ορισμό της συνάρτησης του Möbius.

Ορισμός 15.1.1. Για έναν φυσικό n, ορίζουμε την συνάρτηση $\mu : \mathbb{N} \to \mathbb{Z}$ μέσω του τύπου

$$\mu(n) = \begin{cases} 1 & \text{αν } n = 1, \\ 0 & \text{αν } p^2 \mid n \text{ για κάποιον πρώτο } p, \\ (-1)^r & \text{αν } n = p_1 p_2 \cdots p_r, \text{ όπου οι } p_i \text{ είναι διακεκριμένοι πρώτοι.} \end{cases}$$

Με άλλα λόγια, η συνάρτηση μ συμπεριφέρεται ως εξής: εάν ο φυσικός n **δεν είναι** ελεύθερος τετραγώνων, τότε $\mu(n) = 0$, ενώ αν ο n **είναι** ελεύθερος τετραγώνων, τότε $\mu(n) = \pm 1$, ανάλογα με το αν ο n έχει άρτιο ή περιττό πλήθος διακεκριμένων πρώτων διαιρετών.

Επομένως, $\mu(p) = -1$ αν ο p είναι πρώτος, ενώ $\mu(p^k) = 0$ για p πρώτο και $k \geqslant 2$ φυσικό. Μερικές πρώτες τιμές της συνάρτησης μ φαίνονται στον Πίνακα 15.1.1.

Πίνακας 15.1.1: Οι αρχικές τιμές της συνάρτησης μ

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1	1	0	-1	0

Ως πρώτο βασικό αποτέλεσμα για την συνάρτηση μ θα δείξουμε ότι είναι πολλαπλασιαστική.

Θεώρημα 15.1.2. *Η συνάρτηση μ είναι πολλαπλασιαστική.*

Απόδειξη. Θέλουμε να δείξουμε ότι $\mu(mn) = \mu(m)\mu(n)$ αν $\gcd(m, n) = 1$. Σε περίπτωση που υπάρχει πρώτος p τέτοιος ώστε είτε $p^2 \mid m$ είτε $p^2 \mid n$, θα έχουμε $p^2 \mid mn$ και άρα

$$\mu(mn) = 0 = \mu(m)\mu(n),$$

οπότε ο ισχυρισμός μας ισχύει τετριμμένα σε αυτήν την περίπτωση.

Μπορούμε επομένως να υποθέσουμε ότι οι m, n είναι και οι δύο ελεύθεροι τετραγώνων. Δηλαδή, $m = p_1 p_2 \cdots p_r$ και $n = q_1 q_2 \cdots q_s$, όπου όλοι οι πρώτοι p_i, q_j είναι διακεκριμένοι. Έχουμε τότε ότι

$$\mu(mn) = \mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n),$$

οπότε η απόδειξή μας είναι πλήρης. ■

Εφ' όσον η $\mu(n)$ είναι πολλαπλασιαστική, έπεται από το Θεώρημα 14.1.3 ότι η $\sum_{d|n} \mu(d)$ είναι επίσης πολλαπλασιαστική συνάρτηση. Αυτό το κάνουμε πιο συγκεκριμένο στο επόμενο θεώρημα.

Θεώρημα 15.1.3. *Συμβολίζοντας με $F(n) = \sum_{d|n} \mu(d)$ την αθροιστική συνάρτηση της μ, όπου n φυσικός, έχουμε ότι*

$$F(n) = \begin{cases} 1 & \text{αν } n = 1, \\ 0 & \text{αν } n > 1. \end{cases}$$

Απόδειξη. Είναι σαφές ότι $F(1) = \mu(1) = 1$. Αν τώρα $n > 1$ και $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού n, τότε

$$F(n) = \prod_{i=1}^{r} F(p_i^{k_i}).$$

Αρκεί λοιπόν να υπολογίσουμε την F σε μία δύναμη πρώτου. Έχουμε όμως, για $k \geqslant 1$,

$$\begin{aligned} F(p^k) &= \sum_{d|p^k} \mu(d) \\ &= \mu(1) + \mu(p) + \ldots + \mu(p^k) \\ &= 1 + (-1) + 0 + \ldots + 0 \\ &= 0. \end{aligned}$$

Προκύπτει άμεσα από την παραπάνω σχέση ότι για $n > 1$ έχουμε $F(n) = 0$. ■

Με βάση τον Πίνακα 15.1.1, έχουμε για παράδειγμα

$$\begin{aligned} F(18) &= \mu(1) + \mu(2) + \mu(3) + \mu(6) + \mu(9) + \mu(18) \\ &= 1 + (-1) + (-1) + 1 + 0 + 0 \\ &= 0. \end{aligned}$$

15.2 Αντιστροφή κατά Möbius

Στο επόμενο θεώρημα, το οποίο είναι κεντρικό, διευκρινίζουμε τον ισχυρισμό που κάναμε στον πρόλογο, ότι η συνάρτηση μ έχει ξεχωριστή σημασία.

Θεώρημα 15.2.1 (Τύπος Αντιστροφής του Möbius). *Έστω F και f δύο αριθμοθεωρητικές συναρτήσεις που ικανοποιούν την σχέση*

$$F(n) = \sum_{d|n} f(d).$$

Τότε

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

Απόδειξη. Παρατηρούμε αρχικά ότι η ισότητα μεταξύ των δύο αθροισμάτων

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

ισχύει. Αυτό συμβαίνει διότι μπορούμε να αντικαταστήσουμε τον δείκτη d με τον δείκτη $d' = n/d$. Όπως έχουμε δει και αλλού, καθώς ο d διατρέχει τους διαιρέτες του n, το ίδιο κάνει και ο d'. Αρκεί λοιπόν να δείξουμε ότι

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Κάνουμε τώρα τον εξής χειρισμό:

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{c|(n/d)} f(c) \right) = \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c) \right). \tag{15.2.1}$$

Παρατηρούμε ακόμα ότι $d \mid n$ και $c \mid (n/d)$, αν και μόνο αν $c \mid n$ και $d \mid (n/c)$. Από αυτήν την παρατήρηση έπεται ότι το τελευταίο άθροισμα στην (15.2.1) γράφεται ως

$$\sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c) \right) = \sum_{c|n} \left(\sum_{d|(n/c)} f(c) \mu(d) \right) = \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right). \tag{15.2.2}$$

Σύμφωνα με το Θεώρημα 15.1.3, ο όρος $\sum_{d|(n/c)} \mu(d)$ ισούται με 0 εκτός αν $n/c = 1$, δηλαδή $n = c$, στην οποία περίπτωση ισούται με 1. Επομένως το τελευταίο άθροισμα στην (15.2.2) απλοποιείται

$$\sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d) \right) = \sum_{c=n} f(c) \cdot 1 = f(n)$$

και μας δίνει την ισότητα που θέλαμε να αποδείξουμε. ■

Διασαφηνίζουμε με ένα παράδειγμα πώς ακριβώς λειτουργεί ο «ελιγμός» που περιγράφει η ισότητα (15.2.2). Συγκεκριμένα, για $n = 10$ έχουμε

$$\begin{aligned}
\sum_{d|10} \left(\sum_{c|(10/d)} \mu(d) f(c) \right) &= \mu(1)[f(1) + f(2) + f(5) + f(10)] \\
&\quad + \mu(2)[f(1) + f(5)] + \mu(5)[f(1) + f(2)] + \mu(10) f(1) \\
&= f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] \\
&\quad + f(2)[\mu(1) + \mu(5)] + f(5)[\mu(1) + \mu(2)] + f(10)\mu(1) \\
&= \sum_{c|10} \left(\sum_{d|(10/c)} f(c) \mu(d) \right).
\end{aligned}$$

Ας δούμε τώρα με ένα παράδειγμα πώς λειτουργεί ο τύπος αντιστροφής του Möbius.

Παράδειγμα 15.2.2. Οι συναρτήσεις τ και σ δίνονται από τους τύπους

$$\tau(n) = \sum_{d|n} 1 \qquad \text{και} \qquad \sigma(n) = \sum_{d|n} d.$$

Το Θεώρημα 15.2.1 μας επιτρέπει να γράψουμε

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d) \qquad \text{και} \qquad n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d),$$

όπου και οι δύο ισότητες ισχύουν για κάθε φυσικό n.

Είδαμε στο Θεώρημα 14.1.3 ότι η αθροιστική συνάρτηση μιας πολλαπλασιαστικής συνάρτησης είναι και η ίδια πολλαπλασιαστική. Μπορούμε (και πρέπει) να ρωτήσουμε κατά πόσο ισχύει το αντίστροφο. Δηλαδή, αν ισχύει ότι η $\sum_{d|n} f(d)$ είναι πολλαπλασιαστική συνάρτηση, έπεται ότι η f είναι επίσης πολλαπλασιαστική; Στο επόμενο θεώρημα δίνουμε απάντηση σε αυτό ακριβώς το ερώτημα.

Θεώρημα 15.2.3. *Αν η F είναι πολλαπλασιαστική συνάρτηση, όπου*

$$F(n) = \sum_{d|n} f(d),$$

τότε η f είναι επίσης πολλαπλασιαστική συνάρτηση.

Απόδειξη. Έστω m, n σχετικά πρώτοι φυσικοί. Υπενθυμίζουμε ότι, σύμφωνα με το Λήμμα 14.1.2, κάθε διαιρέτης d του mn γράφεται με μοναδικό τρόπο ως $d = d_1 d_2$, όπου $d_1 \mid m$, $d_2 \mid n$ και $\gcd(d_1, d_2) = 1$.

Χρησιμοποιώντας το Θεώρημα 15.2.1, είμαστε σε θέση να γράψουμε

$$\begin{aligned}
f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\
&= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\
&= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\
&= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\
&= f(m) f(n).
\end{aligned}$$

Εφ' όσον $f(mn) = f(m)f(n)$ για κάθε δύο σχετικά πρώτους m, n, συμπεραίνουμε ότι η f είναι πολλαπλασιαστική συνάρτηση, όπως ακριβώς ζητούσαμε να δείξουμε. ∎

Εφαρμογή 15.2.4. Έστω f πολλαπλασιαστική συνάρτηση που δεν είναι ταυτοτικά ίση με 0. Θα δείξουμε ότι

$$\sum_{d|n} \mu(d)f(d) = \prod_{i=1}^{r}[1 - f(p_i)], \tag{15.2.3}$$

όπου $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού n.

Γνωρίζουμε από το Θεώρημα 15.1.2 ότι η μ είναι πολλαπλασιαστική συνάρτηση, ενώ εξ υποθέσεως η f είναι επίσης πολλαπλασιαστική. Χρησιμοποιώντας την Άσκηση 14.2.4 προκύπτει ότι το γινόμενο μf είναι πολλαπλασιαστική συνάρτηση και άρα η αθροιστική συνάρτηση

$$F(n) = \sum_{d|n} \mu(d)f(d)$$

είναι με την σειρά της πολλαπλασιαστική, χάριν του Θεωρήματος 14.1.3.

Είναι αρκετό επομένως να δείξουμε ότι $F(p^a) = 1 - f(p)$. Έχουμε όμως

$$F(p^a) = \sum_{d|p^a} \mu(d)f(d) = \sum_{i=0}^{a} \mu(p^i)f(p^i) = \mu(1)f(1) + \mu(p)f(p) = 1 - f(p).$$

Η τρίτη ισότητα στην ανωτέρω σχέση προκύπτει από το γεγονός ότι $\mu(p^b) = 0$ για $b \geqslant 2$, ενώ η τελευταία ισότητα είναι απόρροια των σχέσεων $\mu(1) = 1$, $\mu(p) = -1$ και $f(1) = 1$· η τελευταία είναι ισοδύναμη με την αρχική συνθήκη ότι η f δεν είναι ταυτοτικά ίση με 0. ■

15.3 Η συνάρτηση του Mertens

Ορίζουμε, για κάθε φυσικό n, το άθροισμα

$$M(n) = \sum_{k=1}^{n} \mu(k).$$

Η συνάρτηση $M(n)$ εκφράζει την διαφορά μεταξύ του αριθμού των φυσικών $k \leqslant n$ που είναι ελεύθεροι τετραγώνων και έχουν άρτιο πλήθος πρώτων παραγόντων, και του αριθμού των φυσικών $k \leqslant n$ που είναι ελεύθεροι τετραγώνων αλλά έχουν περιττό πλήθος πρώτων παραγόντων.

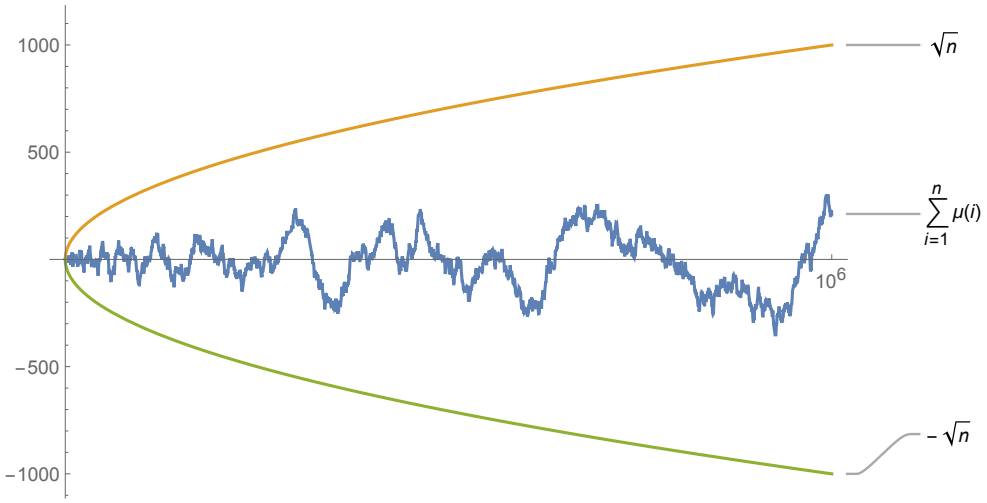
Ο Ολλανδός Thomas Joannes Stieltjes $(1856 - 1894)$ ισχυρίστηκε το 1885 ότι η συνάρτηση $M(n)/\sqrt{n}$ είναι φραγμένη, χωρίς όμως να δημοσιεύσει ποτέ απόδειξη αυτού του ισχυρισμού. Ο Πολωνός Franz Mertens $(1840 - 1927)$ εξέδωσε το 1897 ένα άρθρο με έναν 50σέλιδο πίνακα τιμών της $M(n)$, για $n = 1, 2 \ldots, 10000$. Με βάση τον πίνακα αυτό, ο Mertens κατέληγε ότι η ανισότητα

$$|M(n)| < \sqrt{n} \tag{15.3.1}$$

για $n > 1$ είναι «εξαιρετικά πιθανή».

Το Σχήμα 15.1 τεκμηριώνει ακόμη ισχυρότερα το συμπέρασμα του Mertens για $n \leqslant 10^6$. Η (15.3.1) έμεινε τελικά γνωστή ως «Εικασία του Mertens», ενώ η συνάρτηση $M(n)$ ως «συνάρτηση του Mertens».

Η Εικασία του Mertens μάλιστα επιβεβαιώθηκε με χρήση υπολογιστή το 1963 για $n \leqslant 10^{10}$. Παρ' όλες τις διάφορες αυτές πανίσχυρες ενδείξεις ότι η Εικασία του Mertens είναι αληθής,



Σχήμα 15.1: Η συνάρτηση του Mertens για $n \leqslant 10^6$

οι Andrew Odlyzko και Herman te Riele έδειξαν το 1984 ότι η Εικασία του Mertens δεν ισχύει!

Η απόδειξη των Odlyzko και te Riele, η οποία περιλάμβανε χρήση υπολογιστή και βασιζόταν στον αλγόριθμο LLL, ήταν «έμμεση»· δηλαδή δεν έδινε συγκεκριμένη τιμή του n για την οποία συμβαίνει $|M(n)| \geqslant \sqrt{n}$. Η απόδειξή τους απλώς εξασφάλιζε την ύπαρξη ενός φυσικού n για τον οποίο η (15.3.1) αντιστρέφεται. Το μόνο που έχουμε καταφέρει να δείξουμε έκτοτε, σε ό,τι έχει σχέση με τον πρώτο φυσικό n_0 για τον οποίο ισχύει ότι $|M(n_0)| \geqslant \sqrt{n_0}$, είναι ότι

$$n_0 \lessapprox 10^{1.69 \times 10^{39}},$$

χωρίς όμως να γνωρίζουμε καμία συγκεκριμένη τιμή του n_0.

15.4 Ασκήσεις

Άσκηση 15.4.1. Να υπολογίσετε τις ακόλουθες τιμές της συνάρτησης μ:

$$\mu(105), \qquad \mu(110), \qquad \mu(740), \qquad \mu(999), \qquad \mu(3 \cdot 7 \cdot 13 \cdot 19 \cdot 23), \qquad \mu(10!/(5!)^2).$$

Λύση. Έχουμε

$$\begin{aligned}
\mu(105) &= \mu(3 \cdot 5 \cdot 7) = (-1)^3 = -1, \\
\mu(110) &= \mu(2 \cdot 5 \cdot 11) = (-1)^3 = -1, \\
\mu(740) &= \mu(2^2 \cdot 5 \cdot 37) = 0, \\
\mu(999) &= \mu(3^3 \cdot 37) = 0, \\
\mu(3 \cdot 7 \cdot 13 \cdot 19 \cdot 23) &= (-1)^5 = -1, \\
\mu(10!/(5!)^2) &= \mu(2^2 \cdot 3^2 \cdot 7) = 0.
\end{aligned}$$

Είναι σαφές ότι για κάποιες από τις ανωτέρω ισότητες θα αρκούσε απλά να επισημάνουμε ότι ο αριθμός δεν είναι ελεύθερος τετραγώνων αντί να τον παραγοντοποιήσουμε πλήρως. ■

Άσκηση 15.4.2. Να δειχθεί ότι

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

για κάθε φυσικό n.

Απόδειξη. Οι $n, n+1, n+2, n+3$ είναι τέσσερις διαδοχικοί φυσικοί, επομένως ένας ακριβώς εξ αυτών διαιρείται με τον 4. Συμπεραίνουμε ότι ένας τουλάχιστον από τους παράγοντες του γινομένου $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)$ είναι ίσος με 0 και άρα

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0,$$

όπως θέλαμε να δείξουμε. ■

Άσκηση 15.4.3. Χρησιμοποιώντας αυτό που δείξαμε στην Εφαρμογή 15.2.4 (ή αλλιώς) βρείτε έναν απλό τύπο για τις παρακάτω εκφράσεις, όπου σε κάθε μία υποθέτουμε ότι $n > 1$:

(i) $\sum_{d|n} d\mu(d)$,

(ii) $\sum_{d|n} \mu(d)/d$,

(iii) $\sum_{d|n} \mu(d)\tau(d)$,

(iv) $\sum_{d|n} \mu(d)\sigma(d)$.

Λύση. Υποθέτουμε ότι η κανονική μορφή του φυσικού n είναι $n = p_1^{k_1} \cdots p_r^{k_r}$.

(i) Παίρνοντας $f(n) = n$ στην (15.2.3) έχουμε ότι

$$\sum_{d|n} d\mu(d) = \prod_{i=1}^{r}(1 - p_i).$$

(ii) Εδώ παίρνουμε $f(n) = 1/n$ στην (15.2.3), το οποίο μας δίνει

$$\sum_{d|n} \mu(d)/d = \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$

(iii) Παίρνουμε $f(n) = \tau(n)$ στην (15.2.3) και έχουμε

$$\sum_{d|n} \mu(d)\tau(d) = \prod_{i=1}^{r}(1 - \tau(p_i)) = \prod_{i=1}^{r}(1-2) = (-1)^r.$$

(iv) Παίρνουμε $f(n) = \sigma(n)$ στην (15.2.3) και αυτό μας δίνει

$$\sum_{d|n} \mu(d)\sigma(d) = \prod_{i=1}^{r}(1 - \sigma(p_i)) = \prod_{i=1}^{r}(1 - p_i - 1) = (-1)^r \prod_{i=1}^{r} p_i.$$

Σε κάθε περίπτωση έχουμε βρει τύπους για τις διάφορες εκφράσεις, οπότε η λύση μας είναι πλήρης. ■

Άσκηση 15.4.4. Να αποδείξετε τους ακόλουθους τύπους για κάθε φυσικό n:

(i) $\sum_{d|n} \mu(d)^2 = 2^{\omega(n)}$.

(ii) $\sum_{d|n} \mu(d) 2^{\omega(n/d)} = \mu(n)^2$.

Απόδειξη. (i) Γνωρίζουμε ότι η συνάρτηση μ είναι πολλαπλασιαστική, επομένως μπορούμε να εφαρμόσουμε την (15.2.3) με την επιλογή $f = \mu$ και να πάρουμε

$$\sum_{d|n} \mu(d)^2 = \prod_{i=1}^{r} [1 - \mu(p_i)] = \prod_{i=1}^{r} [1 - (-1)] = 2^r,$$

όπου $n = p_1^{k_1} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού n. Το ζητούμενο προκύπτει από την παρατήρηση ότι $r = \omega(n)$.

(ii) Εφαρμόζουμε το Θεώρημα 15.2.1 στις συναρτήσεις

$$f(n) = \mu(n)^2 \qquad \text{και} \qquad F(n) = \sum_{d|n} \mu(d)^2 = 2^{\omega(n)},$$

όπου η δεύτερη ισότητα στην τελευταία σχέση ισχύει λόγω του (i), και παίρνουμε

$$\mu(n)^2 = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(d) 2^{\omega(n/d)},$$

που είναι ακριβώς η ζητούμενη ισότητα. ■

Άσκηση 15.4.5. Για έναν φυσικό n, ορίζουμε την συνάρτηση $\Lambda : \mathbb{N} \to \mathbb{R}$ μέσω του τύπου

$$\Lambda(n) = \begin{cases} \log p & \text{αν } n = p^k \text{ όπου } p \text{ πρώτος και } k \text{ φυσικός,} \\ 0 & \text{διαφορετικά.} \end{cases}$$

Η συνάρτηση Λ είναι γνωστή και ως **συνάρτηση του von Mangoldt**. Να δειχθούν οι παρακάτω προτάσεις:

(i) Η συνάρτηση Λ δεν είναι ούτε πολλαπλασιαστική ούτε προσθετική.

(ii) Για n φυσικό ισχύει ότι $\sum_{d|n} \Lambda(d) = \log n$.

(iii) Για n φυσικό ισχύει ότι $\Lambda(n) = -\sum_{d|n} \mu(d) \log d$.

Απόδειξη. (i) Έχουμε εξ ορισμού ότι $\Lambda(6) = 0$, ενώ

$$\Lambda(2) + \Lambda(3) = \log 2 + \log 3 = \log 6 \neq 0,$$

άρα η Λ δεν είναι προσθετική. Επίσης,

$$\Lambda(2) \cdot \Lambda(3) = \log 2 \cdot \log 3 \neq 0,$$

άρα η Λ δεν είναι ούτε πολλαπλασιαστική.

(ii) Έστω ότι $n = p_1^{k_1} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού n. Εφ' όσον $\Lambda(d) = 0$ εκτός αν ο d είναι δύναμη πρώτου, μπορούμε να γράψουμε

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{d|p_i^{k_i}} \Lambda(d) = \sum_{i=1}^{r} \sum_{j=1}^{k_i} \Lambda(p_i^j) = \sum_{i=1}^{r} \sum_{j=1}^{k_i} \log(p_i)$$
$$= \sum_{i=1}^{r} k_i \log(p_i) = \sum_{i=1}^{r} \log\left(p_i^{k_i}\right) = \log n.$$

(iii) Εφαρμόζουμε το Θεώρημα 15.2.1 στις συναρτήσεις

$$f(n) = \Lambda(n) \qquad \text{και} \qquad F(n) = \sum_{d|n} \Lambda(d) = \log n,$$

όπου η δεύτερη ισότητα στην τελευταία σχέση ισχύει λόγω του (ii), και παίρνουμε

$$\Lambda(n) = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(d) \log(n/d) = \sum_{d|n} \mu(d)(\log n - \log d)$$
$$= \log n \cdot \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = -\sum_{d|n} \mu(d) \log d.$$

Η τελευταία ισότητα ισχύει επειδή η συνάρτηση

$$\log n \cdot \sum_{d|n} \mu(d)$$

είναι ταυτοτικά ίση με 0. Για $n = 1$ αυτό είναι προφανές αφού $\log 1 = 0$, ενώ για $n > 1$ το Θεώρημα 15.1.3 μας δίνει ότι $\sum_{d|n} \mu(d) = 0$. Η απόδειξή μας είναι πλήρης. ■

Άσκηση 15.4.6. Αληθεύουν οι παρακάτω δύο προτάσεις;

(i) Υπάρχουν άπειροι φυσικοί n τέτοιοι ώστε $\mu(n) + \mu(n+1) = 0$.

(ii) Υπάρχουν άπειροι φυσικοί n τέτοιοι ώστε $\mu(n-1) + \mu(n) + \mu(n+1) = 0$.

Λύση. (i) Η απάντηση είναι **ναι**. Για κάθε φυσικό k, οι $n = 36k + 8$ και $n + 1 = 36k + 9$ είναι διαδοχικοί φυσικοί, ενώ ταυτόχρονα $2^2 = 4 \mid n$ και $3^2 = 9 \mid n + 1$. Επομένως

$$\mu(36k + 8) + \mu(36k + 9) = 0 + 0 = 0.$$

(ii) Η απάντηση είναι **ναι** και εδώ. Αν ο n είναι κοινή λύση του συστήματος ισοτιμιών

$$\begin{cases} x \equiv -1 \pmod 4 \\ x \equiv \ \ 0 \pmod 9 \\ x \equiv \ \ 1 \pmod{25}, \end{cases}$$

τότε $4 \mid (n+1)$, $9 \mid n$ και $25 \mid (n-1)$. Άρα κανένας εκ των $n-1, n, n+1$ δεν είναι ελεύθερος τετραγώνων, που σημαίνει ότι

$$\mu(n-1) + \mu(n) + \mu(n+1) = 0 + 0 + 0 = 0.$$

Το ότι το σύστημα ισοτιμιών επιδέχεται κοινή λύση είναι απόρροια του Κινέζικου Θεωρήματος Υπολοίπων. Η μοναδική λύση του συστήματος είναι η

$$n \equiv 351 \pmod{900},$$

επομένως υπάρχουν άπειροι n με την ιδιότητα που ψάχνουμε. ■

Άσκηση 15.4.7. Για έναν φυσικό n, ορίζουμε την συνάρτηση $\lambda : \mathbb{N} \to \mathbb{Z}$ μέσω του τύπου

$$\lambda(n) = \begin{cases} 1 & \text{αν } n = 1, \\ (-1)^{\Omega(n)} & \text{διαφορετικά.} \end{cases}$$

Η συνάρτηση λ είναι γνωστή και ως **συνάρτηση του Liouville**. Να δειχθούν οι παρακάτω προτάσεις:

(i) Η συνάρτηση λ είναι πλήρως πολλαπλασιαστική.

(ii) Για n φυσικό ισχύει ότι

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{αν } n = m^2 \text{ για κάποιον ακέραιο } m, \\ 0 & \text{διαφορετικά.} \end{cases}$$

(iii) $\sum_{d|n} \mu(d)\lambda(d) = 2^{\omega(n)}$ για κάθε φυσικό n.

Απόδειξη. (i) Έχουμε $\lambda(n) = (-1)^{\Omega(n)}$ για $n > 1$, όπου η συνάρτηση $\Omega(n)$ είναι πλήρως προσθετική. Εφ' όσον η $\lambda(n)$ είναι της μορφής $a^{f(n)}$ με f πλήρως προσθετική, προκύπτει ότι η λ είναι πλήρως πολλαπλασιαστική.

(ii) Η αθροιστική συνάρτηση $F(n) = \sum_{d|n} \lambda(d)$ της λ είναι πολλαπλασιαστική αφού, όπως δείξαμε στο (i), η λ είναι (πλήρως) πολλαπλασιαστική. Έχουμε αρχικά ότι $F(1) = 1$. Αν τώρα $n = p_1^{k_1} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού $n > 1$, τότε

$$F(n) = \prod_{i=1}^{r} F(p_i^{k_i}).$$

Επομένως αρκεί να υπολογίσουμε την F σε δυνάμεις πρώτων. Έστω λοιπόν p πρώτος και a φυσικός. Έχουμε τότε

$$F(p^a) = \sum_{i=0}^{a} \lambda(p^i) = 1 + (-1) + 1 + (-1) + \ldots + (-1)^a = \begin{cases} 1 & \text{αν ο } a \text{ είναι άρτιος,} \\ 0 & \text{αν ο } a \text{ είναι περιττός.} \end{cases}$$

Η μόνη περίπτωση επομένως για να μην έχουμε $F(n) = 0$ είναι κάθε εκθέτης k_i να είναι άρτιος. Σε αυτήν την περίπτωση έχουμε $F(n) = 1$ και $n = m^2$, όπου $m = p_1^{k_1/2} \cdots p_r^{k_r/2}$.

(iii) Για $n = 1$ το ζητούμενο ισχύει αφού και τα δύο μέλη είναι ίσα με 1. Αν $n = p_1^{k_1} \cdots p_r^{k_r}$ είναι η κανονική μορφή του φυσικού $n > 1$, χρησιμοποιούμε πάλι αυτό που δείξαμε στην Εφαρμογή 15.2.4 με $f = \lambda$ (η οποία είναι πολλαπλασιαστική από το (i)) και έχουμε

$$\sum_{d|n} \mu(d)\lambda(d) = \prod_{i=1}^{r} [1 - \lambda(p_i)] = \prod_{i=1}^{r} [1 - (-1)] = 2^r = 2^{\omega(n)},$$

όπως ακριβώς ζητούσαμε να δείξουμε. ■

Κεφάλαιο 16

16η Παράδοση

Στο σημερινό μάθημα θα αναφερθούμε στην συνάρτηση ϕ του Euler και θα αποδείξουμε μερικές από τις βασικότερες ιδιότητές της, όπως για παράδειγμα το ότι είναι πολλαπλασιαστική συνάρτηση.

16.1 Euler ο μαθηματικός

Η σημασία του έργου του Fermat δεν έγκειται τόσο στη συμβολή του στα μαθηματικά της εποχής του, όσο στην εμψυχωτική του επίδραση στις μεταγενέστερες γενιές των Μαθηματικών. Ίσως η μεγαλύτερη απογοήτευση του Fermat από την καριέρα του ήταν η αδυναμία του να κεντρίσει το ενδιαφέρον για τη νέα Θεωρία Αριθμών. Χρειάστηκε να περάσει ένας αιώνας, ώσπου ένας μαθηματικός πρώτης τάξης, ο Leonhard Euler (1707 – 1783), να εκτιμήσει τη σημασία του. Πολλά από τα θεωρήματα που ανακοινώθηκαν χωρίς απόδειξη από τον Fermat, υπέκυψαν στις ικανότητες του Euler, και είναι πιθανό ότι τα επιχειρήματα που επινόησε ο Euler δεν ήταν ουσιαστικά διαφορετικά από αυτά του Fermat.

Η κεντρική προσωπικότητα των μαθηματικών του 18ου αι., ο Euler ήταν γιος ενός Λουθηρανού πάστορα που ζούσε κοντά στη Βασιλεία της Ελβετίας. Ο πατέρας του Euler επιθυμούσε ο γιος του να γίνει κληρικός και τον έστειλε, σε ηλικία 13 ετών, στο Πανεπιστήμιο της Βασιλείας για να σπουδάσει Θεολογία. Εκεί ο νεαρός Euler συνάντησε τον Johann Bernoulli - έναν από τους κορυφαίους τότε Μαθηματικούς της Ευρώπης - και έγινε φίλος με τους δύο γιους του, τον Nicolaus και τον Daniel. Σύντομα, ο Euler διέκοψε τις θεολογικές σπουδές, για να ασχοληθεί αποκλειστικά με τα μαθηματικά. Έλαβε το μεταπτυχιακό του το 1723 και το 1727, σε ηλικία 19 ετών, κέρδισε ένα βραβείο από την Ακαδημία Επιστημών του Παρισιού για μια πραγματεία σχετικά με την πιο αποτελεσματική διάταξη των ιστίων των πλοίων.

Ενώ ο 17ος αι. ήταν μια εποχή σπουδαίων ερασιτεχνών μαθηματικών, ο 18ος αι. ήταν σχεδόν αποκλειστικά μια εποχή επαγγελματιών–καθηγητών πανεπιστημίων και μελών επιστημονικών ακαδημιών. Πολλοί μονάρχες απολάμβαναν να θεωρούνται προστάτες της μάθησης και οι Ακαδημίες χρησίμευαν ως πνευματικά κοσμήματα των βασιλικών αυλών. Αν και τα κίνητρα αυτών των ηγεμόνων μπορεί να μην ήταν εντελώς φιλανθρωπικά, γεγονός παραμένει ότι οι επιστημονικές εταιρείες αποτελούσαν σημαντικούς φορείς για την προώθηση της επιστήμης. Παρείχαν μισθούς σε διακεκριμένους μελετητές, δημοσίευαν περιοδικά ερευνητικών εργασιών σε τακτική βάση και προσέφεραν χρηματικά έπαθλα για επιστημονικές ανακαλύψεις. Ο Euler συνδέθηκε σε διαφορετικές χρονικές στιγμές με δύο από τις νεοσύστατες Ακαδημίες, την αυτοκρατορική Ακαδημία στην Αγία Πετρούπολη $(1727 - 1741, 1766 - 1783)$ και την Βασι-

λική Ακαδημία στο Βερολίνο (1741 – 1766). Το 1725, ο Μέγας Πέτρος ίδρυσε την Ακαδημία της Αγίας Πετρούπολης και προσείλκυσε αρκετούς κορυφαίους Μαθηματικούς στη Ρωσία, συμπεριλαμβανομένων των Nicolaus και Daniel Bernoulli. Κατόπιν σύστασής τους, εξασφαλίστηκε ακρόαση για τον Euler. Λόγω της νεαρής ηλικίας του, είχε πρόσφατα απορριφθεί για μια θέση καθηγητή Φυσικής στο Πανεπιστήμιο της Βασιλείας και ήταν απολύτως έτοιμος να δεχτεί την πρόσκληση της Ακαδημίας. Στην Αγία Πετρούπολη, σύντομα ήρθε σε επαφή με τον πολύπλευρο λόγιο Christian Goldbach (της διάσημης εικασίας), έναν άνθρωπο που από καθηγητής Μαθηματικών στην συνέχεια εξελίχθηκε σε Υπουργό Εξωτερικών της Ρωσίας. Λαμβάνοντας υπ' όψιν τα ενδιαφέροντά του, φαίνεται πιθανό ότι ο Goldbach ήταν αυτός που επέστησε την προσοχή του Euler στο έργο του Fermat σχετικά με την Θεωρία Αριθμών.

Ο Euler απογοητευμένος από την πολιτική καταπίεση στη Ρωσία, αποδέχτηκε το κάλεσμα του Φρειδερίκου του Μεγάλου να γίνει μέλος της Ακαδημίας του Βερολίνου. Λέγεται ότι, κατά τη διάρκεια ακρόασης στη βασιλική αυλή, η βασιλομήτωρ τον υποδέχθηκε ευγενικά και τον ρώτησε γιατί ένας τόσο διακεκριμένος Ακαδημαϊκός είναι τόσο δειλός και επιφυλακτικός. Αυτός απάντησε: «Κυρία, γιατί μόλις ήρθα από μία χώρα όπου, όταν κάποιος μιλά, απαγχονίζεται». Ωστόσο, κολακευμένος από τη ζεστασιά της ρωσικής ψυχής απέναντί του και αβάσταχτα προσβεβλημένος από την ψυχρότητα του Φρειδερίκου και της Αυλής του, επέστρεψε στην Αγία Πετρούπολη το 1766 για το υπόλοιπο του βίου του. Μέσα σε $2-3$ χρόνια από την επιστροφή του, ο Euler τυφλώθηκε εντελώς.

Όμως δεν επέτρεψε στην τύφλωση να επιβραδύνει το επιστημονικό του έργο. Υποβοηθούμενος από την εκπληκτική του μνήμη, εκπόνησε τόσο πολλές εργασίες, ώστε να είναι σχεδόν μη διαχειρίσιμες. Αναμφίβολα, ήταν ο πιο παραγωγικός συγγραφέας σε ολόκληρη την ιστορία των Μαθηματικών. Έγραψε ή υπαγόρευσε πάνω από 700 βιβλία και Μελέτες κατά τη διάρκεια της ζωής του και άφησε ως παρακαταθήκη τόσο εκτενές αδημοσίευτο υλικό, που η Ακαδημία της Αγίας Πετρούπολης χρειάστηκε μετά τον θάνατό του 47 χρόνια για να ολοκληρώσει την εκτύπωση όλων των χειρογράφων του. Η δημοσίευση των έργων του ξεκίνησε από την Ελβετική Ακαδημία Φυσικών Επιστημών το 1911: εκτιμάται ότι περισσότεροι από 75 μεγάλοι τόμοι εν τέλει θα απαιτηθούν για την ολοκλήρωση αυτού του μνημειώδους έργου. Η καλύτερη απόδειξη για την ποιότητα αυτών των Ακαδημαϊκών Έργων αντανακλάται στο γεγονός ότι σε 12 περιπτώσεις κέρδισαν το πολυπόθητο διετές βραβείο της Γαλλικής Ακαδημίας στο Παρίσι.

16.2 Η συνάρτηση ϕ του Euler

Ξεκινούμε με τον ακόλουθο ορισμό.

Ορισμός 16.2.1. Για κάθε φυσικό n, ορίζουμε ως $\phi(n)$ το πλήθος των φυσικών που δεν ξεπερνούν τον n και είναι σχετικά πρώτοι με τον n. Δηλαδή

$$\phi(n) = \#\{k \in \mathbb{N} : k \leqslant n,\ \gcd(k,n) = 1\}.$$

Οι πρώτες τιμές της συνάρτησης ϕ φαίνονται στον Πίνακα 16.2.1. Σε περίπτωση που $n > 1$, έχουμε ότι $\gcd(n,n) = n \neq 1$, επομένως ο $\phi(n)$ είναι ισοδύναμα ο αριθμός των φυσικών που είναι αυστηρά μικρότεροι του n και σχετικά πρώτοι με τον n. Επίσης, παρατηρούμε εύκολα ότι $\phi(1) = 1$ και $\phi(n) = n-1$, αν και μόνο αν ο n είναι πρώτος.

Το πρώτο που θα εξετάσουμε σε σχέση με την συνάρτηση ϕ είναι τι τιμές παίρνει σε δυνάμεις πρώτων. Όταν λίγο αργότερα δείξουμε ότι η ϕ είναι πολλαπλασιαστική, θα μπορούμε να συναγάγουμε γενικό τύπο για τον $\phi(n)$ (βάσει της κανονικής μορφής του n) χρησιμοποιώντας αυτό το αποτέλεσμα.

Πίνακας 16.2.1: Οι αρχικές τιμές της συνάρτησης ϕ

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6

Θεώρημα 16.2.2. *Έστω p πρώτος και k φυσικός. Τότε*

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Απόδειξη. Είναι σαφές ότι $\gcd(n, p^k) = 1$, αν και μόνο αν $p \nmid n$. Τα πολλαπλάσια του p μεταξύ του 1 και του p^k είναι ακριβώς τα

$$p, 2p, 3p, \ldots, (p^{k-1})p,$$

που είναι συνολικά p^{k-1} το πλήθος. Επομένως το σύνολο $\{1, 2, \ldots, p^k\}$ περιέχει ακριβώς $p^k - p^{k-1}$ φυσικούς οι οποίοι είναι σχετικά πρώτοι με τον p. Προκύπτει λοιπόν από τον ορισμό της συνάρτησης ϕ ότι $\phi(p^k) = p^k - p^{k-1}$. ■

Διατυπώνουμε ως ξεχωριστό λήμμα το ακόλουθο αποτέλεσμα.

Λήμμα 16.2.3. *Έστω ακέραιοι a, b, c οι οποίοι δεν είναι όλοι ίσοι με 0. Τότε ισχύει ότι $\gcd(a, bc) = 1$, αν και μόνο αν $\gcd(a, b) = 1$ και $\gcd(a, c) = 1$.*

Απόδειξη. Αρκεί να δείξουμε ότι αν $\gcd(a, bc) = 1$, τότε $\gcd(a, b) = \gcd(a, c) = 1$, αφού το αντίστροφο το έχουμε δείξει στο (i) της Άσκησης 2.3.6.

Έστω τώρα ότι $\gcd(a, bc) = 1$. Θέτουμε $d = \gcd(a, b)$. Εφ' όσον $d \mid a$ και $d \mid b$, έχουμε ότι $d \mid a$ και $d \mid bc$. Άρα $1 = \gcd(a, bc) \geqslant d$ και προκύπτει ότι $d = 1$. Με εντελώς ανάλογο τρόπο δείχνουμε ότι $\gcd(a, c) = 1$. ■

Είμαστε σε θέση τώρα να διατυπώσουμε και να αποδείξουμε το επόμενο κεντρικό αποτέλεσμα για την συνάρτηση ϕ.

Θεώρημα 16.2.4. *Η ϕ είναι πολλαπλασιαστική συνάρτηση.*

Απόδειξη. Καλούμαστε να δείξουμε ότι $\phi(mn) = \phi(m)\phi(n)$, αν οι m, n είναι σχετικά πρώτοι. Εφ' όσον $\phi(1) = 1$, το ζητούμενο ισχύει προφανώς, αν είτε $m = 1$ είτε $n = 1$. Μπορούμε επομένως να υποθέσουμε ότι $m, n > 1$. Διατάσσουμε τώρα τους φυσικούς από το 1 μέχρι και το mn σε m στήλες n φυσικών ως εξής:

$$\begin{array}{rrcrcr}
1 & 2 & \cdots & r & \cdots & m \\
m{+}1 & m{+}2 & \cdots & m{+}r & \cdots & 2m \\
2m{+}1 & 2m{+}2 & \cdots & 2m{+}r & \cdots & 3m \\
\vdots & \vdots & \cdots & \vdots & \ddots & \vdots \\
(n-1)m{+}1 & (n-1)m{+}2 & \cdots & (n-1)m{+}r & \cdots & nm
\end{array}$$

Ο φυσικός $\phi(mn)$ είναι ίσος με τον αριθμό των καταχωρίσεων στον ανωτέρω πίνακα που είναι σχετικά πρώτοι με τον mn. Χάριν του Λήμματος 16.2.3, ο $\phi(mn)$ είναι ίσος με τον αριθμό των φυσικών που είναι σχετικά πρώτοι και με τον m και με τον n.

Πριν δούμε αναλυτικότερα τις λεπτομέρειες του επιχειρήματος, επισημαίνουμε το εξής: λόγω της ισότητας $\gcd(qm+r,m)=\gcd(r,m)$, οι φυσικοί στην rοστή στήλη είναι σχετικά πρώτοι με τον m, αν και μόνο αν ο ίδιος ο r είναι σχετικά πρώτος με τον m. Επιπλέον, υπάρχουν ακριβώς $\phi(m)$ στήλες που περιέχουν φυσικούς σχετικά πρώτους με τον m και σε κάθε τέτοια στήλη όλοι οι φυσικοί είναι σχετικά πρώτοι με τον m.

Το ζήτημα επομένως είναι να δείξουμε ότι σε κάθε μία από τις $\phi(m)$ αυτές στήλες υπάρχουν ακριβώς $\phi(n)$ φυσικοί που είναι σχετικά πρώτοι με τον n. Αν το καταφέρουμε αυτό, θα έχουμε δείξει ότι συνολικά υπάρχουν $\phi(m)\phi(n)$ φυσικοί στον παραπάνω πίνακα οι οποίοι είναι σχετικά πρώτοι και με τον m και με τον n.

Οι φυσικοί της rοστής στήλης (για την οποία υποθέτουμε ότι $\gcd(r,m)=1$) είναι οι

$$r, m+r, 2m+r, \ldots, (n-1)m+r.$$

Υπάρχουν n φυσικοί σε αυτήν την ακολουθία αριθμών οι οποίοι ανά δύο είναι ανισότιμοι $\bmod n$. Πράγματι, αν

$$km+r \equiv jm+r \pmod{n},$$

όπου $0 \leqslant k < j < n$, θα είχαμε $km \equiv jm \pmod{n}$. Εφ' όσον $\gcd(m,n)=1$, θα ήμασταν σε θέση να απλοποιήσουμε τον m και να πάρουμε $k \equiv j \pmod{n}$, που είναι άτοπο.

Συμπεραίνουμε ότι οι αριθμοί της rοστής στήλης είναι ισότιμοι ως προς το μέτρο n με κάποια αναδιάταξη των $0,1,2,\ldots,n-1$. Παρατηρούμε τώρα ότι, αν $s \equiv t \pmod{n}$, τότε $\gcd(s,n)=1$, αν και μόνο αν $\gcd(t,n)=1$. Απόρροια αυτού είναι ότι η rοστή στήλη περιέχει τόσους φυσικούς σχετικά πρώτους με τον n όσους ακριβώς και το σύνολο $\{0,1,2,\ldots,n-1\}$, δηλαδή $\phi(n)$ φυσικούς. Έχουμε δείξει επομένως ότι ο πίνακας περιέχει $\phi(m)\phi(n)$ φυσικούς που είναι σχετικά πρώτοι και με τον m και με τον n, άρα η απόδειξή μας έχει ολοκληρωθεί. ■

Γνωρίζοντας τώρα ότι η ϕ είναι πολλαπλασιαστική, στο επόμενο αποτέλεσμα δίνουμε έναν τύπο για τον $\phi(n)$ βάσει της κανονικής μορφής του n.

Πόρισμα 16.2.5. *Έστω n φυσικός του οποίου η κανονική μορφή είναι $n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$. Τότε*

$$\phi(n)=\prod_{i=1}^{r}\left(p_i^{k_i}-p_i^{k_i-1}\right)=n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια της (14.1.1). ■

Παράδειγμα 16.2.6. Θα υπολογίσουμε τον $\phi(360)$. Έχουμε $360=2^3\cdot 3^2\cdot 5$. Εφαρμόζοντας το Πόρισμα 16.2.5 παίρνουμε

$$\begin{aligned}\phi(360) &= 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\ &= 360\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}=96.\end{aligned}$$

Ίσως έχετε παρατηρήσει ότι για όλες τις τιμές του $n>2$ που έχουμε δει ως τώρα, ο $\phi(n)$ είναι πάντα άρτιος.

Θεώρημα 16.2.7. *Έστω $n>2$ φυσικός. Τότε ο $\phi(n)$ είναι άρτιος.*

Απόδειξη. Εάν ο n είναι μία δύναμη του 2, έστω $n = 2^k$ με $k \geqslant 2$, τότε το Πόρισμα 16.2.5 μας δίνει

$$\phi(n) = \phi(2^k) = 2^k \left(1 - \frac{1}{2}\right) = 2^{k-1},$$

δηλαδή ο $\phi(n)$ είναι άρτιος. Εάν ο n δεν είναι μία δύναμη του 2, τότε ο n διαιρείται από κάποιον περιττό πρώτο p. Μπορούμε επομένως να γράψουμε $n = p^k m$, όπου $k \geqslant 1$ και $\gcd(p^k, m) = 1$. Η πολλαπλασιαστικότητα της ϕ μας επιτρέπει τώρα να γράψουμε

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m).$$

Εφ' όσον $2 \mid p - 1$, ο $\phi(n)$ είναι άρτιος και σ' αυτήν την περίπτωση. ■

Στο επόμενο αποτέλεσμα θα δούμε μια ενδιαφέρουσα ιδιότητα της συνάρτησης ϕ, την οποία ανακάλυψε ο Gauss.

Θεώρημα 16.2.8. *Έστω n φυσικός. Τότε $\sum_{d|n} \phi(d) = n$.*

Απόδειξη. Διαμερίζουμε το σύνολο $\{1, 2, \ldots, n\}$ σε υποσύνολα X_d, όπου d διαιρέτης του n, ως εξής: αν m φυσικός $\leqslant n$, τότε $m \in X_d$, αν και μόνο αν $\gcd(m, n) = d$. Είναι σαφές ότι κάθε φυσικός $\leqslant n$ ανήκει σε ένα και μόνο ένα υποσύνολο X_d και άρα το $\{1, 2, \ldots, n\}$ είναι η ξένη ένωση των X_d, καθώς το d διατρέχει τους διαιρέτες του n. Η συνθήκη $\gcd(m, n) = d$ είναι ισοδύναμη με την $\gcd(m/d, n/d) = 1$, επομένως

$$|X_d| = \#\left\{j \leqslant n/d : \gcd\left(j, n/d\right) = 1\right\} = \phi\left(n/d\right).$$

Τα υποσύνολα X_d διαμερίζουν το $\{1, 2, \ldots, n\}$ που έχει n στοιχεία. Συνεπώς

$$n = \sum_{d|n} |X_d| = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$$

και το ζητούμενο έχει δειχθεί. ■

Ας δούμε με ένα παράδειγμα πώς δουλεύει η απόδειξη που μόλις παρουσιάσαμε.

Παράδειγμα 16.2.9. Ένα απλό αριθμητικό παράδειγμα της «διαδικασίας» που περιγράφει η απόδειξη του Θεωρήματος 16.2.8, μας δίνει ο $n = 10$. Για $n = 10$ λοιπόν, έχουμε

$$X_1 = \{1, 3, 7, 9\}, \qquad X_2 = \{2, 4, 6, 8\}, \qquad X_5 = \{5\}, \qquad X_{10} = \{10\}.$$

Βλέπουμε ότι τα παραπάνω σύνολα περιέχουν αντίστοιχα $\phi(10) = 4$, $\phi(5) = 4$, $\phi(2) = 1$ και $\phi(1) = 1$ φυσικούς. Επομένως

$$\begin{aligned}\sum_{d|10} \phi(d) &= \phi(10) + \phi(5) + \phi(2) + \phi(1) \\ &= 4 + 4 + 1 + 1 = 10.\end{aligned}$$

Θα δούμε στην επόμενη εφαρμογή μία ακόμα ενδιαφέρουσα ταυτότητα που ικανοποιεί η συνάρτηση ϕ.

Εφαρμογή 16.2.10. Αν ο $n > 1$ είναι φυσικός, τότε το άθροισμα των φυσικών που είναι μικρότεροι ή ίσοι του n και σχετικά πρώτοι με τον n, ισούται με $\frac{1}{2}n\phi(n)$. Συμβολικά

$$\sum_{\substack{j\leqslant n\\(j,n)=1}} j = \frac{1}{2}n\phi(n),$$

όπου $(j,n) = \gcd(j,n)$ στο ανωτέρω άθροισμα.

Για να δείξουμε το ζητούμενο, επιχειρηματολογούμε ως εξής: έστω

$$a_1, a_2, \ldots, a_{\phi(n)}$$

οι φυσικοί που είναι μικρότεροι ή ίσοι του n και σχετικά πρώτοι με τον n. Η βασική μας παρατήρηση είναι ότι

$$\gcd(a,n) = 1 \qquad \text{αν και μόνο αν} \qquad \gcd(n-a,n) = 1.$$

Δικαιολογούμε την ανωτέρω ισοδυναμία θέτοντας $d_1 = \gcd(a,n)$ και $d_2 = \gcd(n-a,n)$. Εφ' όσον $d_1 \mid a$ και $d_1 \mid n$, έχουμε $d_1 \mid a$ και $d_1 \mid n-a$, δηλαδή $d_1 \mid d_2$. Ομοίως, οι σχέσεις $d_2 \mid n$ και $d_2 \mid n-a$ συνεπάγονται την $d_2 \mid n-(n-a) = a$, δηλαδή $d_2 \mid d_1$. Προκύπτει ότι $d_2 = d_1$ και άρα $d_1 = 1$, αν και μόνο αν $d_2 = 1$.

Χρησιμοποιώντας αυτήν την παρατήρηση, βλέπουμε ότι οι

$$n-a_1, n-a_2, \ldots, n-a_{\phi(n)}$$

είναι απλά μία αναδιάταξη των $a_1, a_2, \ldots, a_{\phi(n)}$ και άρα

$$\begin{aligned} a_1 + a_2 + \ldots + a_{\phi(n)} &= (n-a_1) + (n-a_2) + \ldots + (n-a_{\phi(n)}) \\ &= \phi(n)n - (a_1 + a_2 + \ldots + a_{\phi(n)}). \end{aligned}$$

Επομένως

$$\phi(n)n = 2(a_1 + a_2 + \ldots + a_{\phi(n)}),$$

που είναι ακριβώς αυτό που θέλαμε να δείξουμε.

Κλείνουμε αυτό το μάθημα με μία τελευταία εφαρμογή που σχετίζεται με την συνάρτηση μ του Möbius.

Εφαρμογή 16.2.11. Θα δείξουμε ότι για κάθε φυσικό n ισχύει

$$\phi(n) = n\sum_{d\mid n}\frac{\mu(d)}{d}.$$

Η απόδειξη είναι ιδιαίτερα απλή. Εφαρμόζουμε τον τύπο αντιστροφής του Möbius (Θεώρημα 15.2.1) στην συνάρτηση

$$F(n) = n = \sum_{d\mid n}\phi(d),$$

όπου η δεύτερη ισότητα ισχύει λόγω του Θεωρήματος 16.2.8. Έχουμε τότε

$$\begin{aligned} \phi(n) &= \sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right) \\ &= \sum_{d\mid n}\mu(d)\frac{n}{d}. \end{aligned}$$

Η ανωτέρω ισότητα είναι προφανώς ισοδύναμη με αυτήν που θέλαμε να δείξουμε.

16.3 Ασκήσεις

Άσκηση 16.3.1. Υπολογίστε τους $\phi(1001)$, $\phi(5040)$ και $\phi(36,000)$.

Λύση. Οι παραγοντοποιήσεις των δοθέντων φυσικών έχουν ως εξής:

$$1001 = 7 \cdot 11 \cdot 13, \qquad 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \qquad \text{και} \qquad 36000 = 2^5 \cdot 3^2 \cdot 5^3.$$

Χρησιμοποιώντας το Πόρισμα 16.2.5 μπορούμε να υπολογίσουμε

$$\begin{aligned}
\phi(1001) &= 1001\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right) = 7 \cdot 11 \cdot 13 \cdot \frac{6}{7} \cdot \frac{10}{11} \cdot \frac{12}{13} = 60 \cdot 12 = 720, \\
\phi(5040) &= 5040\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 1152, \\
\phi(36000) &= 36000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 2^5 \cdot 3^2 \cdot 5^3 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2^7 \cdot 3 \cdot 5^2 = 9600.
\end{aligned}$$

Η λύση μας είναι πλήρης. ■

Άσκηση 16.3.2. Να αποδείξετε κάθε μία από τις παρακάτω προτάσεις:

(i) Αν ο n είναι περιττός, τότε $\phi(2n) = \phi(n)$.

(ii) Αν ο n είναι άρτιος, τότε $\phi(2n) = 2\phi(n)$.

(iii) Ισχύει ότι $\phi(3n) = 3\phi(n)$, αν και μόνο αν $3 \mid n$.

(iv) Ισχύει ότι $\phi(3n) = 2\phi(n)$, αν και μόνο αν $3 \nmid n$.

(v) Ισχύει ότι $\phi(n) = n/2$, αν και μόνο αν $n = 2^k$ για κάποιον φυσικό k.

Υπόδειξη: Γράψτε $n = 2^k m$, όπου m περιττός, και χρησιμοποιήστε την $\phi(n) = n/2$ για να δείξετε ότι $m = 1$.

Απόδειξη. (i) Εφ' όσον ο n είναι περιττός, ο n είναι σχετικά πρώτος με τον 2. Η πολλαπλασιαστικότητα της ϕ μας δίνει ότι $\phi(2n) = \phi(2)\phi(n)$ και το ζητούμενο έπεται από την ισότητα $\phi(2) = 1$.

(ii) Γράφουμε $n = 2^k m$, όπου m περιττός και k φυσικός. Έχουμε τώρα $2n = 2^{k+1}m$ και άρα

$$\phi(2n) = \phi(2^{k+1}m) = \phi(2^{k+1})\phi(m) = 2^{k+1}\left(1-\frac{1}{2}\right)\phi(m) = 2^k\phi(m),$$

όπου για την δεύτερη ισότητα χρησιμοποιούμε την πολλαπλασιαστικότητα της ϕ. Επίσης

$$\phi(n) = \phi(2^k m) = \phi(2^k)\phi(m) = 2^k\left(1-\frac{1}{2}\right)\phi(m) = 2^{k-1}\phi(m) = \frac{1}{2}\phi(2n), \tag{16.3.1}$$

οπότε συμπεραίνουμε ότι $\phi(2n) = 2\phi(n)$.

(iii) Αν ισχύει ότι $\phi(3n) = 3\phi(n)$ αλλά $3 \nmid n$, τότε $\gcd(3, n) = 1$. Επομένως η πολλαπλασιαστικότητα της ϕ μας δίνει $\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$, που είναι άτοπο. Άρα $3 \mid n$, όπως θέλαμε.

Αντίστροφα τώρα, έστω ότι $3 \mid n$. Γράφουμε $n = 3^k m$, όπου m σχετικά πρώτος με τον 3 και k φυσικός. Έχουμε τότε ότι $3n = 3^{k+1}m$, οπότε

$$\phi(3n) = \phi(3^{k+1}m) = \phi(3^{k+1})\phi(m) = 3^{k+1}\left(1 - \frac{1}{3}\right)\phi(m) = 2 \cdot 3^k \phi(m).$$

Επίσης

$$\phi(n) = \phi(3^k m) = \phi(3^k)\phi(m) = 3^k\left(1 - \frac{1}{3}\right)\phi(m) = 2 \cdot 3^{k-1}\phi(m) = \frac{1}{3}\phi(3n).$$

Έχουμε τελικά ότι $\phi(3n) = 3\phi(n)$, που ήταν και το ζητούμενο.

(iv) Όπως δείξαμε στο (iii), αν $3 \mid n$ τότε $\phi(3n) = 3\phi(n) \neq 2\phi(n)$. Επομένως αν $\phi(3n) = 2\phi(n)$, τότε $3 \nmid n$. Αντίστροφα, αν $3 \nmid n$ τότε $\gcd(3, n) = 1$ και χρησιμοποιώντας την πολλαπλασιαστικότητα της ϕ παίρνουμε $\phi(3n) = \phi(3)\phi(n) = 2\phi(n)$.

(v) Υποθέτουμε αρχικά ότι $\phi(n) = n/2$. Από την σχέση αυτήν συμπεραίνουμε ότι ο n θα πρέπει να είναι άρτιος. Έστω λοιπόν ότι $n = 2^k m$, όπου k φυσικός και m περιττός. Όπως δείξαμε στην (16.3.1), ισχύει ότι $\phi(n) = 2^{k-1}\phi(m)$. Άρα

$$2^{k-1}m = n/2 = \phi(n) = 2^{k-1}\phi(m).$$

Συμπεραίνουμε ότι ο m είναι τέτοιος ώστε $m = \phi(m)$. Ο μόνος φυσικός με αυτήν την ιδιότητα όμως είναι ο $m = 1$, αφού αν $m > 1$, τότε $\phi(m) \leqslant m - 1 < m$. Προκύπτει λοιπόν ότι ο n είναι μία δύναμη του 2, όπως θέλαμε να δείξουμε. Αντίστροφα, αν $n = 2^k$ για κάποιον k, τότε βλέπουμε εύκολα ότι $\phi(n) = n/2$, επομένως η απόδειξή μας είναι πλήρης. ■

Άσκηση 16.3.3. Αν κάθε πρώτος που διαιρεί τον φυσικό n, διαιρεί επίσης τον φυσικό m, να δείξετε ότι $\phi(nm) = n\phi(m)$. Συγκεκριμένα, ισχύει ότι $\phi(n^2) = n\phi(n)$ για κάθε φυσικό n.

Απόδειξη. Γράφουμε

$$\phi(nm) = nm \prod_{p \mid nm}\left(1 - \frac{1}{p}\right) = nm \prod_{p \mid m}\left(1 - \frac{1}{p}\right) = n\left[m \prod_{p \mid m}\left(1 - \frac{1}{p}\right)\right] = n\phi(m),$$

όπου η δεύτερη ισότητα προκύπτει από το δεδομένο ότι κάθε φυσικός που διαιρεί τον n διαιρεί και τον m. Παίρνοντας $m = n$ έχουμε $\phi(n^2) = n\phi(n)$ για κάθε φυσικό n. ■

Άσκηση 16.3.4. Να δείξετε ότι αν ο d διαιρεί τον φυσικό n, τότε ο $\phi(d)$ διαιρεί τον $\phi(n)$.

Απόδειξη. Από την πολλαπλασιαστικότητα της ϕ αρκεί να δείξουμε το ζητούμενο για $n = p^a$. Αν λοιπόν ο d είναι ένας διαιρέτης του n, τότε $d = p^b$ για κάποιον $b \leqslant a$. Έχουμε τότε

$$\frac{\phi(n)}{\phi(d)} = \frac{\phi(p^a)}{\phi(p^b)} = \frac{p^a\left(1 - \frac{1}{p}\right)}{p^b\left(1 - \frac{1}{p}\right)} = p^{a-b}.$$

Συμπεραίνουμε ότι $\phi(d) \mid \phi(n)$, που ήταν και το ζητούμενο. ■

Άσκηση 16.3.5. Να δειχθούν οι ακόλουθες προτάσεις:

(i) Υπάρχουν άπειροι φυσικοί n που ικανοποιούν την $\phi(n) = n/3$.

Υπόδειξη: Θεωρήστε φυσικούς της μορφής $n = 2^k 3^j$.

(ii) Κανένας φυσικός n δεν ικανοποιεί την $\phi(n) = n/4$.

Απόδειξη. (i) Θα δείξουμε ότι κάθε φυσικός της μορφής $n = 2^k 3^j$, όπου k, j είναι φυσικοί, έχει την ζητούμενη ιδιότητα. Γράφουμε

$$\phi(n) = n\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = n \cdot \frac{1}{2} \cdot \frac{2}{3} = \frac{n}{3},$$

οπότε και έχουμε το ζητούμενο.

(ii) Ας υποθέσουμε αντίθετα ότι υπάρχει φυσικός n που ικανοποιεί την $\phi(n) = n/4$. Είναι σαφές ότι θα πρέπει να ισχύει $4 \mid n$, άρα $n = 2^k m$, όπου $k \geqslant 2$ φυσικός και m περιττός. Για τον $\phi(n)$ θα έχουμε ότι

$$\phi(n) = \phi(2^k)\phi(m) = 2^{k-1}\phi(m),$$

ενώ η υπόθεσή μας είναι ότι $\phi(n) = n/4 = 2^{k-2}m$. Συμπεραίνουμε ότι $2^{k-2}m = 2^{k-1}\phi(m)$ ή ισοδύναμα $m = 2\phi(m)$. Η τελευταία αυτή σχέση όμως είναι αδύνατη, αφού συνεπάγεται την $2 \mid m$, όπου ο m είναι περιττός. Καταλήγουμε ότι δεν υπάρχει φυσικός n τέτοιος ώστε $\phi(n) = n/4$, που ήταν και το ζητούμενο. ■

Άσκηση 16.3.6. Να δείξετε ότι αν ο φυσικός n είναι σύνθετος, τότε $\phi(n) \leqslant n - \sqrt{n}$. Πότε ισχύει η ισότητα;

Απόδειξη. Έστω p ο μικρότερος πρώτος διαιρέτης του n. Εφ' όσον ο n είναι σύνθετος, ισχύει ότι $p \leqslant \sqrt{n}$. Προκύπτει τώρα ότι

$$\phi(n) \leqslant n\left(1 - \frac{1}{p}\right) \leqslant n\left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n},$$

όπως θέλαμε να δείξουμε. Η ισότητα ισχύει αν και μόνο αν $n = p^2$. ■

Άσκηση 16.3.7. Έστω $n > 1$ φυσικός με κανονική μορφή $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Να δειχθούν οι ακόλουθες ανισότητες:

(i) $\sigma(n)\phi(n) \geqslant n^2\left(1 - 1/p_1^2\right)\left(1 - 1/p_2^2\right)\cdots\left(1 - 1/p_r^2\right)$.

(ii) $\tau(n)\phi(n) \geqslant n$.

Να συμπεράνετε ακολούθως ότι, λόγω της (ii), έχουμε $\phi(n) \geqslant \frac{1}{2}\sqrt{n}$ για κάθε φυσικό n και άρα $\lim_{n\to\infty} \phi(n) = \infty$.

Σημείωση: Ένα πόρισμα της $\phi(n) \geqslant \frac{1}{2}\sqrt{n}$ (ή, αν προτιμάτε, της σχέσης $\lim_{n\to\infty} \phi(n) = \infty$) είναι ότι για κάθε φυσικό m το πλήθος των λύσεων της εξίσωσης $\phi(n) = m$ είναι πεπερασμένο και $\geqslant 0$.

Απόδειξη. (i) Εξετάζουμε αρχικά τι συμβαίνει όταν ο n είναι δύναμη πρώτου. Για p πρώτο και a φυσικό, έχουμε

$$\sigma(p^a)\phi(p^a) = \frac{p^{a+1} - 1}{p - 1} \cdot p^{a-1}(p-1) = (p^{a+1} - 1)p^{a-1}$$
$$= p^{2a} - p^{a-1} \geqslant p^{2a} - p^{2(a-1)} = p^{2a}\left(1 - \frac{1}{p^2}\right).$$

Παρατηρούμε τώρα ότι η $\sigma(n)\phi(n)$ είναι γινόμενο πολλαπλασιαστικών συναρτήσεων, άρα και η ίδια πολλαπλασιαστική. Επομένως

$$\sigma(n)\phi(n) = \prod_{i=1}^{r} \sigma(p_i^{k_i})\phi(p_i^{k_i}) \geqslant \prod_{i=1}^{r} p_i^{2k_i}\left(1-\frac{1}{p_i^2}\right) = \prod_{i=1}^{r} p_i^{2k_i} \cdot \prod_{i=1}^{r}\left(1-\frac{1}{p_i^2}\right) = n^2 \prod_{i=1}^{r}\left(1-\frac{1}{p_i^2}\right),$$

όπως ακριβώς ζητούσαμε να δείξουμε.

(ii) Όπως και στο (i), εξετάζουμε πρώτα την περίπτωση που ο n είναι δύναμη πρώτου. Έχουμε, για p πρώτο και a φυσικό,

$$\tau(p^a)\phi(p^a) = (a+1)p^a\left(1-\frac{1}{p}\right) \geqslant 2p^a\left(1-\frac{1}{p}\right) \geqslant 2p^a\left(1-\frac{1}{2}\right) = p^a.$$

Συμπεραίνουμε ότι

$$\tau(n)\phi(n) = \prod_{i=1}^{r} \tau(p_i^{k_i})\phi(p_i^{k_i}) \geqslant \prod_{i=1}^{r} p_i^{k_i} = n$$

και έχουμε δείξει το ζητούμενο.

Χρησιμοποιούμε τώρα αυτό που δείξαμε στην Άσκηση 13.2.4 και έχουμε ότι για κάθε φυσικό n ισχύει η ανισότητα

$$2\sqrt{n}\phi(n) \geqslant \tau(n)\phi(n) \geqslant n.$$

Επομένως $\phi(n) \geqslant \frac{1}{2}\sqrt{n}$, όπως ακριβώς ζητούσαμε να δείξουμε. ■

Άσκηση 16.3.8. Να δείξετε ότι η ϕ είναι η μοναδική αριθμοθεωρητική συνάρτηση που ικανοποιεί την συναρτησιακή εξίσωση του Θεωρήματος 16.2.8. Δηλαδή, αν η f είναι μία αριθμητική συνάρτηση η οποία ικανοποιεί την

$$\sum_{d|n} f(d) = n \tag{16.3.2}$$

για κάθε φυσικό n, τότε $f(n) = \phi(n)$ για κάθε n.

Απόδειξη. Εφαρμόζοντας τον τύπο αντιστροφής του Möbius στην (16.3.2) παίρνουμε

$$f(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n}\frac{\mu(d)}{d} = \phi(n),$$

για κάθε φυσικό n, όπου η δεύτερη ισότητα προκύπτει από την Εφαρμογή 16.2.11. Η απόδειξή μας είναι πλήρης. ■

Άσκηση 16.3.9. Υπενθυμίζουμε τον ορισμό της συνάρτησης

$$\gamma(n) = \prod_{p|n} p$$

την οποία συναντήσαμε ξανά στην Άσκηση 14.2.2, και η οποία καλείται συνήθως ο πυρήνας (ή το ριζικό) του n. Να δείξετε ότι ο

$$\frac{\phi(n)+\sigma(n)}{\gamma(n)^2}$$

είναι ακέραιος για άπειρες τιμές του φυσικού n.

Υπόδειξη: Θεωρήστε φυσικούς της μορφής $n = 32 \cdot 3^{2r+1}$, όπου r φυσικός.

Απόδειξη. Θα δείξουμε ότι οι αριθμοί $n = 32 \cdot 3^{2r+1}$, για $r = 1, 2, \ldots$, ικανοποιούν το ζητούμενο. Για να το πετύχουμε αυτό, αρκεί να δείξουμε ότι αν $n = 32 \cdot 3^{2r+1}$, τότε ο

$$\phi(n) + \sigma(n) = 16 \cdot 3^{2r} \cdot 2 + 63 \cdot \frac{3^{2r+2} - 1}{2}$$

είναι πολλαπλάσιο του $36 = \gamma(n)^2$. Παρατηρούμε ότι $36 \mid 16 \cdot 3^{2r} \cdot 2$ και $9 \mid 63$. Αρκεί λοιπόν να δείξουμε ότι $4 \mid (3^{2r+2} - 1)/2$ ή ισοδύναμα ότι $8 \mid 3^{2r+2} - 1$. Αυτό όμως είναι άμεση συνέπεια της

$$3^{2r+2} \equiv 9^{r+1} \equiv 1 \pmod 8 .$$

Το ζητούμενο έχει δειχθεί. ■

Άσκηση 16.3.10. Να δείξετε ότι αν οι m, n είναι φυσικοί και $d = \gcd(m, n)$, τότε

$$\phi(m)\phi(n) = \phi(mn)\frac{\phi(d)}{d}.$$

Απόδειξη. Ένας τρόπος να δείξουμε το ζητούμενο είναι να συνδυάσουμε αποτελέσματα που έχουμε ήδη αποδείξει. Έστω ότι οι m, n είναι φυσικοί. Για ευκολία στον συμβολισμό, ας θέσουμε $e = \operatorname{lcm}(m, n)$. Γνωρίζουμε από το Θεώρημα 3.2.2 ότι $de = mn$, επομένως $\phi(de) = \phi(mn)$. Παρατηρούμε όμως ότι κάθε πρώτος που διαιρεί τον d, διαιρεί και τον e, άρα είμαστε σε θέση να χρησιμοποιήσουμε αυτό που δείξαμε στην Άσκηση 16.3.3 και να πάρουμε $\phi(de) = d\phi(e)$, δηλαδή

$$\phi(mn) = d\phi(e). \tag{16.3.3}$$

Εφ' όσον έχουμε δείξει ότι η ϕ είναι πολλαπλασιαστική, μπορούμε επίσης να χρησιμοποιήσουμε την Εφαρμογή 14.1.7 για να γράψουμε

$$\phi(m)\phi(n) = \phi(d)\phi(e) = \frac{\phi(d)}{d}\phi(mn),$$

όπου η δεύτερη ισότητα προκύπτει από την (16.3.3). Το ζητούμενο έχει δειχθεί. ■

Άσκηση 16.3.11. Έστω $n > 1$ φυσικός και p, q αντίστοιχα ο μικρότερος και ο μεγαλύτερος πρώτος διαιρέτης του n. Να δείξετε, χρησιμοποιώντας κατάλληλο επαγωγικό επιχείρημα (ή αλλιώς) ότι

$$\phi(n) \geqslant \frac{p-1}{q}n.$$

Απόδειξη. Έστω $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ η κανονική μορφή του φυσικού $n > 1$, όπου $p = p_1$ είναι ο μικρότερος πρώτος διαιρέτης του n και $q = p_r$ ο μεγαλύτερος. Θα δείξουμε το ζητούμενο με επαγωγή στο r.

Αν $r = 1$, τότε $n = p^{k_1}$ και

$$\phi(n) = \phi(p^{k_1}) = \frac{p-1}{p}p^{k_1} = \frac{p-1}{p}n,$$

οπότε το ζητούμενο ισχύει σε αυτήν την περίπτωση. Υποθέτουμε τώρα ότι $r > 1$ και ότι ο ισχυρισμός ισχύει για κάθε φυσικό με λιγότερους από r διακεκριμένους πρώτους διαιρέτες. Θέτουμε $m = p_2^{r_2} \cdots p_r^{k_r}$. Η επαγωγική υπόθεση μας εξασφαλίζει ότι

$$\phi(m) \geqslant \frac{p_2 - 1}{q} m,$$

οπότε έχουμε

$$\phi(n) = \phi(p^{k_1})\phi(m) = p^{k_1}\left(\frac{p-1}{p}\right)\phi(m) \geqslant p^{k_1}\left(\frac{p-1}{p}\right)\left(\frac{p_2-1}{q}\right)m = n\left(\frac{p-1}{p}\right)\left(\frac{p_2-1}{q}\right) = \left(\frac{p-1}{q}n\right)\left(\frac{p_2-1}{p}\right) \geqslant \frac{p-1}{q}n$$

όπου η τελευταία ανισότητα προκύπτει από την $p_2 > p$. Η επαγωγή μας έχει ολοκληρωθεί. ■

Άσκηση 16.3.12. Να βρεθούν οι λύσεις της εξίσωσης $\phi(n) = 12$.

Υπόδειξη: Αν ο $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ ικανοποιεί την $\phi(n) = k$, τότε

$$p_1^{k_1-1} p_2^{k_2-1} \cdots p_r^{k_r-1} \prod_{i=1}^{r} (p_i - 1) = k.$$

Επομένως οι φυσικοί $d_i = p_i - 1$, $1 \leqslant i \leqslant r$, μπορούν να καθοριστούν από τις σχέσεις:

1. $d_i \mid k$,
2. ο $d_i + 1$ είναι πρώτος,
3. οι πρώτοι διαιρέτες του $k / \prod_{i=1}^{r} d_i$ ανήκουν στο $\{p_1, p_2, \ldots, p_r\}$.

Λύση. Η αρχική μας παρατήρηση είναι ότι αν κάποιος πρώτος p διαιρεί τον n, τότε ο $p-1$ διαιρεί τον 12 και άρα $p \in \{2, 3, 5, 7, 13\}$. Παρατηρούμε μετά ότι αν $p^2 \mid n$ για κάποιον πρώτο p, τότε $p \mid 12$. Προκύπτει από αυτό ότι μόνο οι 2, 3 μπορούν να εμφανιστούν στην ανάλυση του n σε δύναμη μεγαλύτερη του 1. Δηλαδή αν $v_p(n) > 1$, τότε $p \in \{2, 3\}$.

Αν τώρα $3^3 \mid n$, τότε

$$\phi(n) \geqslant \phi(3^3) = 18 > 12$$

που είναι άτοπο. (Η πρώτη ανισότητα προκύπτει χρησιμοποιώντας, για παράδειγμα, την Άσκηση 16.3.4.) Έστω τώρα ότι $3^2 \mid n$, δηλαδή $n = 9k$ με $3 \nmid k$. Τότε

$$12 = \phi(n) = \phi(9)\phi(k) = 6\phi(k)$$

και άρα $\phi(k) = 2$. Για να βρούμε τους k οι οποίοι ικανοποιούν την $\phi(k) = 2$, μπορούμε να κάνουμε το εξής. Στην Άσκηση 16.3.7 δείξαμε ότι $\phi(k) \geqslant \frac{1}{2}\sqrt{k}$ για κάθε φυσικό k. Για να έχουμε $\phi(k) = 2$ επομένως, θα πρέπει να ισχύει $k \leqslant 16$. Συμβουλευόμαστε τον Πίνακα 16.2.1 και παρατηρούμε ότι μόνος k με $\phi(k) = 2$ και $3 \nmid k$ είναι ο $k = 4$. Μία λύση λοιπόν της $\phi(n) = 12$ είναι η $n = 36$.

Εξετάζουμε τώρα την περίπτωση $5 \mid n$. Εφ' όσον $5^2 \nmid n$ σύμφωνα με τις αρχικές παρατηρήσεις, θα έχουμε $n = 5k$ με $5 \nmid k$. Άρα

$$12 = \phi(n) = \phi(5)\phi(k) = 4\phi(k)$$

που συνεπάγεται ότι $\phi(k) = 3$. Αυτό όμως είναι άτοπο λόγω του Θεωρήματος 16.2.7.

Στην συνέχεια, εξετάζουμε την διαιρετότητα του n με τον 7. Σε περίπτωση που $7 \mid n$, θα έχουμε $n = 7k$ με $7 \nmid k$. Άρα

$$12 = \phi(n) = \phi(7)\phi(k) = 6\phi(k),$$

δηλαδή $\phi(k) = 2$. Σύμφωνα πάλι με τον Πίνακα 16.2.1, οι k που ικανοποιούν τις $\phi(k) = 2$ και $7 \nmid k$ είναι οι $k = 4$, $k = 3$ και $k = 6$. Έχουμε εντοπίσει λοιπόν τις λύσεις $n = 21$, $n = 28$ και $n = 42$.

Θα δείξουμε τώρα ότι αν ο n είναι άρτιος, τότε $v_2(n) \leqslant 2$. Αν $t = v_2(n)$, τότε $n = 2^t k$, όπου k περιττός. Επομένως $\phi(2^t) = 2^{t-1} \mid 12$ και άρα $t \leqslant 3$. Η περίπτωση $t = 3$ αποκλείεται γιατί οδηγεί στην

$$12 = \phi(n) = \phi(8)\phi(k) = 4\phi(k),$$

δηλαδή $\phi(k) = 3$, που είναι άτοπο. Άρα όντως $v_2(n) \leqslant 2$.

Είμαστε σε θέση τώρα να συμπεράνουμε ότι αν ο n ικανοποιεί την $\phi(n) = 12$, τότε

$$n = 2^t 3^a 13^b,$$

όπου $t \in \{0, 1, 2\}$ και $a, b \in \{0, 1\}$. Αν $b = 1$ τότε αναγκαστικά $a = 0$ και $t = 0$ ή $t = 1$, αφού θα πρέπει $\phi(n/13) = 1$, δηλαδή $n/13 = 1$ ή $n/13 = 2$. Δύο ακόμα λύσεις επομένως είναι οι $n = 13$ και $n = 26$.

Είναι τώρα σαφές ότι δεν υπάρχουν άλλες λύσεις, διότι αν $n = 2^t 3^a$, όπου $t \in \{0, 1, 2\}$ και $a \in \{0, 1\}$, τότε $n \leqslant 12$ και άρα $\phi(n) \leqslant 11$. Συνολικά το σύνολο λύσεων της εξίσωσης $\phi(n) = 12$ είναι το $\{13, 21, 26, 28, 36, 42\}$. ■

Άσκηση 16.3.13. $(*)$ Να δείξετε το ακόλουθο θεώρημα που οφείλεται στον Somayajulu (1950):

$$\limsup_{n\to\infty} \frac{\phi(n+1)}{\phi(n)} = \infty \qquad \text{και} \qquad \liminf_{n\to\infty} \frac{\phi(n+1)}{\phi(n)} = 0.$$

Υπόδειξη: Θεωρήστε γινόμενα πρώτων και χρησιμοποιήστε κατάλληλα το Θεώρημα του Dirichlet για πρώτους σε αριθμητικές προόδους. Μπορείτε να θεωρήσετε γνωστό ότι το άθροισμα $\sum_p \frac{1}{p}$ αποκλίνει στο ∞ ή ισοδύναμα ότι το γινόμενο $\prod_p (1 - 1/p)$ αποκλίνει στο 0.

Σημείωση: Το να δείξετε αυτό που ζητά η άσκηση είναι ισοδύναμο με το να βρείτε ακολουθίες (u_n), (v_n) που είναι τέτοιες ώστε

$$\lim_{n\to\infty} \frac{\phi(u_n+1)}{\phi(u_n)} = \infty \qquad \text{και} \qquad \lim_{n\to\infty} \frac{\phi(v_n+1)}{\phi(v_n)} = 0.$$

Ο Schinzel έχει δείξει το ακόμη ισχυρότερο:

$$\text{Η ακολουθία } \left(\frac{\phi(n+1)}{\phi(n)}\right) \text{ είναι πυκνή στο } (0, +\infty).$$

Απόδειξη. Έστω r φυσικός. Θέτουμε $n = p_1 p_2 \cdots p_r$, όπου p_i είναι ως συνήθως ο iοστός πρώτος. Το Θεώρημα 7.2.3 μας εξασφαλίζει την ύπαρξη ενός φυσικού k τέτοιου ώστε ο $q = kn + 1$ να είναι πρώτος. Έχουμε τότε $\phi(q) = q - 1 = kn$ και

$$\phi(q-1) = \phi(kn) = kn \prod_{p \mid kn} \left(1 - \frac{1}{p}\right) \leqslant kn \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = \phi(q) \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Προκύπτει λοιπόν ότι

$$\frac{\phi(q)}{\phi(q-1)} \geqslant \frac{1}{\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)}.$$

Όμως το $\sum_p \frac{1}{p}$ αποκλίνει στο ∞ και άρα το $\prod_p(1-1/p)$ αποκλίνει στο 0. Συμπεραίνουμε ότι, καθώς ο $r \to \infty$, έχουμε

$$\limsup_{n\to\infty} \frac{\phi(n+1)}{\phi(n)} = \infty.$$

Σχετικά με το δεύτερο όριο, έστω k φυσικός τέτοιος ώστε ο $q = kn - 1$ να είναι πρώτος, όπου $n = p_1 p_2 \cdots p_r$ όπως και πριν. Τότε $\phi(q) = q - 1 = kn - 2$ και

$$\phi(q+1) = \phi(kn) = kn \prod_{p|kn}\left(1-\frac{1}{p}\right) \leqslant kn \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

Άρα

$$\frac{\phi(q+1)}{\phi(q)} \leqslant \frac{kn}{kn-2}\prod_{i=1}^{r}(1-1/p_i).$$

Καταλήγουμε ότι, καθώς ο r πηγαίνει στο άπειρο, έχουμε

$$\liminf_{n\to\infty} \frac{\phi(n+1)}{\phi(n)} = 0,$$

όπως θέλαμε να δείξουμε. ■

Κεφάλαιο 17

17η Παράδοση

Στο σημερινό μάθημα θα μιλήσουμε για το Θεώρημα του Euler, το οποίο αποτελεί γενίκευση του Θεωρήματος του Fermat και είναι το τρίτο και τελευταίο κομμάτι του τρίπτυχου κανονικών θεωρημάτων στα οποία κάναμε αναφορά πιο πριν. Θα δούμε ακόμα το Θεώρημα του Rédei, το οποίο γενικεύει με την σειρά του το Θεώρημα του Euler.

17.1 Το Θεώρημα του Euler

Όπως αναφέραμε πρωτύτερα, η πρώτη δημοσιευμένη απόδειξη του (μικρού) Θεωρήματος του Fermat δόθηκε από τον Euler το 1736. Αργότερα, το 1760, ο Euler κατάφερε να γενικεύσει το Θεώρημα του Fermat από έναν πρώτο p σε έναν οποιονδήποτε φυσικό n. Το αποτέλεσμα-ορόσημο αυτό έχει ως εξής:

$$\text{Αν } \gcd(a,n)=1, \text{ όπου } n \text{ φυσικός και } a \text{ ακέραιος, τότε } a^{\phi(n)} \equiv 1 \pmod{n}.$$

Για παράδειγμα για $n=30$ και $a=11$ έχουμε

$$11^{\phi(30)} \equiv 11^8 \equiv \left(11^2\right)^4 \equiv (121)^4 \equiv 1^4 \equiv 1 \pmod{30}.$$

Για την απόδειξη του Θεωρήματος του Euler θα χρειαστούμε ένα λήμμα.

Λήμμα 17.1.1. *Έστω $n>1$ φυσικός και a ακέραιος σχετικά πρώτος με τον n. Αν οι $a_1, a_2, \ldots, a_{\phi(n)}$ είναι οι φυσικοί μικρότεροι του n και σχετικά πρώτοι με τον n, τότε οι*

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

είναι ισότιμοι $\bmod n$ με τους $a_1, a_2, \ldots, a_{\phi(n)}$ σε κάποια σειρά.

Απόδειξη. Παρατηρούμε αρχικά ότι οι $aa_1, aa_2, \ldots, aa_{\phi(n)}$ είναι ανά δύο ανισότιμοι $\bmod n$. Αν αντίθετα $aa_i \equiv aa_j \pmod{n}$, με $1 \leqslant i < j \leqslant \phi(n)$, τότε $a_i \equiv a_j \pmod{n}$ (εφ' όσον $\gcd(a,n)=1$ ο a μπορεί να απλοποιηθεί) και άρα $a_i = a_j$, που είναι άτοπο. Επίσης, επειδή για κάθε δείκτη i ισχύει ότι $\gcd(a_i,n)=1$ και $\gcd(a,n)=1$, βλέπουμε εύκολα (από το Λήμμα 16.2.3 για παράδειγμα) ότι $\gcd(aa_i,n)=1$.

Για έναν aa_i τώρα, υπάρχει μοναδικός ακέραιος b με $0 \leqslant b < n$ για τον οποίο ισχύει ότι $aa_i \equiv b \pmod{n}$. Εφ' όσον όμως

$$\gcd(b,n) = \gcd(aa_i,n) = 1,$$

ο b είναι αναγκαστικά ένας εκ των $a_1, a_2, \ldots, a_{\phi(n)}$. Συμπεραίνουμε ότι οι $aa_1, aa_2, \ldots, aa_{\phi(n)}$ είναι όντως ισότιμοι ως προς το μέτρο n με μία αναδιάταξη των $a_1, a_2, \ldots, a_{\phi(n)}$. ■

Θεώρημα 17.1.2 (Το Θεώρημα του Euler). *Έστω n φυσικός και a ακέραιος ώστε $\gcd(a, n) = 1$. Τότε ισχύει ότι $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Απόδειξη. Μπορούμε να υποθέσουμε ότι $n > 1$. Έστω $a_1, a_2, \ldots, a_{\phi(n)}$ οι φυσικοί που είναι μικρότεροι του n και σχετικά πρώτοι με τον n. Εφ' όσον $\gcd(a, n) = 1$, έπεται από το Λήμμα 17.1.1 ότι οι $aa_1, aa_2, \ldots, aa_{\phi(n)}$ είναι ισότιμοι $\bmod n$ με τους $a_1, a_2, \ldots, a_{\phi(n)}$ σε κάποια σειρά. Έχουμε δηλαδή ότι

$$\begin{aligned} aa_1 &\equiv a'_1 \pmod{n} \\ aa_2 &\equiv a'_2 \pmod{n} \\ &\vdots \\ aa_{\phi(n)} &\equiv a'_{\phi(n)} \pmod{n}, \end{aligned}$$

όπου οι $a'_1, a'_2, \ldots, a'_{\phi(n)}$ είναι μία αναδιάταξη των $a_1, a_2, \ldots, a_{\phi(n)}$. Πολλαπλασιάζοντας τις ανωτέρω ισοτιμίες παίρνουμε

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a'_1 a'_2 \cdots a'_{\phi(n)} \pmod{n} \\ &\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \end{aligned}$$

και άρα

$$a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}.$$

Εφ' όσον όμως για κάθε δείκτη i ισχύει ότι $\gcd(a_i, n) = 1$, το Λήμμα 16.2.3 συνεπάγεται ότι $\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$. Επομένως ο κοινός όρος $a_1 a_2 \cdots a_{\phi(n)}$ μπορεί να απλοποιηθεί στην ανωτέρω ισοτιμία, οπότε και παίρνουμε την

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

που είναι ακριβώς η σχέση που ζητούσαμε να δείξουμε. ■

Αναφέραμε πρωτύτερα ότι το Θεώρημα του Euler γενικεύει το Θεώρημα του Fermat. Πράγματι, αν ο $n = p$ είναι πρώτος και ο a είναι ακέραιος σχετικά πρώτος με τον p, τότε $\phi(p) = p - 1$ και το Θεώρημα του Euler μας δίνει

$$a^{\phi(p)} = a^{p-1} \equiv 1 \pmod{p}$$

που είναι το περιεχόμενο του Θεωρήματος του Fermat.

Ας δούμε τώρα με ένα συγκεκριμένο παράδειγμα πώς δουλεύει το επιχείρημα που χρησιμοποιήσαμε στην απόδειξη του Θεωρήματος 17.1.2.

Παράδειγμα 17.1.3. Θεωρούμε τον φυσικό $n = 9$ και παρατηρούμε ότι οι φυσικοί που είναι μικρότεροι του 9 και σχετικά πρώτοι με τον 9 είναι οι

$$1, 2, 4, 5, 7, 8.$$

Αυτοί ακριβώς οι αριθμοί παίζουν τον ρόλο των $a_1, a_2, \ldots, a_{\phi(n)}$ στην απόδειξη. Αν τώρα $a = -4$, οι ακέραιοι aa_i είναι οι

$$-4, -8, -16, -20, -28, -32$$

και έχουμε

$$-4 \equiv 5, \qquad -8 \equiv 1, \qquad -16 \equiv 2, \qquad -20 \equiv 7, \qquad -28 \equiv 8, \qquad -32 \equiv 4,$$

όπου όλες οι παραπάνω ισοτιμίες είναι ως προς το μέτρο 9. Πολλαπλασιάζοντας μεταξύ τους όλες αυτές τις ισοτιμίες παίρνουμε

$$(-4)(-8)(-16)(-20)(-28)(-32) \equiv 5 \cdot 1 \cdot 2 \cdot 7 \cdot 8 \cdot 4 \pmod 9$$

δηλαδή

$$(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)(-4)^6 \equiv (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8) \pmod 9 .$$

Καθένας όμως εκ των $1, 2, 4, 5, 7, 8$ είναι σχετικά πρώτος με τον 9 και άρα μπορεί να απλοποιηθεί στην παραπάνω ισοτιμία. Έχουμε λοιπόν ότι

$$(-4)^6 \equiv 1 \pmod 9 .$$

Ο υπολογισμός

$$(-4)^6 \equiv 4^6 \equiv 64^2 \equiv 1^2 \equiv 1 \pmod 9$$

επιβεβαιώνει την ανωτέρω ισοτιμία.

Στο επόμενο παράδειγμα θα δούμε πώς το Θεώρημα του Euler μπορεί να χρησιμοποιηθεί ώστε να απλουστευθεί ένας υπολογισμός.

Παράδειγμα 17.1.4. Θα βρούμε τα τελευταία δύο δεκαδικά ψηφία του αριθμού 3^{256}. Για να το πετύχουμε αυτό, αρκεί να βρούμε τον μη αρνητικό $r \leqslant 99$ που είναι τέτοιος ώστε $3^{256} \equiv r \pmod{100}$. Εφ' όσον $\gcd(3, 100) = 1$ και

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40,$$

το Θεώρημα του Euler μας δίνει ότι

$$3^{40} \equiv 1 \pmod{100} .$$

Από τον Αλγόριθμο της Διαίρεσης έχουμε $256 = 6 \cdot 40 + 16$, επομένως

$$3^{256} \equiv 3^{6 \cdot 40 + 16} \equiv (3^{40})^6 3^{16} \equiv 3^{16} \pmod{100} .$$

Οπότε αρκεί να υπολογίσουμε τον $3^{16} \pmod{100}$. Υψώνοντας στο τετράγωνο διαδοχικά έχουμε

$$3^2 \equiv 9 \pmod{100} \quad 3^4 \equiv 81 \pmod{100} \quad 3^8 \equiv 61 \pmod{100} \quad 3^{16} \equiv 21 \pmod{100} .$$

Έχουμε τελικά ότι $3^{256} \equiv 21 \pmod{100}$, όπως ζητούσαμε να βρούμε.

Παρουσιάζουμε τώρα ένα ενδιαφέρον θεωρητικό αποτέλεσμα σχετικά με την ύπαρξη γεωμετρικών προόδων μέσα σε αριθμητικές, το οποίο αποτελεί εφαρμογή του Θεωρήματος του Euler.

Εφαρμογή 17.1.5. Θα δείξουμε ότι κάθε αριθμητική πρόοδος της οποίας οι όροι είναι όλοι ακέραιοι περιέχει μια (άπειρη) γεωμετρική πρόοδο.

Έστω λοιπόν ότι μας δίνεται η πρόοδος

$$a, a+r, a+2r, \ldots, \tag{17.1.1}$$

όπου οι a, r είναι ακέραιοι. Αν $r = 0$ δεν υπάρχει κάτι να δείξουμε, αφού σε αυτήν την περίπτωση η (17.1.1) είναι η ίδια γεωμετρική πρόοδος (με λόγο 1).

Αν $r < 0$, αρκεί να δείξουμε το ζητούμενο για την πρόοδο που προκύπτει από την αρχική αλλάζοντας το πρόσημο σε κάθε όρο της. Επομένως μπορούμε να υποθέσουμε ότι $r > 0$. Μπορούμε ακόμη να υποθέσουμε ότι $\gcd(a, r) = 1$. Αν αυτό δεν συμβαίνει και έχουμε $d = \gcd(a, r) > 1$, τότε $a = da'$, $r = dr'$, όπου $\gcd(a', r') = 1$, οπότε αρκεί να δείξουμε το ζητούμενο για την πρόοδο $a', a'+r', a'+2r', \ldots$

Τέλος, εφ' όσον $r > 0$, από ένα σημείο και έπειτα όλοι οι όροι της (17.1.1) είναι μεγαλύτεροι του 1. Μπορούμε δηλαδή να υποθέσουμε, εξαιρώντας μερικούς αρχικούς όρους αν χρειάζεται, ότι $a > 1$. Επειδή τώρα $\gcd(a, r) = 1$, το Θεώρημα του Euler μας επιτρέπει να γράψουμε $a^{\phi(r)} \equiv 1 \pmod{r}$ και άρα $a^{n\phi(r)} \equiv 1 \pmod{r}$ για κάθε φυσικό n. Επομένως ο $k_n = (aa^{n\phi(r)} - a)/r$ είναι ακέραιος για κάθε φυσικό n. Όμως $a + k_n r = a(a^{\phi(r)})^n$ για $n = 1, 2, \ldots$, οπότε, εφ' όσον $a > 0$, έχουμε ότι $0 \leqslant k_1 < k_2 < \ldots$ και οι $a + k_n r$ για n φυσικό σχηματίζουν γεωμετρική πρόοδο. ■

Για $a = 3$ και $r = 4$ για παράδειγμα, η Εφαρμογή 17.1.5 μας λέει ότι η αριθμητική πρόοδος

$$3, 7, 11, 15, 19, 23, 27, \ldots$$

περιέχει την γεωμετρική πρόοδο

$$27, 243, 2187, 19683, 177147, \ldots$$

της οποίας ο γενικός όρος είναι ο $3 \cdot 9^n$.

Το επόμενο αποτέλεσμα, το οποίο οφείλεται στον Ούγγρο László Rédei (1900−1980), γενικεύει το Θεώρημα του Euler.

Θεώρημα 17.1.6 (Το Θεώρημα του Rédei). *Για κάθε φυσικό $n > 1$ και κάθε ακέραιο a ισχύει ότι*

$$a^n \equiv a^{n-\phi(n)} \pmod{n}.$$

Απόδειξη. Έστω $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ η κανονική μορφή του φυσικού n και i ένας από τους αριθμούς $1, 2, \ldots, r$. Αν $\gcd(a, p_i) = 1$ τότε

$$a^{\phi(p_i^{k_i})} \equiv 1 \left(\mathrm{mod}\ p_i^{k_i}\right).$$

Όμως $\phi(p_i^{k_i}) \mid \phi(n)$ από το Πόρισμα 16.2.5, επομένως

$$a^{\phi(n)} \equiv 1 \left(\mathrm{mod}\ p_i^{k_i}\right).$$

Παρατηρούμε τώρα ότι, αν ο $x \geqslant 2$ είναι φυσικός, τότε $x^{b-1} \geqslant b$ για κάθε φυσικό b. Αυτό αποδεικνύεται εύκολα, για παράδειγμα, με επαγωγή. Από την άλλη, για κάθε $i \in \{1, 2, \ldots, r\}$

έχουμε ότι $p_i^{k_i-1} \mid n$ και $p_i^{k_i-1} \mid \phi(n)$. Προκύπτει ότι $p_i^{k_i-1} \mid n-\phi(n)$. Εφ' όσον $n-\phi(n)>0$ για $n>1$, έχουμε ότι

$$n-\phi(n) \geqslant p_i^{k_i-1} \geqslant k_i.$$

Άρα αν $\gcd(a,p_i)>1$, δηλαδή αν $p_i \mid a$, τότε $p_i^{k_i} \mid p_i^{n-\phi(n)} \mid a^{n-\phi(n)}$.

Συμπεραίνουμε ότι για κάθε ακέραιο a και για κάθε δείκτη $i \in \{1,2,\ldots,r\}$ ισχύει η

$$p_i^{k_i} \mid a^{n-\phi(n)}(a^{\phi(n)}-1).$$

Έπεται ότι

$$n \mid a^{n-\phi(n)}(a^{\phi(n)}-1)$$

που είναι ισοδύναμη με την σχέση που θέλαμε να δείξουμε. ■

Κλείνουμε το θεωρητικό κομμάτι του μαθήματος επισημαίνοντας την χρησιμότητα του Θεωρήματος του Euler σε ό,τι αφορά στην εύρεση πολλαπλασιαστικών αντιστρόφων και στην επίλυση γραμμικών ισοτιμιών. Συγκεκριμένα, αν οι a, n είναι σχετικά πρώτοι, τότε το Θεώρημα 17.1.2 μας δίνει

$$a \cdot a^{\phi(n)-1} \equiv a^{\phi(n)} \equiv 1 \pmod{n}.$$

Μπορούμε επομένως να συμπεράνουμε ότι ο $a^{\phi(n)-1} \pmod{n}$ είναι ο πολλαπλασιαστικός αντίστροφος του $a \pmod{n}$. Για παράδειγμα έχουμε ότι

$$2^{\phi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod{9}$$

και άρα ο πολλαπλασιαστικός αντίστροφος του $2 \pmod 9$ είναι ο $5 \pmod 9$.

Αυτή η παρατήρηση μας επιτρέπει ακόμα να λύνουμε γραμμικές ισοτιμίες. Υποθέτουμε πάλι ότι οι a, n είναι σχετικά πρώτοι και αναζητούμε την λύση της γραμμικής ισοτιμίας $ax \equiv b \pmod{n}$. Πολλαπλασιάζοντας με $a^{\phi(n)-1}$, παίρνουμε

$$a^{\phi(n)-1}ax \equiv a^{\phi(n)-1}b \pmod{n}.$$

Επομένως η λύση της ισοτιμίας είναι η $x \equiv a^{\phi(n)-1}b \pmod{n}$. Για παράδειγμα η λύση της $3x \equiv 7 \pmod{10}$ είναι η

$$x \equiv 3^{\phi(10)-1} \cdot 7 \equiv 3^3 \cdot 7 \equiv 9 \pmod{10},$$

αφού $\phi(10)=4$.

17.2 Ασκήσεις

Άσκηση 17.2.1. Να δείξετε ότι αν ο n είναι περιττός φυσικός τότε $2^{n!} \equiv 1 \pmod{n}$.

Απόδειξη. Εφ' όσον ο n είναι περιττός, έχουμε $\gcd(2,n)=1$. Το Θεώρημα του Euler μας δίνει $2^{\phi(n)} \equiv 1 \pmod{n}$. Όμως $\phi(n) \leqslant n$ και άρα $\phi(n) \mid n!$. Αν $n! = t\phi(n)$, όπου t φυσικός, τότε $(2^{\phi(n)})^t \equiv 1^t \equiv 1 \pmod{n}$, δηλαδή $2^{n!} \equiv 1 \pmod{n}$, όπως θέλαμε να δείξουμε. ■

Άσκηση 17.2.2. Αν οι m, n είναι σχετικά πρώτοι φυσικοί, να δείξετε ότι

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

Απόδειξη. Από το Θεώρημα του Euler έχουμε $m^{\phi(n)} \equiv 1 \pmod{n}$, ενώ προφανώς ισχύει ότι $n^{\phi(m)} \equiv 0 \pmod{n}$. Προσθέτοντας τις δύο αυτές ισοτιμίες παίρνουμε την $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{n}$. Με παρόμοιο τρόπο αποδεικνύουμε ότι $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{m}$. Επειδή όμως $\gcd(m, n) = 1$, έχουμε την ενιαία ισοτιμία $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$, που ήταν και το ζητούμενο. ■

Άσκηση 17.2.3. Αποδείξτε ότι, αν οι a, n είναι φυσικοί τέτοιοι που $\gcd(a, n) = \gcd(a-1, n) = 1$, τότε

$$1 + a + a^2 + \ldots + a^{\phi(n)-1} \equiv 0 \pmod{n}.$$

Απόδειξη. Από το Θεώρημα του Euler έχουμε ότι

$$(a-1)(1 + a + a^2 + \ldots + a^{\phi(n)-1}) \equiv a^{\phi(n)} - 1 \equiv 0 \pmod{n}.$$

Όμως $\gcd(a-1, n) = 1$ και άρα $n \mid (1 + \ldots + a^{\phi(n)-1})$, όπως θέλαμε. ■

Άσκηση 17.2.4. Να δείξετε ότι ένας φυσικός ο οποίος δεν διαιρείται ούτε με τον 2 ούτε με τον 5 είναι διαιρέτης ενός φυσικού του οποίου τα δεκαδικά ψηφία είναι όλα ίσα με 1.

Απόδειξη. Εξ υποθέσεως έχουμε $\gcd(n, 10) = 1$ και άρα $\gcd(9n, 10) = 1$. Η τελευταία ισότητα φαίνεται και άμεσα, αλλά προκύπτει και από το Λήμμα 16.2.3 για παράδειγμα. Από το Θεώρημα του Euler τώρα έχουμε

$$10^{\phi(9n)} \equiv 1 \pmod{9n}.$$

Συμπεραίνουμε ότι υπάρχει φυσικός k τέτοιος ώστε $nk = (10^{\phi(9n)} - 1)/9$. Τα ψηφία αυτού του αριθμού είναι όλα ίσα με 1 και άρα το ζητούμενο έχει δειχθεί. ■

Άσκηση 17.2.5. Να δείξετε ότι η ισοτιμία

$$n^9 \equiv n^3 \pmod{504}$$

ισχύει για κάθε φυσικό n.

Απόδειξη. Παρατηρούμε αρχικά ότι $504 = 2^3 \cdot 3^2 \cdot 7$ και άρα θα είναι αρκετό να δείξουμε τις

$$n^9 \equiv n^3 \pmod{7}, \qquad n^9 \equiv n^3 \pmod{8}, \qquad n^9 \equiv n^3 \pmod{9}$$

για κάθε φυσικό n.

Από το Θεώρημα του Fermat έχουμε ότι $n^7 \equiv n \pmod{7}$, οπότε πολλαπλασιάζουμε με n^2 και παίρνουμε $n^9 \equiv n^3 \pmod{7}$.

Για το μέτρο 8 διακρίνουμε περιπτώσεις: αν ο n είναι άρτιος, τότε $n^3 \equiv 0 \pmod{8}$ και άρα $n^9 \equiv 0 \equiv n^3 \pmod{8}$. Αν από την άλλη ο n είναι περιττός, τότε $n^2 \equiv 1 \pmod{8}$ από το Παράδειγμα 2.1.3, οπότε και $n^8 \equiv 1 \pmod{8}$. Συμπεραίνουμε ότι $n^9 \equiv n \equiv n^3 \pmod{8}$ και άρα η $n^9 \equiv n^3 \pmod{8}$ ισχύει σε κάθε περίπτωση.

Τέλος, για το μέτρο 9 χρησιμοποιούμε το Θεώρημα του Rédei το οποίο μας δίνει

$$n^9 \equiv n^{9-\phi(9)} \equiv n^{9-6} \equiv n^3 \pmod{9}$$

για κάθε φυσικό n. Η απόδειξη έχει τελειώσει. ■

Άσκηση 17.2.6. Έστω $n > 1$ φυσικός και a ακέραιος σχετικά πρώτος με τον n. Να δείξετε ότι, αν ο k είναι ο ελάχιστος φυσικός τέτοιος ώστε $a^k \equiv 1 \pmod{n}$, τότε $a^h \equiv 1 \pmod{n}$, αν και μόνο αν $k \mid h$. Συγκεκριμένα, έχουμε ότι $k \mid \phi(n)$.

Απόδειξη. Υποθέτουμε αρχικά ότι $k \mid h$ έτσι ώστε $h = jk$ για κάποιον ακέραιο j. Επειδή $a^k \equiv 1 \pmod{n}$, έχουμε ότι $(a^k)^j \equiv 1^j \pmod{n}$, δηλαδή $a^h \equiv 1 \pmod{n}$. Αντίστροφα, έστω h φυσικός που ικανοποιεί την $a^h \equiv 1 \pmod{n}$. Από τον Αλγόριθμο της Διαίρεσης, υπάρχουν q και r τέτοιοι ώστε $h = qk + r$, όπου $0 \leqslant r < k$. Επομένως

$$a^h = a^{qk+r} = (a^k)^q a^r.$$

Έχουμε εξ υποθέσεως ότι

$$a^h \equiv 1 \pmod{n} \qquad \text{και} \qquad a^k \equiv 1 \pmod{n}$$

οι οποίες συνεπάγονται την $a^r \equiv 1 \pmod{n}$. Εφ' όσον $0 \leqslant r < k$, συμπεραίνουμε ότι $r = 0$. Διαφορετικά, ο ορισμός του k ως ελάχιστου φυσικού τέτοιου ώστε $a^k \equiv 1 \pmod{n}$ παραβιάζεται. Επομένως $h = qk$ και άρα $k \mid h$, όπως θέλαμε να δείξουμε. ■

Άσκηση 17.2.7. Να δείξετε ότι, αν οι m, a, r είναι φυσικοί με $\gcd(a, r) = 1$ και S είναι ένα άπειρο σύνολο όρων της αριθμητικής προόδου $a + kr$, $k = 1, 2, \ldots$, τότε η πρόοδος περιέχει όρους οι οποίοι είναι γινόμενα περισσότερων από m διακεκριμένων στοιχείων του S.

Απόδειξη. Επιλέγουμε $s = m\phi(r) + 1$ διακεκριμένους αριθμούς από το σύνολο S, έστω τους $t_1, t_2, \ldots, t_s$. Αυτοί οι ακέραιοι, εφ' όσον είναι όροι της αριθμητικής προόδου $(a + kr)$, είναι όλοι ισότιμοι με $a \pmod{r}$. Επομένως

$$t_1 t_2 \ldots t_s \equiv a^s \equiv a \cdot a^{m\phi(r)} \pmod{r}.$$

Από το Θεώρημα του Euler και λαμβάνοντας υπ' όψιν ότι $\gcd(a, r) = 1$, έχουμε ότι $a^{\phi(r)} \equiv 1 \pmod{r}$. Συμπερασματικά

$$t_1 t_2 \ldots t_s \equiv a \pmod{r},$$

δηλαδή το γινόμενο $t_1 t_2 \ldots t_s$ είναι όρος της αριθμητικής προόδου $(a + kr)$. Επιπλέον $s = m\phi(r) + 1 > m$, οπότε το ζητούμενο έχει δειχθεί. ■

Άσκηση 17.2.8. Περιγράψτε την ακολουθία που ορίζεται μέσω των

$$a_1 = 3 \qquad \text{και} \qquad a_n = 3^{a_{n-1}} \pmod{100}$$

για μεγάλες τιμές του n.

Λύση. Έχουμε $a_1 = 3$, $a_2 = 3^3 = 27$, $a_3 = 3^{27} \pmod{100}$ και θέλουμε σε αυτό το σημείο να υπολογίσουμε τον a_3. Γνωρίζουμε ότι

$$3^{\phi(100)} \equiv 3^{40} \equiv 1 \pmod{100}.$$

Γνωρίζουμε επίσης από την Άσκηση 17.2.6 ότι ο ελάχιστος φυσικός s που είναι τέτοιος ώστε $3^s \equiv 1 \pmod{100}$ είναι θετικός διαιρέτης του $\phi(100) = 40$. Οι θετικοί διαιρέτες του 40 είναι οι $\{1, 2, 4, 5, 8, 10, 20, 40\}$. Κάνοντας μερικές πράξεις, οι οποίες συνοψίζονται στον Πίνακα 17.2.1, βλέπουμε ότι $s = 20$.[1]

[1] Στην πραγματικότητα, οι πράξεις οι οποίες χρειάζονται είναι λίγες. Τις τέσσερις πρώτες τιμές του Πίνακα 17.2.1 μπορούμε να τις βρούμε χωρίς καμία πράξη ουσιαστικά. Το να βρούμε τους $3^8 \pmod{100}$, $3^{10} \pmod{100}$ και $3^{20} \pmod{100}$ είναι στην συνέχεια ζήτημα μίας ύψωσης στο τετράγωνο.

Πίνακας 17.2.1: Η τάξη του 3 (mod 100)

d	1	2	4	5	8	10	20	40
$3^d \pmod{100}$	3	9	81	43	61	49	1	1

Έχουμε λοιπόν ότι

$$a_3 \equiv 3^{27} \equiv 3^{20} \cdot 3^7 \equiv 3^4 \cdot 3^3 \equiv 81 \cdot 27 \equiv 87 \pmod{100}.$$

Προκύπτει εύκολα τώρα ότι

$$3^{87} \equiv (3^{20})^4 \cdot 3^7 \equiv 1^4 \cdot 87 \equiv 87 \pmod{100}$$

και άρα $a_n = 87$ για κάθε $n \geqslant 3$. ■

Άσκηση 17.2.9. Βρείτε τις λύσεις της ισοτιμίας $x^x \equiv 3 \pmod{10}$ στους φυσικούς x.

Λύση. Αν ένας φυσικός x ικανοποιεί την ισοτιμία, τότε, εφ' όσον $\gcd(3, 10) = 1$, θα έχουμε $\gcd(x, 10) = 1$ και άρα $\gcd(x + 20k, 10) = 1$ για κάθε φυσικό k. Λαμβάνοντας υπ' όψιν μας ότι $\phi(10) = 4$, το Θεώρημα του Euler μας δίνει ότι $(x + 20k)^4 \equiv 1 \pmod{10}$, οπότε και $(x + 20k)^{20k} \equiv 1 \pmod{10}$. Από την άλλη, η ισοτιμία $(x + 20k)^x \equiv x^x \pmod{10}$ ισχύει προφανώς για κάθε φυσικό x. Πολλαπλασιάζοντας τις δύο αυτές ισοτιμίες, παίρνουμε

$$(x + 20k)^{x+20k} \equiv x^x \pmod{10}$$

για κάθε φυσικό k. Αν τώρα ο x ικανοποιεί την $x^x \equiv 3 \pmod{10}$, τότε όλοι οι όροι της $(x+20k)$ επίσης την ικανοποιούν. Ελέγχουμε με υπολογισμούς ότι οι μόνοι ακέραιοι x με $0 \leqslant x < 20$ που ικανοποιούν την ισοτιμία είναι οι $x = 7$ και $x = 13$. Συμπεραίνουμε ότι οι λύσεις της $x^x \equiv 3 \pmod{10}$ είναι οι φυσικοί $7 + 20k$ και $13 + 20k$ για $k \in \mathbb{N}$. ■

Άσκηση 17.2.10. $(*)$ Να δείξετε ότι η ακολουθία $a_n = 2^n - 3, n > 1$ περιέχει μία υπακολουθία φυσικών, οι όροι της οποίας είναι σχετικά πρώτοι ανά δύο.

Υπόδειξη: Αν έχουμε βρει ένα σύνολο k όρων $\{a_{n_1}, a_{n_2}, \ldots, a_{n_k}\}$ οι οποίοι είναι σχετικά πρώτοι ανά δύο, τότε μπορούμε να επισυνάψουμε σε αυτό το σύνολο τον όρο $2^{\phi(a_{n_1} \cdots a_{n_k})} - 3$. Δείξτε ότι το νέο αυτό σύνολο εξακολουθεί να αποτελείται από όρους της ακολουθίας που είναι σχετικά πρώτοι ανά δύο.

Απόδειξη. Εύκολα βρίσκουμε 2 όρους της ακολουθίας που είναι σχετικά πρώτοι. Μπορούμε για παράδειγμα να διαλέξουμε τους $a_2 = 1$ και $a_3 = 5$. Ακολουθώντας την υπόδειξη, υποθέτουμε ότι έχουμε βρει ένα σύνολο k όρων $\{a_{n_1}, a_{n_2}, \ldots, a_{n_k}\}$ οι οποίοι είναι σχετικά πρώτοι ανά δύο και ας συμβολίσουμε το γινόμενο αυτών των όρων με s_k, δηλαδή $s_k = a_{n_1} \cdots a_{n_k}$. Ισχυριζόμαστε ότι ο $b = 2^{\phi(s_k)} - 3$ είναι σχετικά πρώτος με τον $a_{n_i} = 2^{n_i} - 3$ για κάθε $i \leqslant k$. Παρατηρούμε ότι ο s_k είναι γινόμενο περιττών και άρα και ο ίδιος περιττός. Επομένως $\gcd(2, s_k) = 1$. Από το Θεώρημα του Euler προκύπτει ότι $2^{\phi(s_k)} \equiv 1 \pmod{s_k}$, δηλαδή $s_k \mid 2^{\phi(s_k)} - 1$. Έστω τώρα $i \in \{1, 2, \ldots, k\}$ τυχαίος δείκτης. Ας υποθέσουμε ότι $d = \gcd(a_{n_i}, b) > 1$. Εφ' όσον $d \mid a_{n_i} \mid s_k \mid 2^{\phi(s_k)} - 1$ και $d \mid b$, έχουμε ότι $d \mid (2^{\phi(s_k)} - 1) - b = 2$, δηλαδή $d = 2$, που είναι άτοπο, αφού $d \mid a_{n_i}$ και ο a_{n_i} είναι περιττός. Συμπεραίνουμε ότι ο $b > 1$ είναι σχετικά πρώτος με όλους τους a_{n_i} και άρα επεκτείνει το αρχικό μας σύνολο. Από την στιγμή που μπορούμε να κάνουμε το σύνολο όσο μεγάλο θέλουμε, το ζητούμενο έχει δειχθεί. ■

Κεφάλαιο 18

18η Παράδοση

Το παρόν και τα επόμενα δύο μαθήματα είναι αφιερωμένα στην θεωρία των πρωταρχικών ριζών. Σήμερα, συγκεκριμένα, θα αναφερθούμε στην έννοια της «τάξης» ενός ακεραίου και στην έννοια της πρωταρχικής ρίζας.

18.1 Η τάξη ενός ακεραίου

Από το Θεώρημα του Euler γνωρίζουμε ότι $a^{\phi(n)} \equiv 1 \pmod{n}$, όταν ισχύει ότι $\gcd(a, n) = 1$. Συμβαίνει συχνά όμως (δείτε και την Άσκηση 17.2.8) δυνάμεις του a μικρότερες του $a^{\phi(n)}$ να είναι ισότιμες με 1 ως προς το μέτρο n. Αυτό μας οδηγεί στον ακόλουθο ορισμό.

Ορισμός 18.1.1. Έστω $n > 1$ φυσικός και a ακέραιος σχετικά πρώτος με τον n. Η **τάξη του a ως προς το μέτρο n** είναι ο ελάχιστος φυσικός k που είναι τέτοιος ώστε $a^k \equiv 1 \pmod{n}$.

Αν θεωρήσουμε για παράδειγμα τις διαδοχικές δυνάμεις του 2 ως προς το μέτρο 7, θα πάρουμε τις ισοτιμίες

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 1, \quad 2^4 \equiv 2, \quad 2^5 \equiv 4, \quad 2^6 \equiv 1, \quad \dots$$

από τις οποίες προκύπτει ότι ο 2 έχει τάξη 3 ως προς το μέτρο 7. Παρατηρήστε ότι, αν δύο ακέραιοι είναι ισότιμοι ως προς κάποιο μέτρο n, τότε έχουν την ίδια τάξη ως προς αυτό το μέτρο. Αυτό ισχύει γιατί, αν $a \equiv b \pmod{n}$ και $a^k \equiv 1 \pmod{n}$, τότε το Θεώρημα 8.1.3 μας επιτρέπει να συμπεράνουμε ότι $a^k \equiv b^k \pmod{n}$, και άρα $b^k \equiv 1 \pmod{n}$. Εφιστούμε την προσοχή ως προς το εξής: ο ορισμός της τάξης ενός ακεραίου ως προς κάποιο μέτρο n αφορά μόνο σε εκείνους τους ακεραίους που είναι σχετικά πρώτοι ως προς το μέτρο n.

Πράγματι, αν $\gcd(a, n) > 1$, τότε γνωρίζουμε από το Θεώρημα 9.3.1 ότι η γραμμική ισοτιμία $ax \equiv 1 \pmod{n}$ δεν έχει καμία λύση, επομένως η σχέση

$$a^k \equiv 1 \pmod{n} \qquad k \geqslant 1$$

δεν είναι δυνατόν να ισχύει, αφού διαφορετικά ο $x = a^{k-1}$ θα ήταν λύση της $ax \equiv 1 \pmod{n}$. Άρα, όποτε κάνουμε αναφορά στην τάξη του a ως προς το μέτρο n, υποθέτουμε (ακόμα κι αν δεν το αναφέρουμε ρητά) ότι $\gcd(a, n) = 1$.

Είδαμε προηγουμένως ότι $2^k \equiv 1 \pmod{7}$ όποτε ο k είναι πολλαπλάσιο του 3, όπου 3 είναι η τάξη του 2 ως προς το μέτρο 7. Στο ακόλουθο θεώρημα, το οποίο συναντήσαμε προηγουμένως ως Άσκηση 17.2.6, βλέπουμε ότι αυτό είναι ενδεικτικό μιας γενικότερης κατάστασης.

Αναδιατυπώνουμε απλώς το περιεχόμενο εκείνης της άσκησης ως θεώρημα και παραλείπουμε την απόδειξη την οποία έχουμε ήδη δώσει.

Θεώρημα 18.1.2. *Αν ο ακέραιος a έχει τάξη k ως προς το μέτρο n, τότε $a^h \equiv 1 \pmod{n}$, αν και μόνο αν $k \mid h$. Συγκεκριμένα, έχουμε ότι $k \mid \phi(n)$.*

Το Θεώρημα 18.1.2 επιταχύνει τον υπολογισμό όταν προσπαθούμε να βρούμε την τάξη ενός ακέραιου a ως προς κάποιο μέτρο n. Αντί να εξετάσουμε όλες τις δυνάμεις του a, μπορούμε να αναζητήσουμε τον προς εύρεσιν εκθέτη μεταξύ των διαιρετών του $\phi(n)$. Ας βρούμε, ενδεικτικά, την τάξη του 2 ως προς το μέτρο 13.

Εφ' όσον $\phi(13) = 12$, η τάξη του 2 ισούται με κάποιον ακέραιο εκ των $1, 2, 3, 4, 6, 12$. Από τις

$$2^1 \equiv 2 \quad 2^2 \equiv 4 \quad 2^3 \equiv 8 \quad 2^4 \equiv 3 \quad 2^6 \equiv 12 \quad 2^{12} \equiv 1 \pmod{13}$$

βλέπουμε ότι η τάξη του 2 ως προς το μέτρο 13 ισούται με 12.

Για έναν αυθαίρετα επιλεγμένο διαιρέτη d του $\phi(n)$, δεν είναι πάντα αλήθεια ότι υπάρχει ένας ακέραιος a με τάξη d ως προς το μέτρο n. Ένα παράδειγμα είναι το $n = 12$. Εδώ $\phi(12) = 4$, αλλά δεν υπάρχει ακέραιος με τάξη 4 ως προς το μέτρο 12. Πράγματι, βλέπουμε ότι

$$1^1 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

και ως εκ τούτου οι μόνες τάξεις είναι οι 1 και 2. Μία ακόμη βασική ιδιότητα των τάξεων είναι η ακόλουθη.

Θεώρημα 18.1.3. *Αν η τάξη του ακεραίου a είναι k ως προς το μέτρο n, τότε $a^i \equiv a^j \pmod{n}$, αν και μόνο αν $i \equiv j \pmod{k}$.*

Απόδειξη. Ας υποθέσουμε αρχικά ότι $a^i \equiv a^j \pmod{n}$, όπου $i \geqslant j$. Εφ' όσον ο a είναι σχετικά πρώτος με τον n, δυνάμεις του a μπορούν να απλοποιηθούν, οπότε και παίρνουμε την $a^{i-j} \equiv 1 \pmod{n}$. Λόγω του Θεωρήματος 18.1.2, αυτή η ισοτιμία ισχύει, αν και μόνο αν $k \mid i - j$, δηλαδή αν και μόνο αν $i \equiv j \pmod{k}$. Αντίστροφα, έστω ότι $i \equiv j \pmod{k}$. Έχουμε τότε ότι $i = j + qk$ για κάποιον ακέραιο q. Από τον ορισμό του k έχουμε ότι $a^k \equiv 1 \pmod{n}$ και άρα

$$a^i \equiv a^{j+qk} \equiv a^j (a^k)^q \equiv a^j \pmod{n},$$

που είναι αυτό που θέλαμε να δείξουμε. ■

Πόρισμα 18.1.4. *Αν ο ακέραιος a έχει τάξη k ως προς το μέτρο n, τότε οι ακέραιοι $a, a^2, \ldots, a^k$ είναι ανισότιμοι ως προς το μέτρο n.*

Απόδειξη. Αν $a^i \equiv a^j \pmod{n}$ για $1 \leqslant i \leqslant j \leqslant k$, τότε το Θεώρημα 18.1.3 μας εξασφαλίζει ότι $i \equiv j \pmod{k}$. Αυτό όμως είναι δυνατό, μόνο αν $i = j$. ■

Το ακόλουθο ερώτημα προκύπτει τώρα με φυσικό τρόπο: μπορούμε να εκφράσουμε την τάξη μιας ακέραιας δύναμης του a συναρτήσει της τάξης του a; Η απάντηση σε αυτό το ερώτημα είναι το περιεχόμενο του επόμενου θεωρήματος.

Θεώρημα 18.1.5. *Αν ο ακέραιος a έχει τάξη k ως προς το μέτρο n και $h > 0$, τότε ο a^h έχει τάξη $k/\gcd(h, k)$ ως προς το μέτρο n.*

Απόδειξη. Έστω $d = \gcd(h, k)$. Μπορούμε τότε να γράψουμε $h = h_1 d$ και $k = k_1 d$, όπου $\gcd(h_1, k_1) = 1$. Είναι τώρα σαφές ότι

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 \pmod{n}.$$

Αν ο a^h έχει τάξη r ως προς το μέτρο n, τότε σύμφωνα με το Θεώρημα 18.1.2 ισχύει ότι $r \mid k_1$. Από την άλλη, εφ' όσον ο a έχει τάξη k ως προς το μέτρο n, η ισοτιμία

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

μας δίνει ότι $k \mid hr$. Δηλαδή, $k_1 d \mid h_1 dr$ ή $k_1 \mid h_1 r$. Όμως $\gcd(k_1, h_1) = 1$ και άρα $k_1 \mid r$. Αυτή η σχέση διαιρετότητας, σε συνδυασμό με την προηγούμενη, δίνουν

$$r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h, k)}.$$

Η απόδειξη έχει ολοκληρωθεί. ■

Το επόμενο αποτέλεσμα είναι άμεση συνέπεια του θεωρήματος που μόλις δείξαμε.

Πόρισμα 18.1.6. *Έστω ότι ο ακέραιος a έχει τάξη k ως προς το μέτρο n. Τότε ο a^h έχει επίσης τάξη k, αν και μόνο αν $\gcd(h, k) = 1$.*

Ας δούμε με ένα συγκεκριμένο παράδειγμα πώς δουλεύουν όσα έχουμε περιγράψει στα δύο τελευταία αποτελέσματα.

Παράδειγμα 18.1.7. Στον Πίνακα 18.1.1 εμφανίζονται οι τάξεις ως προς το μέτρο 13 των φυσικών που είναι μικρότεροι του 13.

Πίνακας 18.1.1: Οι τάξεις των θετικών υπολοίπων (mod 13)

Υπόλοιπο	1	2	3	4	5	6	7	8	9	10	11	12
Τάξη	1	12	3	6	4	12	12	4	3	6	12	2

Παρατηρούμε ότι η τάξη του 2 ως προς το μέτρο 13 είναι 12, ενώ οι τάξεις των 2^2 και 2^3 είναι 6 και 4 αντίστοιχα, αφού

$$6 = \frac{12}{\gcd(2, 12)} \quad \text{και} \quad 4 = \frac{12}{\gcd(3, 12)},$$

σε συμφωνία με το Θεώρημα 18.1.5. Οι ακέραιοι οι οποίοι επίσης έχουν τάξη 12 ως προς το μέτρο 13 είναι οι δυνάμεις 2^k για τις οποίες $\gcd(k, 12) = 1$, δηλαδή οι

$$2^1 \equiv 2 \pmod{13}, \quad 2^5 \equiv 6 \pmod{13}, \quad 2^7 \equiv 11 \pmod{13}, \quad 2^{11} \equiv 7 \pmod{13}.$$

18.2 Η έννοια της πρωταρχικής ρίζας

Αν ένας ακέραιος a έχει την μεγαλύτερη δυνατή τάξη, τότε καλείται πρωταρχική ρίζα του n.

Ορισμός 18.2.1. Αν $\gcd(a, n) = 1$ και ο a έχει τάξη $\phi(n)$ ως προς το μέτρο n, τότε ο a καλείται **πρωταρχική ρίζα** του n.

Για να το πούμε διαφορετικά, ο n έχει τον a ως πρωταρχική ρίζα, αν $a^{\phi(n)} \equiv 1 \pmod{n}$, αλλά $a^k \not\equiv 1 \pmod{n}$ για κάθε φυσικό $k < \phi(n)$. Μπορούμε για παράδειγμα να δούμε ότι ο 3 είναι πρωταρχική ρίζα του 7, αφού

$$3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4 \quad 3^5 \equiv 5 \quad 3^6 \equiv 1 \pmod{7}.$$

Πιο γενικά, μπορούμε να δείξουμε ότι πρωταρχικές ρίζες υπάρχουν για κάθε μέτρο που είναι πρώτος και αυτό είναι ένα κεντρικό αποτέλεσμα. Παρόλο που ο n μπορεί να έχει πρωταρχική ρίζα χωρίς να είναι πρώτος (για παράδειγμα ο 2 είναι πρωταρχική ρίζα του 9), δεν έχουμε λόγο γενικά να αναμένουμε ότι ένας ακέραιος n έχει πρωταρχική ρίζα. Πράγματι, η ύπαρξη πρωταρχικών ριζών είναι περισσότερο η εξαίρεση παρά ο κανόνας.

Παράδειγμα 18.2.2. Θα δείξουμε ότι αν ο $F_n = 2^{2^n} + 1$, όπου $n > 1$, είναι πρώτος, τότε ο 2 δεν είναι πρωταρχική ρίζα του F_n. (Παρατηρούμε ότι ο 2 *είναι* πρωταρχική ρίζα του $5 = F_1$.) Από την παραγοντοποίηση $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$ έχουμε ότι

$$2^{2^{n+1}} \equiv 1 \pmod{F_n}$$

και άρα η τάξη του 2 ως προς το μέτρο F_n είναι το πολύ 2^{n+1}. Εφ' όσον όμως ο F_n είναι πρώτος, έχουμε ότι

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

και ένα εύκολο επαγωγικό επιχείρημα δείχνει ότι $2^{2^n} > 2^{n+1}$ για $n > 1$. Επομένως η τάξη του 2 ως προς το μέτρο F_n είναι μικρότερη από $\phi(F_n)$ και άρα, λόγω του Ορισμού 18.2.1, έχουμε ότι ο 2 δεν μπορεί να είναι πρωταρχική ρίζα του F_n.

Μία από τις βασικές αρετές των πρωταρχικών ριζών βρίσκεται στο επόμενο θεώρημα.

Θεώρημα 18.2.3. *Έστω ότι* $\gcd(a, n) = 1$ *και ότι οι* $a_1, a_2, \ldots, a_{\phi(n)}$ *είναι οι φυσικοί που είναι μικρότεροι του* n *και σχετικά πρώτοι με τον* n*. Αν ο* a *είναι πρωταρχική ρίζα του* n*, τότε οι*

$$a, a^2, \ldots, a^{\phi(n)}$$

είναι ισότιμοι ως προς το μέτρο n *με τους* $a_1, a_2, \ldots, a_{\phi(n)}$ *σε κάποια σειρά.*

Απόδειξη. Εφ' όσον ο a είναι σχετικά πρώτος με τον n, το ίδιο ισχύει για κάθε δύναμη του a. Επομένως κάθε a^k είναι ισότιμος ως προς το μέτρο n με κάποιον από τους a_i. Οι $\phi(n)$ αριθμοί του συνόλου $\{a, a^2, \ldots, a^{\phi(n)}\}$ είναι ανά δύο ανισότιμοι από το Πόρισμα 18.1.4, επομένως είναι μια αναδιάταξη των $a_1, a_2, \ldots, a_{\phi(n)}$. ■

Μία συνέπεια αυτού που μόλις δείξαμε, είναι ότι μπορούμε να προσδιορίσουμε ακριβώς το πλήθος των πρωταρχικών ριζών, όταν αυτές υπάρχουν.

Πόρισμα 18.2.4. *Αν ο* n *έχει πρωταρχική ρίζα, τότε έχει ακριβώς* $\phi(\phi(n))$ *πρωταρχικές ρίζες.*

Απόδειξη. Έστω ότι ο a είναι πρωταρχική ρίζα του n. Από το Θεώρημα 18.2.3 κάθε άλλη πρωταρχική ρίζα ανήκει στο σύνολο $\{a, a^2, \ldots, a^{\phi(n)}\}$. Όμως το πλήθος των δυνάμεων a^k, $1 \leqslant k \leqslant \phi(n)$, που έχουν τάξη $\phi(n)$ ισούται με τον αριθμό των φυσικών k που είναι τέτοιοι ώστε $\gcd(k, \phi(n)) = 1$. Υπάρχουν $\phi(\phi(n))$ τέτοιοι φυσικοί και άρα τόσες ακριβώς πρωταρχικές ρίζες. ■

18.3 Ασκήσεις

Άσκηση 18.3.1. Βρείτε τις τάξεις των ακεραίων 2, 3 και 5:

(i) mod 17,

(ii) mod 19,

(iii) mod 23.

Λύση. (i) Η τάξη ενός ακεραίου ως προς το μέτρο 17 διαιρεί τον $\phi(17) = 16$ και άρα ανήκει στο $\{1, 2, 4, 8, 16\}$.

- Παρατηρούμε εύκολα ότι $2^4 = 16 \equiv -1 \pmod{17}$ και άρα $2^8 \equiv 1 \pmod{17}$, οπότε η τάξη του 2 είναι 8.
- Για την τάξη του 3, βλέπουμε ότι $3^4 \equiv 13 \equiv -4 \pmod{17}$, οπότε $3^8 \equiv 16 \equiv -1 \pmod{17}$. Προκύπτει ότι η τάξη του 3 είναι 16, δηλαδή ο 3 είναι πρωταρχική ρίζα του 17.
- Για τον 5 τώρα, έχουμε $5^2 = 25 \equiv 8 \pmod{17}$, άρα $5^4 \equiv 64 \equiv 13 \equiv -4 \pmod{17}$. Επομένως $5^8 \equiv 16 \equiv -1 \pmod{17}$, οπότε η τάξη του 5 είναι 16 και άρα και ο 5 είναι πρωταρχική ρίζα του 17.

Από το Πόρισμα 18.2.4 γνωρίζουμε ότι ο 17 έχει $\phi(\phi(17)) = \phi(16) = 8$ πρωταρχικές ρίζες. Αυτές είναι οι $\{3, 5, 6, 7, 10, 11, 12, 14\}$. Τις δύο πρώτες εξ αυτών τις βρήκαμε παραπάνω.

(ii) Η τάξη ενός ακεραίου ως προς το μέτρο 19 διαιρεί τον $\phi(19) = 18$ και άρα ανήκει στο $\{1, 2, 3, 6, 9, 18\}$. Παρατηρήστε σε αυτό το σημείο ότι, αν ένας ακέραιος a σχετικά πρώτος με τον 19 είναι τέτοιος ώστε $a^6 \not\equiv 1 \pmod{19}$ και $a^9 \not\equiv 1 \pmod{19}$, τότε αναγκαστικά η τάξη του a ως προς το μέτρο 19 ισούται με 18 και άρα ο a είναι πρωταρχική ρίζα του 19.

Αυτό ακριβώς συμβαίνει με τους 2 και 3. Έχουμε δηλαδή

$$a^6 \equiv 7 \pmod{19} \qquad \text{και} \qquad a^9 \equiv 18 \equiv -1 \pmod{19},$$

για $a = 2, 3$. Η τάξη του 5 είναι ίση με 9, αφού $5^3 \equiv 11 \pmod{19}$ και $11^3 \equiv 1 \pmod{19}$. Οι πρωταρχικές ρίζες του 19 είναι οι $\{2, 3, 10, 13, 14, 15\}$ οι οποίες είναι $\phi(18) = 6$ το πλήθος.

(iii) Ως προς το μέτρο 23, παραλείπω τις πράξεις και σας δίνω κατ' ευθείαν το αποτέλεσμα. Η τάξη των 2 και 3 είναι ίση με 11, ενώ ο 5 είναι πρωταρχική ρίζα του 23. Το σύνολο πρωταρχικών ριζών του 23 είναι το $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$. Το σύνολο αυτό έχει $10 = \phi(22)$ στοιχεία, σε συμφωνία με το Πόρισμα 18.2.4. ■

Άσκηση 18.3.2. Δείξτε ότι ο 8 δεν έχει πρωταρχικές ρίζες.

Απόδειξη. Μόνο οι 1, 3, 5, 7 είναι σχετικά πρώτοι με τον 8. Έχουμε ότι $1^2, 3^2, 5^2, 7^2 \equiv 1 \pmod{8}$, αλλά $\phi(8) = 4$. ■

Άσκηση 18.3.3. Δείξτε τις ακόλουθες προτάσεις:

(i) Αν ο ακέραιος a έχει τάξη hk ως προς το μέτρο n, τότε ο a^h έχει τάξη k.

(ii) Αν ο a έχει τάξη $2k$ ως προς το μέτρο p, όπου p περιττός πρώτος, τότε $a^k \equiv -1 \pmod{p}$.

(iii) Αν ο ακέραιος a έχει τάξη $n - 1$ ως προς το μέτρο $n > 1$, τότε ο n είναι πρώτος.

Απόδειξη. (i) Από το Θεώρημα 18.1.5 γνωρίζουμε ότι η τάξη του a^h είναι ίση με

$$\frac{hk}{\gcd(h,hk)} = \frac{hk}{h} = k.$$

(ii) Αν θέσουμε $x = a^k$, τότε, χρησιμοποιώντας πάλι το Θεώρημα 18.1.5, βλέπουμε ότι η τάξη του x είναι ίση με 2 και άρα $x^2 \equiv 1 \pmod{p}$, ενώ $x \not\equiv 1 \pmod{p}$. Άρα $p \mid x^2 - 1 = (x-1)(x+1)$ και από αυτήν την σχέση προκύπτει ότι $p \mid (x-1)$ ή $p \mid (x+1)$. Εφ' όσον $x \not\equiv 1 \pmod{p}$, η πρώτη περίπτωση αποκλείεται, οπότε καταλήγουμε ότι $p \mid (x+1)$, δηλαδή $x \equiv -1 \pmod{p}$, που ήταν αυτό που θέλαμε να δείξουμε.

(iii) Ας συμβολίσουμε με k την τάξη του a ως προς το μέτρο n. Από το Θεώρημα 18.1.2 γνωρίζουμε ότι $k \mid \phi(n) \leqslant n-1$. Εφ' όσον $k = n-1$, έχουμε αναγκαστικά $\phi(n) = n-1$. Δηλαδή, κάθε φυσικός μικρότερος του n είναι σχετικά πρώτος με τον n και αυτό είναι προφανώς ισοδύναμο με το να είναι ο n πρώτος. Το ζητούμενο έχει δειχθεί. ■

Άσκηση 18.3.4. Να δείξετε ότι για όλους τους φυσικούς $a > 1$ και n ισχύει ότι $n \mid \phi(a^n - 1)$.

Απόδειξη. Παρατηρούμε αρχικά ότι $\gcd(a, a^n - 1) = 1$ και ότι για κάθε φυσικό $k < n$ ο $a^k - 1$ είναι αυστηρά μικρότερος του $a^n - 1$ και άρα $a^k \not\equiv 1 \pmod{a^n - 1}$. Επίσης, ισχύει προφανώς ότι $a^n \equiv 1 \pmod{a^n - 1}$. Επομένως η τάξη του a ως προς το μέτρο $a^n - 1$ είναι ίση με n. Επικαλούμαστε πάλι το Θεώρημα 18.1.2 για να συμπεράνουμε ότι $n \mid \phi(a^n - 1)$. ■

Άσκηση 18.3.5. (i) Να δείξετε ότι, αν οι p, q είναι περιττοί πρώτοι και $q \mid a^p - 1$, τότε είτε $q \mid a - 1$ είτε $q = 2kp + 1$ για κάποιον φυσικό k.

Υπόδειξη: Η τάξη του a ως προς το μέτρο q είναι 1 ή p και αν είναι p τότε $p \mid \phi(q)$.

(ii) Χρησιμοποιώντας το (i), να δείξετε ότι, αν ο p είναι περιττός πρώτος, τότε οι πρώτοι διαιρέτες του $2^p - 1$ είναι της μορφής $2kp + 1$.

(iii) Βρείτε τους μικρότερους πρώτους διαιρέτες των $2^{11} - 1$ και $2^{23} - 1$.

Απόδειξη. (i) Παρατηρούμε αρχικά ότι $\gcd(a, q) = 1$. Έστω τώρα r η τάξη του a ως προς το μέτρο q. Μας δίνεται ότι $a^p \equiv 1 \pmod{q}$ και άρα $r \mid p$ από το Θεώρημα 18.1.2. Επομένως $r = 1$ ή $r = p$. Αν $r = 1$, τότε $a \equiv 1 \pmod{q}$, δηλαδή $q \mid a - 1$. Διαφορετικά έχουμε $r = p$, οπότε από το Θεώρημα 18.1.2 και πάλι $p \mid \phi(q) = q - 1$. Άρα $q - 1 = \ell p$ για κάποιον φυσικό ℓ. Εφ' όσον όμως οι p, q είναι περιττοί, θα πρέπει ο ℓ να είναι άρτιος. Μπορούμε να γράψουμε επομένως $\ell = 2k$ για κάποιον φυσικό k, οπότε έχουμε ότι $q = 2kp + 1$.

(ii) Παρατηρούμε ότι κάθε πρώτος διαιρέτης του $2^p - 1$ είναι περιττός και φυσικά δεν διαιρεί τον $2 - 1$. Άρα, παίρνοντας $a = 2$ στο (i), κάθε πρώτος διαιρέτης του $2^p - 1$ είναι της μορφής $2kp + 1$.

(iii) Από το (ii) έχουμε ότι οι πρώτοι διαιρέτες του $2^{11} - 1$ είναι της μορφής $22k + 1$. Δοκιμάζουμε τον 23 και έχουμε $2^4 \equiv -7 \pmod{23}$ και άρα $2^8 \equiv 49 \equiv 3 \pmod{23}$. Πολλαπλασιάζοντας με 8 την τελευταία ισοτιμία παίρνουμε $2^{11} \equiv 24 \equiv 1 \pmod{23}$. Επομένως ο μικρότερος πρώτος διαιρέτης του $2^{11} - 1$ είναι ο 23. Ομοίως, οι πρώτοι διαιρέτες του $2^{23} - 1$ είναι της μορφής $46k + 1$. Δοκιμάζουμε τον 47 και έχουμε $2^5 \equiv 32 \pmod{47}$. Άρα $2^{20} \equiv 32^4 \equiv 37^2 \equiv 6 \pmod{47}$. Πολλαπλασιάζοντας με 8 την τελευταία ισοτιμία, παίρνουμε $2^{23} \equiv 48 \equiv 1 \pmod{47}$. Επομένως ο μικρότερος πρώτος διαιρέτης του $2^{23} - 1$ είναι ο 47. ■

Άσκηση 18.3.6. Να δείξετε ότι ο r είναι πρωταρχική ρίζα ως προς το μέτρο p, όπου p περιττός πρώτος, αν και μόνο αν $\gcd(r,p)=1$ και

$$r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

για κάθε πρώτο διαιρέτη q του $p-1$.

Απόδειξη. Υποθέτουμε αρχικά ότι ο r είναι πρωταρχική ρίζα ως προς το μέτρο p. Τότε εξ ορισμού $\gcd(r,p)=1$. Εφ' όσον τώρα ο p είναι πρώτος, $\phi(p)=p-1$ και $r^{p-1}\equiv 1 \pmod{p}$. Ακόμα, ο $p-1$ είναι η μικρότερη δύναμη k του r για την οποία ισχύει $r^k \equiv 1 \pmod{p}$. Επομένως, αν ο q είναι ένας πρώτος διαιρέτης του $p-1$, τότε $(p-1)/q < p-1$ και άρα

$$r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}\,.$$

Αντίστροφα τώρα, έστω ότι ο r δεν είναι πρωταρχική ρίζα ως προς το μέτρο p. Τότε υπάρχει φυσικός t τέτοιος ώστε $r^t \equiv 1 \pmod{p}$ με $t < p-1$. Εφ' όσον ο t διαιρεί τον $\phi(p)=p-1$, έχουμε $p-1=st$ για κάποιον φυσικό $s>1$ και άρα $(p-1)/s=t$. Έστω q πρώτος διαιρέτης του s. Τότε $(p-1)/q = t(s/q)$, επομένως

$$r^{\frac{p-1}{q}} = r^{t\frac{s}{q}} = (r^t)^{\frac{s}{q}} \equiv 1 \pmod{p}\,.$$

Η απόδειξη έχει ολοκληρωθεί. ■

Άσκηση 18.3.7. Δείξτε ότι ο n δεν διαιρεί τον 2^n-1 για $n>1$ φυσικό.

Απόδειξη. Εφ' όσον ο 2^n-1 είναι περιττός, το ζητούμενο ισχύει προφανώς για n άρτιο. Υποθέτουμε τώρα ότι υπάρχει περιττός n που διαιρεί τον 2^n-1 και καλούμε p τον ελάχιστο πρώτο διαιρέτη του n. Ισχυριζόμαστε αρχικά ότι $\gcd(p-1,n)=1$. Διαφορετικά, επιλέγουμε έναν πρώτο διαιρέτη q του $\gcd(p-1,n)$. Ο q διαιρεί τον n και είναι μικρότερος του p, που είναι άτοπο.

Έστω τώρα d η τάξη του 2 ως προς το μέτρο p. Γνωρίζουμε ότι $d \mid p-1=\phi(p)$. Από την άλλη, εφ' όσον ο n διαιρεί τον 2^n-1 και ο p διαιρεί τον n, έχουμε ότι $2^n \equiv 1 \pmod{p}$. Επομένως ο d διαιρεί τον n και άρα ο d διαιρεί τον $\gcd(p-1,n)=1$. Συμπεραίνουμε ότι $d=1$, άρα και $2\equiv 1 \pmod{p}$, άτοπο. Το ζητούμενο έχει δειχθεί. ■

Άσκηση 18.3.8. $(*)$ Για κάθε ακέραιο a θέτουμε $n_a = 101a - 100\cdot 2^a$. Να δείξετε ότι για $0\leqslant a,b,c,d\leqslant 99$, η σχέση $n_a+n_b \equiv n_c+n_d \pmod{10100}$ συνεπάγεται την $\{a,b\}=\{c,d\}$.

Υπόδειξη: Δείξτε πρώτα ότι ο 2 είναι πρωταρχική ρίζα του 101 και έπειτα χρησιμοποιήστε κατάλληλα το Κινέζικο Θεώρημα Υπολοίπων.

Απόδειξη. Δείχνουμε πρώτα ότι ο 2 είναι πρωταρχική ρίζα του 101. Χρησιμοποιώντας αυτό που δείξαμε στην Άσκηση 18.3.6, αρκεί να δείξουμε ότι

$$2^{50} \not\equiv 1 \pmod{101} \qquad \text{και} \qquad 2^{20} \not\equiv 1 \pmod{101}\,.$$

Έχουμε ότι $2^{10}=1024\equiv 14 \pmod{101}$. Άρα

$$2^{20} \equiv 196 \equiv 95 \pmod{101} \qquad \text{και} \qquad 2^{50} \equiv (-6)^2\cdot 14 \equiv 36\cdot 14 \equiv 100 \pmod{101}\,.$$

Εφ' όσον $2^{20}, 2^{50} \not\equiv 1 \pmod{101}$, ο 2 είναι όντως πρωταρχική ρίζα του 101. Προκύπτει τώρα από το Θεώρημα 18.1.3 ότι $2^a \equiv 2^b \pmod{101}$, αν και μόνο αν $a \equiv b \pmod{101}$, όπου a, b μη αρνητικοί ακέραιοι.

Από το Κινέζικο Θεώρημα Υπολοίπων, η ισοτιμία $n_a + n_b \equiv n_c + n_d \pmod{10100}$ είναι ισοδύναμη με τις

$$a + b \equiv c + d \pmod{100} \tag{18.3.1}$$

και

$$2^a + 2^b \equiv 2^c + 2^d \pmod{101}. \tag{18.3.2}$$

Από το Θεώρημα του Fermat η (18.3.1) συνεπάγεται την $2^{a+b} \equiv 2^{c+d} \pmod{101}$, δηλαδή την

$$2^a 2^b \equiv 2^c 2^d \pmod{101}. \tag{18.3.3}$$

Λύνοντας ως προς 2^b στην (18.3.2) και αντικαθιστώντας στην (18.3.3), παίρνουμε

$$2^a(2^c + 2^d - 2^a) \equiv 2^c 2^d \pmod{101}$$

ή ισοδύναμα

$$0 \equiv (2^a - 2^c)(2^a - 2^d) \pmod{101}.$$

Άρα $2^a \equiv 2^c \pmod{101}$ ή $2^a \equiv 2^d \pmod{101}$. Από την παρατήρηση στο τέλος της πρώτης παραγράφου έχουμε ότι ο a είναι ισότιμος είτε με c είτε με d ως προς το μέτρο 100 και άρα από την (18.3.1) ο b είναι ισότιμος είτε με τον d είτε με τον c. Εφ' όσον όμως $0 \leqslant a, b, c, d \leqslant 99$, οι ισοτιμίες αυτές είναι στην πραγματικότητα ισότητες και άρα το ζητούμενο έχει δειχθεί. ■

Κεφάλαιο 19

19η Παράδοση

Συνεχίζουμε την μελέτη των πρωταρχικών ριζών. Σκοπός μας στο παρόν και στο επόμενο μάθημα είναι να περιγράψουμε το σύνολο των φυσικών οι οποίοι έχουν πρωταρχικές ρίζες. Το αποτέλεσμα που περιγράφει αυτό το σύνολο οφείλεται στον Gauss και εμφανίζεται για πρώτη φορά στο έργο του Disquisitiones Arithmeticae (1801). Σήμερα, συγκεκριμένα, θα δείξουμε ότι κάθε πρώτος έχει πρωταρχικές ρίζες.

19.1 Το Θεώρημα του Lagrange

Ξεκινούμε με το ακόλουθο βοηθητικό αποτέλεσμα το οποίο οφείλεται στον Lagrange.

Θεώρημα 19.1.1 (Lagrange). *Αν ο p είναι ένας πρώτος και το*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad a_n \not\equiv 0 \pmod{p}$$

είναι ένα πολυώνυμο βαθμού $n \geqslant 1$ με ακέραιους συντελεστές, τότε η ισοτιμία

$$f(x) \equiv 0 \pmod{p}$$

έχει το πολύ n ανισότιμες λύσεις ως προς το μέτρο p.

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στον n, τον βαθμό του $f(x)$. Αν $n = 1$, τότε το πολυώνυμο έχει την μορφή $f(x) = a_1 x + a_0$. Εφ' όσον $\gcd(a_1, p) = 1$, η ισοτιμία $a_1 x \equiv -a_0 \pmod{p}$ έχει μοναδική λύση ως προς το μέτρο p σύμφωνα με το Θεώρημα 9.3.1 και άρα το θεώρημα ισχύει για $n = 1$. Η επαγωγική μας υπόθεση τώρα είναι ότι το θεώρημα ισχύει για πολυώνυμα βαθμού $k-1$. Έστω $f(x)$ πολυώνυμο βαθμού k. Τότε είτε η ισοτιμία $f(x) \equiv 0 \pmod{p}$ δεν έχει καμία λύση (και σ' αυτήν την περίπτωση έχουμε τελειώσει) είτε έχει τουλάχιστον μία λύση την οποία καλούμε a. Αν το $f(x)$ διαιρεθεί με το $x - a$, το αποτέλεσμα είναι

$$f(x) = (x - a)q(x) + r,$$

όπου το $q(x)$ είναι ένα πολυώνυμο βαθμού $k-1$ με ακέραιους συντελεστές και ο r είναι ένας ακέραιος. Αντικαθιστώντας $x = a$, παίρνουμε

$$0 \equiv f(a) = (a - a)q(a) + r = r \pmod{p}$$

και άρα $f(x) \equiv (x - a)q(x) \pmod{p}$. Αν τώρα b είναι μία άλλη από τις ανισότιμες λύσεις της $f(x) \equiv 0 \pmod{p}$, τότε

$$0 \equiv f(b) \equiv (b - a)q(b) \pmod{p}.$$

Επειδή όμως $b - a \not\equiv 0 \pmod{p}$, μπορούμε να απλοποιήσουμε το όρο $b - a$ και να πάρουμε $q(b) \equiv 0 \pmod{p}$. Με άλλα λόγια, κάθε λύση της $f(x) \equiv 0 \pmod{p}$ που είναι διαφορετική της a θα πρέπει να ικανοποιεί την ισοτιμία $q(x) \equiv 0 \pmod{p}$. Από την επαγωγική μας υπόθεση όμως, αυτή η ισοτιμία (ως προς $q(x)$) έχει το πολύ $k-1$ ανισότιμες λύσεις. Μπορούμε επομένως να συμπεράνουμε ότι η $f(x) \equiv 0 \pmod{p}$ έχει το πολύ k ανισότιμες λύσεις και μ' αυτό ολοκληρώνεται η επαγωγή και η απόδειξή μας. ■

Το επόμενο αποτέλεσμα προκύπτει άμεσα από το Θεώρημα του Lagrange.

Πόρισμα 19.1.2. *Αν ο p είναι ένας πρώτος αριθμός και $d \mid p-1$, τότε η ισοτιμία*

$$x^d - 1 \equiv 0 \pmod{p}$$

έχει ακριβώς d λύσεις.

Απόδειξη. Εφ' όσον $d \mid p-1$, έχουμε $p - 1 = dk$ για κάποιον φυσικό k. Επομένως

$$x^{p-1} - 1 = (x^d - 1)f(x),$$

όπου το πολυώνυμο $f(x) = x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1$ έχει ακέραιους συντελεστές και βαθμό $d(k-1) = p - 1 - d$. Από το Θεώρημα του Lagrange η ισοτιμία $f(x) \equiv 0 \pmod{p}$ έχει το πολύ $p - 1 - d$ λύσεις. Γνωρίζουμε επίσης από το Θεώρημα του Fermat ότι η ισοτιμία $x^{p-1} - 1 \equiv 0 \pmod{p}$ έχει ακριβώς $p-1$ λύσεις· ήτοι τους φυσικούς $1, 2, \ldots, p-1$. Αν τώρα η $x \equiv a \pmod{p}$ είναι λύση της $x^{p-1} - 1 \equiv 0 \pmod{p}$ αλλά όχι της $f(x) \equiv 0 \pmod{p}$, τότε θα πρέπει να ικανοποιεί την $x^d - 1 \equiv 0 \pmod{p}$. Αυτό διότι η ισοτιμία

$$0 \equiv a^{p-1} - 1 = (a^d - 1)f(a) \pmod{p}$$

με $p \nmid f(a)$ συνεπάγεται ότι $p \mid a^d - 1$. Προκύπτει ότι η $x^d - 1 \equiv 0 \pmod{p}$ θα έχει τουλάχιστον

$$p - 1 - (p - 1 - d) = d$$

λύσεις. Από το Θεώρημα του Lagrange και πάλι η $x^d - 1 \equiv 0 \pmod{p}$ δεν μπορεί να έχει περισσότερες από d λύσεις και άρα έχει ακριβώς d λύσεις. ■

Εκμεταλλευόμαστε άμεσα το πόρισμα που μόλις αποδείξαμε για να παρουσιάσουμε μια διαφορετική απόδειξη του Θεωρήματος του Wilson. Δοθέντος ενός πρώτου p, ορίζουμε το πολυώνυμο $f(x)$ ως

$$\begin{aligned} f(x) &= (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1} - 1) \\ &= a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_1 x + a_0 \end{aligned}$$

και παρατηρούμε ότι ο βαθμός του $f(x)$ είναι ίσος με $p-2$. Από το Θεώρημα του Fermat γνωρίζουμε ότι οι $p-1$ ακέραιοι $1, 2, \ldots, p-1$ αποτελούν διακεκριμένες λύσεις της

$$f(x) \equiv 0 \pmod{p}.$$

Αυτό όμως έρχεται σε αντίθεση με το το Θεώρημα του Lagrange, εκτός αν

$$a_{p-2} \equiv a_{p-3} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 \pmod{p}.$$

Προκύπτει λοιπόν ότι για κάθε επιλογή του ακεραίου x

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

Αντικαθιστώντας $x = 0$ παίρνουμε

$$(-1)(-2)\cdots(-(p-1)) + 1 \equiv 0 \pmod{p}$$

ή ισοδύναμα

$$(-1)^{p-1}(p-1)! + 1 \equiv 0 \pmod{p}.$$

Είτε ο $p-1$ είναι άρτιος είτε $p = 2$, στην οποία περίπτωση $-1 \equiv 1 \pmod{p}$. Τελικά, σε κάθε περίπτωση, έχουμε ότι

$$(p-1)! \equiv -1 \pmod{p}.$$

19.2 Πρωταρχικές ρίζες πρώτων

Έχοντας το Θεώρημα του Lagrange στην διάθεσή μας μπορούμε τώρα να δείξουμε ότι, για κάθε πρώτο p, υπάρχουν ακέραιοι των οποίων η τάξη είναι ίση με d για κάθε διαιρέτη d του $p-1$. Το κάνουμε αυτό πιο συγκεκριμένο στο επόμενο θεώρημα.

Θεώρημα 19.2.1. *Αν ο p είναι πρώτος και $d \mid p-1$, τότε υπάρχουν ακριβώς $\phi(d)$ ανισότιμοι ακέραιοι οι οποίοι έχουν τάξη d ως προς το μέτρο p.*

Απόδειξη. Έστω d διαιρέτης του $p-1$ και ας συμβολίσουμε με $\psi(d)$ τον αριθμό των φυσικών k, όπου $1 \leqslant k \leqslant p-1$, οι οποίοι έχουν τάξη d ως προς το μέτρο p. Επειδή κάθε φυσικός μεταξύ του 1 και του $p-1$ έχει τάξη d για κάποιον διαιρέτη d του $p-1$, προκύπτει ότι

$$p - 1 = \sum_{d \mid p-1} \psi(d).$$

Συγχρόνως, το Θεώρημα 16.2.8 του Gauss μας δίνει ότι

$$p - 1 = \sum_{d \mid p-1} \phi(d).$$

Συνδυάζοντας τις δύο αυτές εξισώσεις, παίρνουμε την

$$\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d). \tag{19.2.1}$$

Σκοπός μας τώρα είναι να δείξουμε ότι $\psi(d) \leqslant \phi(d)$ για κάθε διαιρέτη d του $p-1$. Εφ' όσον το καταφέρουμε αυτό, θα είμαστε σε θέση, λόγω της (19.2.1), να συμπεράνουμε ότι $\psi(d) = \phi(d) \neq 0$ για κάθε $d \mid p-1$. (Διαφορετικά το πρώτο άθροισμα θα ήταν αυστηρά μικρότερο του δεύτερου.)

Δοθέντος ενός διαιρέτη d του $p-1$, υπάρχουν δύο δυνατότητες: είτε $\psi(d) = 0$ είτε $\psi(d) > 0$. Αν $\psi(d) = 0$, τότε σίγουρα $\psi(d) \leqslant \phi(d)$. Ας υποθέσουμε ότι $\psi(d) > 0$, έτσι ώστε να υπάρχει ακέραιος a τάξης d. Τότε οι d ακέραιοι $a, a^2, \ldots, a^d$ είναι ανισότιμοι ως προς το μέτρο p, ενώ καθένας από αυτούς ικανοποιεί την πολυωνυμική ισοτιμία

$$x^d - 1 \equiv 0 \pmod{p}, \tag{19.2.2}$$

αφού $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}$. Από το Πόρισμα 19.1.2 η (19.2.2) δεν έχει άλλες λύσεις. Συμπεραίνουμε ότι κάθε ακέραιος τάξης d ως προς το μέτρο p είναι ισότιμος με έναν εκ των $a, a^2, \ldots, a^d$. Όμως μόνο $\phi(d)$ από αυτές τις δυνάμεις του a έχουν τάξη d, ήτοι οι a^k για τις οποίες ο εκθέτης k είναι τέτοιος ώστε $\gcd(k, d) = 1$. Ως εκ τούτου, στην παρούσα κατάσταση,

$\psi(d) = \phi(d)$ και ο αριθμός των ακεραίων που έχουν τάξη d ως προς το μέτρο p ισούται με $\phi(d)$. Αυτό ακριβώς θέλαμε να αποδείξουμε. ■

Παίρνοντας $d = p - 1$ στο Θεώρημα 19.2.1 προκύπτει το επόμενο πόρισμα.

Πόρισμα 19.2.2. *Αν ο p είναι πρώτος, τότε υπάρχουν ακριβώς $\phi(p-1)$ ανισότιμες πρωταρχικές ρίζες του p.*

Ας θεωρήσουμε για παράδειγμα τον πρώτο $p = 13$. Γι' αυτό το μέτρο, σύμφωνα και με τον Πίνακα 18.1.1, ο 1 έχει τάξη 1, ο 12 έχει τάξη 2, οι 3 και 9 έχουν τάξη 3, οι 5 και 8 έχουν τάξη 4, οι 4 και 10 έχουν τάξη 6 και τέσσερις ακέραιοι, συγκεκριμένα οι $2, 6, 7, 11$, έχουν τάξη 12. Επομένως

$$\begin{aligned}\sum_{d|12} \psi(d) &= \psi(1) + \psi(2) + \psi(3) + \psi(4) + \psi(6) + \psi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12,\end{aligned}$$

όπως περιμέναμε. Προσέξτε επίσης ότι

$$\begin{array}{ll} \psi(1) = 1 = \phi(1) & \psi(4) = 2 = \phi(4) \\ \psi(2) = 1 = \phi(2) & \psi(6) = 2 = \phi(6) \\ \psi(3) = 2 = \phi(3) & \psi(12) = 4 = \phi(12). \end{array}$$

Παρεμπιπτόντως, υπάρχει ένας συντομότερος και κομψότερος τρόπος να αποδείξουμε ότι $\psi(d) = \phi(d)$ για κάθε $d \mid p - 1$. Εφαρμόζουμε τον τύπο αντιστροφής του Möbius στην ισότητα $d = \sum_{c|d} \psi(c)$ και παίρνουμε

$$\psi(d) = \sum_{c|d} \mu(c) \frac{d}{c}.$$

Το δεξί μέλος της ανωτέρω ισότητας είναι ίσο με $\phi(d)$ λόγω του Θεωρήματος 16.2.8. Φυσικά, χρειαζόμαστε το Πόρισμα 19.1.2 για να δικαιολογήσουμε την ισότητα $d = \sum_{c|d} \psi(c)$.

Είμαστε επίσης σε θέση να δώσουμε μία διαφορετική απόδειξη ότι, αν ο p είναι ένας πρώτος της μορφής $4k+1$, τότε η τετραγωνική ισοτιμία $x^2 \equiv -1 \pmod{p}$ έχει λύση. Εφ' όσον $4 \mid p-1$, το Θεώρημα 19.2.1 εξασφαλίζει την ύπαρξη ενός ακεραίου a με τάξη 4 ως προς το μέτρο p. Δηλαδή

$$a^4 \equiv 1 \pmod{p}$$

ή ισοδύναμα

$$(a^2 - 1)(a^2 + 1) \equiv 0 \pmod{p}.$$

Εφ' όσον ο p είναι πρώτος, προκύπτει ότι

$$a^2 - 1 \equiv 0 \pmod{p} \qquad \text{ή} \qquad a^2 + 1 \equiv 0 \pmod{p}.$$

Αν ίσχυε η πρώτη ισοτιμία, τότε ο a θα έπρεπε να έχει τάξη το πολύ ίση με 2, κάτι που είναι άτοπο. Επομένως $a^2 + 1 \equiv 0 \pmod{p}$ και άρα ο a είναι λύση της ισοτιμίας $x^2 \equiv -1 \pmod{p}$.

Το Θεώρημα 19.2.1 έχει ένα προφανές μειονέκτημα. Ενώ εξασφαλίζει την ύπαρξη πρωταρχικών ριζών για κάθε πρώτο p, η απόδειξη είναι μη κατασκευαστική. Δηλαδή, δεν υποδεικνύει κανέναν τρόπο εύρεσης συγκεκριμένης πρωταρχικής ρίζας.

Σε γενικές γραμμές, για να βρούμε μία πρωταρχική ρίζα πρέπει να ελέγξουμε εξαντλητικά μία-μία τις επιλογές ή να ανατρέξουμε σε πίνακες που έχουν κατασκευαστεί γι' αυτόν τον σκοπό. Στον Πίνακα 19.2.1 παρουσιάζουμε την ελάχιστη θετική πρωταρχική ρίζα κάθε πρώτου που είναι μικρότερος του 200. Αν συμβολίσουμε με $\chi(p)$ την ελάχιστη θετική πρωταρχική ρίζα του πρώτου p, τότε ο Πίνακας 19.2.1 δείχνει ότι $\chi(p) \leqslant 19$ για κάθε $p < 200$. Στην πραγματικότητα, ισχύει ότι $\lim_{p\to\infty} \chi(p) = \infty$.

Πρώτος	Ελάχιστη θετική πρωταρχική ρίζα	Πρώτος	Ελάχιστη θετική πρωταρχική ρίζα
2	1	89	3
3	2	97	5
5	2	101	2
7	3	103	5
11	2	107	2
13	2	109	6
17	3	113	3
19	2	127	3
23	5	131	2
29	2	137	3
31	3	139	2
37	2	149	2
41	6	151	6
43	3	157	5
47	5	163	2
53	2	167	5
59	2	173	2
61	2	179	2
67	2	181	2
71	7	191	19
73	5	193	5
79	3	197	2
83	2	199	3

Πίνακας 19.2.1: Οι ελάχιστες θετικές πρωταρχικές ρίζες των πρώτων < 200

Ο πίνακας υποδεικνύει επίσης, αν και δεν γνωρίζουμε την απάντηση μέχρι στιγμής, ότι υπάρχουν άπειροι πρώτοι p για τους οποίους $\chi(p) = 2$. Στις περισσότερες περιπτώσεις πάντως ο $\chi(p)$ είναι αρκετά μικρός. Μεταξύ των 78498 περιττών πρώτων μέχρι το 10^6, ισχύει ότι $\chi(p) \leqslant 6$ περίπου στο 80% των περιπτώσεων. Επίσης, ισχύει ότι $\chi(p) = 2$ για 29841 πρώτους, δηλαδή για το 37% (περίπου) των περιπτώσεων, ενώ ισχύει ότι $\chi(p) = 3$ για 17814 πρώτους, δηλαδή για το 22% (περίπου) των περιπτώσεων.

Στο Disquisitiones Arithmeticae, ο Gauss διατύπωσε την εικασία ότι ο 10 είναι πρωταρχική ρίζα άπειρων πρώτων. Το 1927 ο Emil Artin διατύπωσε την εξής γενικότερη εικασία: αν ο a είναι διάφορος των 1, -1 και δεν είναι τέλειο τετράγωνο, τότε υπάρχουν άπειροι πρώτοι για τους οποίους ο a είναι πρωταρχική ρίζα. Δεν υπάρχουν ιδιαίτερες αμφιβολίες ότι η Εικασία του Artin (όπως έχει μείνει γνωστή) είναι αληθής, αλλά μέχρι τώρα δεν έχει αποδειχτεί.

Δικαιολογούμε τους περιορισμούς στην Εικασία του Artin. Έστω ότι ο a είναι τέλειο τετράγωνο, ας πούμε $a = x^2$, και έστω p περιττός πρώτος τέτοιος ώστε $\gcd(a, p) = 1$. Αν $p \nmid x$, τότε $x^{p-1} \equiv 1 \pmod{p}$ από το Θεώρημα του Fermat. Επομένως

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv 1 \pmod{p},$$

οπότε ο a δεν μπορεί να είναι πρωταρχική ρίζα του p. (Αν $p \mid x$, τότε $p \mid a$ και τότε σίγουρα $a^{p-1} \not\equiv 1 \pmod{p}$.) Επιπλέον, επειδή $(-1)^2 = 1$, ο -1 δεν είναι πρωταρχική ρίζα του p οποτεδήποτε $p - 1 > 2$.

Παράδειγμα 19.2.3. Θα χρησιμοποιήσουμε τα διάφορα αποτελέσματα που έχουμε αποδείξει για να βρούμε τους $\phi(6) = 2$ ακεραίους που έχουν τάξη 6 ως προς το μέτρο 31.

Ξεκινούμε επισημαίνοντας ότι υπάρχουν

$$\phi(\phi(31)) = \phi(30) = 8$$

πρωταρχικές ρίζες του 31. Μπορούμε να συμβουλευτούμε τον Πίνακα 19.2.1 και να δούμε ότι ο 3 είναι πρωταρχική ρίζα του 31. Εφ' όσον ισχύει αυτό, κάθε ακέραιος που είναι σχετικά πρώτος με τον 31 είναι ισότιμος ως προς το μέτρο 31 με έναν ακέραιο της μορφής 3^k, όπου $1 \leqslant k \leqslant 30$. Σύμφωνα με το Θεώρημα 18.1.5 η τάξη του 3^k ισούται με $30/\gcd(k, 30)$ και αυτή η ποσότητα θα είναι ίση με 6, αν και μόνο αν $\gcd(k, 30) = 5$. Οι τιμές του k για τις οποίες ισχύει αυτή η ισότητα είναι οι $k = 5$ και $k = 25$. Επομένως αρκεί να προσδιορίσουμε τους 3^5 και 3^{25} ως προς το μέτρο 31. Ένας απλός υπολογισμός μας δίνει

$$\begin{aligned} 3^5 &\equiv (27)9 \equiv (-4)9 \equiv -36 \equiv 26 \pmod{31} \\ 3^{25} &\equiv \left(3^5\right)^5 \equiv (26)^5 \equiv (-5)^5 \equiv (-125)(25) \equiv -1(25) \equiv 6 \pmod{31} \end{aligned}$$

και άρα οι 6 και 26 είναι οι μόνοι ανισότιμοι ακέραιοι που έχουν τάξη 6 ως προς το μέτρο 31.

19.3 Ασκήσεις

Άσκηση 19.3.1. Βρείτε τις πρωταρχικές ρίζες των πρώτων 11, 19 και 23 και εκφράστε κάθε μία ως μία δύναμη κάποιας πρωταρχικής ρίζας.

Λύση. Οι πρωταρχικές ρίζες του 11 είναι οι $\{2, 6, 7, 8\}$ και έχουμε ότι $2 \equiv 2^1$, $6 \equiv 2^9$, $7 \equiv 2^7$ και $8 \equiv 2^3$. Παρατηρήστε ότι οι εκθέτες $1, 9, 7, 3$ είναι ακριβώς εκείνοι οι φυσικοί < 10 οι οποίοι είναι σχετικά πρώτοι με τον 10.

Οι πρωταρχικές ρίζες του 19 είναι οι $\{2, 3, 10, 13, 14, 15\}$ και έχουμε ότι $2 \equiv 2^1$, $3 \equiv 2^{13}$, $10 \equiv 2^{17}$, $13 \equiv 2^5$, $14 \equiv 2^7$ και $15 \equiv 2^{11}$.

Οι πρωταρχικές ρίζες του 23 είναι οι $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$ και έχουμε ότι $5 \equiv 5^1$, $7 \equiv 5^{19}$, $10 \equiv 5^3$, $11 \equiv 5^9$, $14 \equiv 5^{21}$, $15 \equiv 5^{17}$, $17 \equiv 5^7$, $19 \equiv 5^{15}$, $20 \equiv 5^5$ και $21 \equiv 5^{13}$. ■

Άσκηση 19.3.2. Επαληθεύστε ότι κάθε μία από τις ισοτιμίες $x^2 \equiv 1 \pmod{15}$, $x^2 \equiv -1 \pmod{65}$ και $x^2 \equiv -2 \pmod{33}$ έχει 4 ανισότιμες λύσεις. Επομένως, το Θεώρημα του Lagrange *δεν* ισχύει αναγκαστικά, αν το μέτρο είναι σύνθετος αριθμός.

Λύση. Ένας τρόπος να λύσουμε αυτήν την άσκηση θα ήταν να δοκιμάσουμε όλες τις δυνατές περιπτώσεις. Κάτι τέτοιο όμως θα ήταν ασύμφορο, ειδικά στην περίπτωση του 65.

Εναλλακτικά, μπορούμε να επιχειρηματολογήσουμε ως εξής: στην περίπτωση της ισοτιμίας $x^2 \equiv 1 \pmod{15}$, ο x την ικανοποιεί, αν και μόνο αν ο x ικανοποιεί ταυτόχρονα τις

$$x^2 \equiv 1 \pmod 5 \qquad \text{και} \qquad x^2 \equiv 1 \pmod 3 .$$

Οι λύσεις της $x^2 \equiv 1 \pmod 5$ είναι οι

$$x \equiv 1 \pmod 5 \qquad \text{και} \qquad x \equiv 4 \pmod 5 ,$$

ενώ οι λύσεις της $x^2 \equiv 1 \pmod 3$ είναι οι

$$x \equiv 1 \pmod 3 \qquad \text{και} \qquad x \equiv 2 \pmod 3 .$$

Χρησιμοποιώντας το Κινέζικο Θεώρημα Υπολοίπων, μπορούμε να δούμε ότι η λύση του συστήματος $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 3$ είναι η $x \equiv 1 \pmod{15}$. Αποτυπώνουμε τις λύσεις των τεσσάρων συστημάτων που προκύπτουν στις επόμενες δύο εξισώσεις:

$$\left.\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 3 \end{aligned}\right\} \longmapsto x \equiv 1 \pmod{15} \qquad \left.\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 3 \end{aligned}\right\} \longmapsto x \equiv 11 \pmod{15}$$

και

$$\left.\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 1 \pmod 3 \end{aligned}\right\} \longmapsto x \equiv 4 \pmod{15} \qquad \left.\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 2 \pmod 3 \end{aligned}\right\} \longmapsto x \equiv 14 \pmod{15}$$

Επομένως οι λύσεις της $x^2 \equiv 1 \pmod{15}$ είναι οι $x \equiv 1, 11, 4, 14 \pmod{15}$.

Εργαζόμενοι με αυτήν την μέθοδο, βρίσκουμε ότι οι λύσεις της ισοτιμίας $x^2 \equiv -1 \pmod{65}$ είναι οι $x \equiv 8, 18, 47, 57 \pmod{65}$, ενώ οι λύσεις της ισοτιμίας $x^2 \equiv -2 \pmod{33}$ είναι οι $x \equiv 8, 14, 19, 25 \pmod{33}$. ■

Άσκηση 19.3.3. Δίνεται ότι ο 3 είναι πρωταρχική ρίζα του 43. Βρείτε:

(i) Όλους τους φυσικούς < 43 που έχουν τάξη 6 ως προς το μέτρο 43.

(ii) Όλους τους φυσικούς < 43 που έχουν τάξη 14 ως προς το μέτρο 43.

Λύση. (i) Εργαζόμαστε όπως στο Παράδειγμα 19.2.3 για να βρούμε τους $\phi(6) = 2$ ζητούμενους φυσικούς. Εφ' όσον ο 3 είναι πρωταρχική ρίζα του 43, κάθε υπόλοιπο γράφεται ως μία δύναμη του 3. Για να βρούμε τους ζητούμενους φυσικούς επομένως, αρκεί να προσδιορίσουμε τους εκθέτες j που είναι τέτοιοι ώστε η τάξη του 3^j ως προς το μέτρο 43 να ισούται με 6.

Σύμφωνα με το Θεώρημα 18.1.5 η τάξη του 3^j ισούται με $42/\gcd(j, 42)$. Άρα ψάχνουμε τους εκθέτες που είναι τέτοιοι ώστε $1 \leqslant j \leqslant 42$ και $\gcd(j, 42) = 7$. Δηλαδή θα πρέπει $j = 7k$ με $1 \leqslant k \leqslant 6$ και $\gcd(k, 6) = 1$. Επομένως $k = 1$ ή $k = 5$ και άρα $j = 7$ και ή $j = 35$.

Μας μένει τώρα να υπολογίσουμε τους $3^7 \pmod{43}$ και $3^{35} \pmod{43}$. Έχουμε $3^3 \equiv 27 \pmod{43}$ και $3^4 \equiv 38 \pmod{43}$. Άρα $3^7 \equiv 27 \cdot 38 \equiv 37 \pmod{43}$. Επίσης,

$$3^{35} \equiv (3^7)^5 \equiv (-6)^5 \equiv 36 \cdot 36 \cdot (-6) \equiv (-7)(-7)(-6) \equiv 49 \cdot 37 \equiv 6 \cdot 37 \equiv 7 \pmod{43} .$$

Συμπεραίνουμε ότι οι ζητούμενοι φυσικοί είναι οι 37 και 7.

(ii) Εργαζόμαστε με παρόμοιο τρόπο. Εδώ αρκεί να προσδιορίσουμε τους εκθέτες j που είναι τέτοιοι ώστε η τάξη του 3^j ως προς το μέτρο 43 να ισούται με 14.

Σύμφωνα με το Θεώρημα 18.1.5 και πάλι η τάξη του 3^j ισούται με $42/\gcd(j,42)$. Άρα ψάχνουμε τους εκθέτες που είναι τέτοιοι ώστε $1 \leqslant j \leqslant 42$ και $\gcd(j,42) = 3$. Δηλαδή θα πρέπει $j = 3k$ με $1 \leqslant k \leqslant 14$ και $\gcd(k,14) = 1$.

Επομένως $k = 1, 3, 5, 9, 11, 13$ και άρα $j = 3, 9, 15, 27, 33, 39$. Παραλείπω τις πράξεις που απομένουν, και δίνω κατ' ευθείαν το αποτέλεσμα: οι ζητούμενοι φυσικοί είναι οι 27, 32, 22, 2, 39 και 8. ■

Άσκηση 19.3.4. Έστω p πρώτος και ας συμβολίσουμε με P το γινόμενο των $\phi(p-1)$ πρωταρχικών ριζών του p. Να δείξετε ότι $P \equiv (-1)^{\phi(p-1)} \pmod{p}$.

Υπόδειξη: Αν ο r είναι πρωταρχική ρίζα του p, τότε ο r^k είναι πρωταρχική ρίζα του p, αν και μόνο αν $\gcd(k, p-1) = 1$. Τώρα χρησιμοποιήστε την Εφαρμογή 16.2.10.

Απόδειξη. Έστω ότι ο r είναι πρωταρχική ρίζα του p. Τότε κάθε άλλη πρωταρχική ρίζα του p είναι μία δύναμη r^k του r. Συγκεκριμένα, η τάξη του r^k είναι ίση με $p-1$, αν και μόνο αν $\gcd(k, p-1) = 1$ από το Πόρισμα 18.1.6. Επομένως

$$P = \prod_{\substack{j \leqslant n \\ (j,p-1)=1}} r^j = r^s,$$

όπου

$$s = \sum_{\substack{j \leqslant n \\ (j,p-1)=1}} j = \frac{1}{2}(p-1)\phi(p-1).$$

Η δεύτερη ισότητα στο ανωτέρω άθροισμα προκύπτει από την Εφαρμογή 16.2.10. Θέτοντας $g = r^{(p-1)/2}$ και συνδυάζοντας τις ανωτέρω ισότητες, βλέπουμε ότι

$$P = r^{\frac{1}{2}(p-1)\phi(p-1)} = g^{\phi(p-1)}.$$

Σε ό,τι αφορά στον g τώρα, παρατηρούμε ότι $g^2 = r^{p-1} \equiv 1 \pmod{p}$. Έχουμε επισημάνει σε διάφορα σημεία ότι η ισοτιμία $g^2 \equiv 1 \pmod{p}$ (όπου ο p είναι πρώτος) ισχύει, μόνο αν $g \equiv 1 \pmod{p}$ ή $g \equiv -1 \pmod{p}$. Στην συγκεκριμένη περίπτωση, ο g έχει τάξη 2 ως προς το μέτρο p (αφού ο r είναι πρωταρχική ρίζα και άρα έχει τάξη $p-1$ ως προς το μέτρο p), οπότε δεν μπορεί να ισχύει ότι $g \equiv 1 \pmod{p}$. Αναγκαστικά λοιπόν έχουμε ότι $g \equiv -1 \pmod{p}$ και άρα

$$P = g^{\phi(p-1)} \equiv (-1)^{\phi(p-1)} \pmod{p},$$

όπως θέλαμε να δείξουμε. ■

Σημείωση: Παρατηρήστε ότι για $p > 3$ ο $\phi(p-1)$ είναι άρτιος (αφού ο $\phi(n)$ είναι άρτιος για κάθε $n > 2$ φυσικό από το Θεώρημα 16.2.7) και άρα $P \equiv 1 \pmod{p}$, ενώ για $p = 2$ ή $p = 3$ έχουμε $P \equiv -1 \pmod{p}$.

Άσκηση 19.3.5. Χρησιμοποιήστε το γεγονός ότι κάθε πρώτος p έχει πρωταρχική ρίζα, για να δώσετε μια διαφορετική απόδειξη του Θεωρήματος του Wilson.

Υπόδειξη: Αν ο r είναι πρωταρχική ρίζα του p, τότε από το Θεώρημα 18.2.3 έχουμε ότι $(p-1)! \equiv r^{1+2+\ldots+(p-1)} \pmod{p}$.

Απόδειξη. Ακολουθώντας την υπόδειξη, αν ο r είναι πρωταρχική ρίζα του p, τότε από το Θεώρημα 18.2.3 έχουμε ότι

$$(p-1)! \equiv r^{1+2+\ldots+(p-1)} \equiv r^{\frac{p(p-1)}{2}} \pmod{p}.$$

Συμβολίζοντας με $g = r^{(p-1)/2}$, επιχειρηματολογούμε όπως και στην απόδειξη της Άσκησης 19.3.4 για να γράψουμε $g \equiv -1 \pmod{p}$. Έχουμε δηλαδή ότι

$$(p-1)! \equiv g^p \equiv (-1)^p \equiv -1 \pmod{p}$$

και αυτό ισχύει είτε $p = 2$ είτε $p > 2$. Το ζητούμενο έχει δειχθεί. ■

Άσκηση 19.3.6. Να δείξετε ότι, αν ο p είναι περιττός πρώτος και οι a, b είναι πρωταρχικές ρίζες $\bmod p$, τότε ο ab δεν είναι πρωταρχική ρίζα.

Απόδειξη. Εφ' όσον οι a, b είναι πρωταρχικές ρίζες ως προς το μέτρο p, έχουμε ότι

$$a^{p-1} \equiv 1 \pmod{p} \qquad \text{και} \qquad b^{p-1} \equiv 1 \pmod{p}.$$

Επομένως

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \qquad \text{και} \qquad b^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

χρησιμοποιώντας το γνωστό επιχείρημα με την παρατήρηση ότι για $x = a^{\frac{p-1}{2}}$ ή $x = b^{\frac{p-1}{2}}$ έχουμε ότι $x \not\equiv 1 \pmod{p}$, αφού η $x \equiv 1 \pmod{p}$ έρχεται σε αντίφαση με το γεγονός ότι η τάξη του a και η τάξη του b είναι ίσες με $\phi(p) = p-1$. Άρα

$$(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (-1)(-1) \equiv 1 \pmod{p},$$

οπότε ο ab δεν είναι πρωταρχική ρίζα ως προς το μέτρο p. ■

Άσκηση 19.3.7. Αν ο p είναι περιττός πρώτος, δείξτε ότι

$$1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{αν } p-1 \nmid n, \\ -1 \pmod{p} & \text{αν } p-1 \mid n. \end{cases}$$

Υπόδειξη: Αν ο r είναι πρωταρχική ρίζα του p, τότε το άθροισμα είναι ισότιμο ως προς το μέτρο p με το

$$1 + r^n + r^{2n} + \cdots + r^{(p-2)n} = \frac{r^{(p-1)n} - 1}{r^n - 1}.$$

Απόδειξη. Εξετάζουμε πρώτα την περίπτωση $p-1 \mid n$. Εφ' όσον ισχύει αυτό, υπάρχει φυσικός t τέτοιος ώστε $n = (p-1)t$. Επίσης, από το Θεώρημα του Fermat ισχύει ότι για κάθε $j \in \{1, 2, \ldots, p-1\}$

$$j^n \equiv j^{(p-1)t} \equiv (j^{p-1})^t \equiv 1^t \equiv 1 \pmod{p}.$$

Άρα

$$1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv \underbrace{1 + 1 + \ldots + 1}_{p-1} \equiv p - 1 \equiv -1 \pmod{p}.$$

Μένει επομένως να δείξουμε ότι, αν $p-1 \nmid n$, τότε $1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv 0 \pmod{p}$. Συμβολίζουμε με $S = 1^n + 2^n + 3^n + \cdots + (p-1)^n$ και θεωρούμε μία πρωταρχική ρίζα r του p. Σύμφωνα με την υπόδειξη,

$$S = 1 + r^n + r^{2n} + \cdots + r^{(p-2)n} = \frac{r^{(p-1)n} - 1}{r^n - 1}.$$

Επομένως

$$S(r^n - 1) \equiv r^{(p-1)n} - 1 \equiv 0 \pmod{p},$$

όπου η δεύτερη ισοδυναμία ισχύει λόγω του Θεωρήματος του Fermat. Εφ' όσον $r^n - 1 \not\equiv 0 \pmod{p}$ (κάτι που ισχύει επειδή $p-1 \nmid n$), ο όρος $r^n - 1$ μπορεί να απλοποιηθεί, οπότε και παίρνουμε την ζητούμενη ισοδυναμία $S \equiv 0 \pmod{p}$. ■

Κεφάλαιο 20

20η Παράδοση

Σκοπός μας στο σημερινό μάθημα είναι να ολοκληρώσουμε την μελέτη των πρωταρχικών ριζών την οποία ξεκινήσαμε στα δύο προηγούμενα μαθήματα. Συγκεκριμένα, θα αποδείξουμε ένα σημαντικό θεώρημα που οφείλεται στον Gauss και εμφανίζεται για πρώτη φορά στο γνωστό του έργο Disquisitiones Arithmeticae. Σύμφωνα με το θεώρημα αυτό, ο φυσικός $n > 1$ έχει πρωταρχικές ρίζες, αν και μόνο αν $n = 2, 4, p^k$ ή $2p^k$, όπου p περιττός πρώτος.

20.1 Πρωταρχικές ρίζες σύνθετων φυσικών

Στο προηγούμενο μάθημα αποδείξαμε ότι κάθε πρώτος αριθμός έχει πρωταρχικές ρίζες. Είδαμε όμως ότι ο 2 είναι πρωταρχική ρίζα του 9 για παράδειγμα, κάτι που σημαίνει ότι και σύνθετοι φυσικοί μπορούν να έχουν πρωταρχικές ρίζες. Ο στόχος μας είναι να προσδιορίσουμε όλους εκείνους τους σύνθετους φυσικούς οι οποίοι έχουν πρωταρχικές ρίζες και θα ξεκινήσουμε το πρόγραμμά μας με δύο αρνητικά αποτελέσματα.

Θεώρημα 20.1.1. *Για $k \geqslant 3$ φυσικό, ο 2^k δεν έχει πρωταρχικές ρίζες.*

Απόδειξη. Ισχυριζόμαστε αρχικά ότι αν ο a είναι περιττός, τότε για $k \geqslant 3$ ισχύει ότι

$$a^{2^{k-2}} \equiv 1 \left(\mathrm{mod}\ 2^k\right) \tag{20.1.1}$$

και δικαιολογούμε αυτόν τον ισχυρισμό κάνοντας επίκληση στο περιεχόμενο της Άσκησης 8.2.6.

Παρατηρούμε τώρα ότι οι φυσικοί που είναι σχετικά πρώτοι με τον 2^k είναι ακριβώς οι περιττοί φυσικοί και $\phi(2^k) = 2^{k-1}$. Με βάση την ισότητα (20.1.1), είμαστε σε θέση να γράψουμε

$$a^{\phi(2^k)/2} \equiv 1 \left(\mathrm{mod}\ 2^k\right).$$

Επομένως, ο 2^k όντως δεν έχει πρωταρχική ρίζα. ■

Στο ίδιο πνεύμα είναι και το επόμενο αποτέλεσμα.

Θεώρημα 20.1.2. *Αν $\gcd(m, n) = 1$, όπου $m > 2$ και $n > 2$, τότε ο mn δεν έχει πρωταρχικές ρίζες.*

Απόδειξη. Έστω a ακέραιος τέτοιος ώστε $\gcd(a, mn) = 1$. Παρατηρούμε ότι $\gcd(a, m) = \gcd(a, n) = 1$ και θέτουμε $h = \operatorname{lcm}(\phi(m), \phi(n))$, $d = \gcd(\phi(m), \phi(n))$. Από το Θεώρημα 16.2.7 έχουμε ότι και ο $\phi(m)$ και ο $\phi(n)$ είναι άρτιοι και άρα σίγουρα ισχύει ότι $d \geqslant 2$. Επομένως

$$h = \frac{\phi(m)\phi(n)}{d} \leqslant \frac{\phi(mn)}{2},$$

όπου η πρώτη ισότητα ισχύει λόγω του Θεωρήματος 3.2.2.

Από το Θεώρημα του Euler τώρα, έχουμε ότι $a^{\phi(m)} \equiv 1 \pmod{m}$. Υψώνοντας τα δύο μέλη αυτής της ισοδυναμίας στην δύναμη $\phi(n)/d$, παίρνουμε

$$a^h = (a^{\phi(m)})^{\phi(n)/d} \equiv 1^{\phi(n)/d} \equiv 1 \pmod{m}.$$

Με το ίδιο ακριβώς επιχείρημα έχουμε ακόμα ότι $a^h \equiv 1 \pmod{n}$. Λαμβάνοντας υπ' όψιν την υπόθεση $\gcd(m, n) = 1$, συμπεραίνουμε ότι αναγκαστικά ισχύει η

$$a^h \equiv 1 \pmod{mn}.$$

Προκύπτει λοιπόν ότι η τάξη κάθε ακεραίου σχετικά πρώτου με τον mn είναι το πολύ ίση με $\phi(mn)/2$ και άρα αυστηρά μικρότερη του $\phi(mn) = \phi(m)\phi(n)$. Οδηγούμαστε επομένως στο συμπέρασμα ότι ο mn δεν έχει πρωταρχικές ρίζες, που ήταν και το ζητούμενο. ■

Μερικές ειδικές περιπτώσεις του Θεωρήματος 20.1.2 χρήζουν ξεχωριστής μνείας και τις αποτυπώνουμε στο επόμενο αποτέλεσμα.

Πόρισμα 20.1.3. *Ο φυσικός n **δεν** έχει πρωταρχικές ρίζες, αν*

(i) *είτε ο n διαιρείται από δύο διακεκριμένους περιττούς πρώτους*

(ii) *είτε ο n είναι της μορφής $n = 2^m p^k$, όπου p περιττός πρώτος και $m \geqslant 2$.*

Με βάση το Πόρισμα 20.1.3, απομένει να εξετάσουμε αν οι φυσικοί 2, 4, p^k και $2p^k$, όπου ο p είναι περιττός πρώτος, έχουν πρωταρχικές ρίζες ή όχι. Ο στόχος μας από εδώ και στο εξής είναι να δείξουμε ότι σε κάθε μία από τις παραπάνω περιπτώσεις υπάρχουν όντως πρωταρχικές ρίζες. Η δυσκολότερη περίπτωση, η οποία θέλει κάμποση δουλειά, είναι η δύναμη ενός περιττού πρώτου. Επειδή το επιχείρημα είναι μακροσκελές, το σπάμε σε επί μέρους κομμάτια.

Θεώρημα 20.1.4. *Αν ο p είναι ένας περιττός πρώτος και ο r είναι μία πρωταρχική ρίζα του p, τότε τουλάχιστον ένας εκ των r, $r + p$ είναι πρωταρχική ρίζα του p^2.*

Απόδειξη. Εφ' όσον ο r είναι πρωταρχική ρίζα του p, η τάξη του r ως προς το μέτρο p είναι ίση με $p - 1$. Έστω n η τάξη του r ως προς το μέτρο p^2, έτσι ώστε $r^n \equiv 1 \pmod{p^2}$. Σίγουρα ισχύει ότι $r^n \equiv 1 \pmod{p}$, επομένως $p-1 \mid n$ από το Θεώρημα 18.1.2, ενώ από το ίδιο θεώρημα παίρνουμε ότι $n \mid \phi(p^2) = p(p-1)$. Η σχέση $p - 1 \mid n \mid p(p-1)$ συνεπάγεται ότι $n = p - 1$ ή $n = p(p-1)$. Αν $n = p(p-1)$, ο r είναι πρωταρχική ρίζα ως προς το μέτρο p^2 και έχουμε τελειώσει. Μπορούμε επομένως να υποθέσουμε ότι $n = p - 1$ και άρα

$$r^{p-1} \equiv 1 \pmod{p^2} \tag{20.1.2}$$

Έστω τώρα $s = r + p$. Επειδή $s \equiv r \pmod{p}$, ο s είναι επίσης πρωταρχική ρίζα του p. Άρα η τάξη του s ως προς το μέτρο p^2 είναι ίση με $p - 1$ ή $p(p-1)$. Αυτό που μένει τώρα να κάνουμε είναι να αποκλείσουμε την πρώτη περίπτωση. Εφ' όσον το καταφέρουμε αυτό, θα

έχουμε δείξει ότι ο $s = r + p$ είναι πρωταρχική ρίζα του p^2. Από το Διωνυμικό Θεώρημα έχουμε ότι

$$s^{p-1} = (r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2} r^{p-3}p^2 + \ldots + p^{p-1}$$
$$\equiv r^{p-1} + (p-1)p \cdot r^{p-2} \pmod{p^2}.$$

Άρα, λόγω της (20.1.2), βλέπουμε ότι

$$s^{p-1} \equiv 1 + (p-1)p \cdot r^{p-2} \equiv 1 - pr^{p-2} \pmod{p^2}.$$

Από την τελευταία αυτή ισοτιμία μπορούμε να δείξουμε ότι

$$s^{p-1} \not\equiv 1 \pmod{p^2}.$$

Αν αντίθετα $s^{p-1} \equiv 1 \pmod{p^2}$, τότε $pr^{p-2} \equiv 0 \pmod{p^2}$, δηλαδή $r^{p-2} \equiv 0 \pmod{p}$. Αυτό όμως είναι αδύνατο, αφού $p \nmid r$ (υπενθυμίζουμε ότι ο r είναι πρωταρχική ρίζα του p). Συμπεραίνουμε ότι η τάξη του $s = r + p$ ως προς το μέτρο p^2 είναι ίση με $p(p-1) = \phi(p^2)$ και άρα ο s είναι πρωταρχική ρίζα του p^2, όπως θέλαμε να δείξουμε. ■

Παράδειγμα 20.1.5. Ο $r = 3$ είναι πρωταρχική ρίζα του $p = 7$. Σύμφωνα με τις εξηγήσεις που δώσαμε στην ανωτέρω απόδειξη, η τάξη του 3 ως προς το μέτρο $49 = 7^2$ είναι είτε 6 είτε $6 \cdot 7 = 42$. Όμως

$$r^{p-1} = 3^6 \not\equiv 1 \pmod{49}.$$

Προκύπτει ότι η τάξη του 3 ως προς το μέτρο 49 είναι ίση με 42 και άρα ο 3 είναι πρωταρχική ρίζα του $p^2 = 49$.

Ξεκαθαρίζουμε ότι είναι πιθανό και ο r και ο $r + p$ να είναι πρωταρχικές ρίζες του p^2 για κάποιον πρώτο p και κάποια πρωταρχική ρίζα r του p. Για παράδειγμα, οι 2 και $5 = 2 + 3$ είναι πρωταρχικές ρίζες του 3^2, ενώ οι 3 και $8 = 3 + 5$ είναι πρωταρχικές ρίζες του 5^2. Επίσης είναι γενικά απίθανο να ισχύει ότι

$$r^{p-1} \equiv 1 \pmod{p^2} \tag{20.1.3}$$

για r πρωταρχική ρίζα του πρώτου p και $r < p$. Επομένως σπάνια ο r *δεν* είναι πρωταρχική ρίζα του p^2. Όταν αυτό συμβαίνει όμως, το Θεώρημα 20.1.4 μας εξασφαλίζει ότι ο $r + p$ είναι πρωταρχική ρίζα του p^2.

Ένα παράδειγμα όπου ισχύει η (20.1.3) είναι για $r = 14$ και $p = 29$. Ο 14 είναι πρωταρχική ρίζα του 29 και ταυτόχρονα ισχύει ότι

$$14^{28} \equiv 1 \pmod{29^2}.$$

Επομένως ο 14 δεν είναι πρωταρχική ρίζα του 29^2, αλλά φυσικά ο $43 = 14 + 29$ είναι.

Το επόμενο βήμα τώρα είναι να δείξουμε ότι δυνάμεις περιττών πρώτων έχουν πρωταρχικές ρίζες.

Θεώρημα 20.1.6. *Αν ο p είναι ένας περιττός πρώτος, τότε ο p^k έχει πρωταρχικές ρίζες για κάθε φυσικό k. Επιπλέον, αν ο r είναι πρωταρχική ρίζα του p^2, τότε ο r είναι πρωταρχική ρίζα του p^k για κάθε επιλογή του φυσικού k.*

Απόδειξη. Γνωρίζουμε από το Θεώρημα 20.1.4 ότι ο p έχει τουλάχιστον μία πρωταρχική ρίζα r η οποία είναι πρωταρχική ρίζα και του p^2. Επομένως

$$r^{p-1} \not\equiv 1 \pmod{p^2}. \tag{20.1.4}$$

Θα χρησιμοποιήσουμε επαγωγή για να δείξουμε ότι για αυτήν την πρωταρχική ρίζα r ισχύει η ανισοτιμία

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \tag{20.1.5}$$

για κάθε φυσικό $k \geqslant 2$. Εφ' όσον το έχουμε καταφέρει αυτό, θα είμαστε σε θέση να δείξουμε ότι ο r είναι πρωταρχική ρίζα και του p^k με το εξής επιχείρημα: έστω n η τάξη του r ως προς το μέτρο p^k. Γνωρίζουμε από το Θεώρημα 18.1.2 ότι

$$n \mid \phi(p^k) = p^{k-1}(p-1).$$

Ισχύει όμως ότι $r^n \equiv 1 \pmod{p^k}$, άρα και

$$r^n \equiv 1 \pmod{p}$$

Επειδή ο r είναι πρωταρχική ρίζα του p, η τάξη του ως προς το μέτρο p είναι ίση με $\phi(p) = p-1$. Συνεπώς $p-1 \mid n$ από το Θεώρημα 18.1.2 και άρα

$$p-1 \mid n \mid p^{k-1}(p-1).$$

Επομένως ισχύει ότι $n = p^t(p-1)$ για κάποιον ακέραιο t τέτοιον ώστε $0 \leqslant t \leqslant k-1$. Αν $t \leqslant k-2$, τότε

$$r^{p^{k-2}(p-1)} = \left(r^{p^t(p-1)}\right)^{p^{k-2-t}} \equiv 1 \pmod{p^k}$$

που έρχεται σε αντίθεση με την (20.1.5). Επομένως η τάξη του r ως προς το μέτρο p^k είναι ίση με $p^{k-1}(p-1) = \phi(p^k)$ και άρα όντως ο r είναι πρωταρχική ρίζα και του p^k.

Αυτό που απομένει τώρα είναι να δείξουμε επαγωγικά την (20.1.5). Για $k = 2$ η (20.1.5) ισχύει, γιατί ισχύει η (20.1.4). Υποθέτουμε ότι ο ισχυρισμός αληθεύει για τον φυσικό $k \geqslant 2$. Εφ' όσον $\gcd(r,p) = 1$, έπεται ότι $\gcd(r, p^{k-1}) = 1$. Επομένως το Θεώρημα του Euler μας δίνει ότι

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}},$$

δηλαδή υπάρχει φυσικός d τέτοιος ώστε

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1},$$

όπου $p \nmid d$, αφού εξ υποθέσεως $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. Υψώνουμε και τα δύο μέλη της ανωτέρω ισότητας στην pοστή δύναμη και, χρησιμοποιώντας το Διωνυμικό Θεώρημα και το γεγονός ότι ο p είναι περιττός, παίρνουμε

$$\begin{aligned} r^{p^{k-1}(p-1)} &= \left(1 + dp^{k-1}\right)^p \\ &= 1 + p(dp^{k-1}) + \binom{p}{2}(dp^{k-1})^2 + \ldots + (dp^{k-1})^p \\ &\equiv 1 + dp^k \pmod{p^{k+1}}. \end{aligned}$$

Εφ' όσον $p \nmid d$, μπορούμε να συμπεράνουμε ότι

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}.$$

Έτσι έχουμε ολοκληρώσει την επαγωγή και την απόδειξη. ■

Μας μένει τώρα να εξετάσουμε την περίπτωση $2p^k$.

Πόρισμα 20.1.7. *Ο $2p^k$, όπου p περιττός πρώτος και k φυσικός, έχει πρωταρχικές ρίζες.*

Απόδειξη. Έστω r πρωταρχική ρίζα του p^k. Δεν βλάπτεται η γενικότητα να θεωρήσουμε ότι ο r είναι περιττός. (Αν ο r είναι άρτιος, τότε ο $r+p^k$ είναι περιττός και είναι επίσης πρωταρχική ρίζα του p^k.) Έχουμε τώρα ότι $\gcd(r, 2p^k) = 1$. Η τάξη n του r ως προς το μέτρο $2p^k$ διαιρεί τον

$$\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k).$$

Όμως η σχέση $r^n \equiv 1 \pmod{2p^k}$ συνεπάγεται την $r^n \equiv 1 \pmod{p^k}$ και άρα $\phi(p^k) \mid n$. Από τις δύο αυτές σχέσεις διαιρετότητας προκύπτει η $n = \phi(2p^k)$, που καθιστά τον r πρωταρχική ρίζα του $2p^k$. ■

Ο πρώτος 5 έχει $\phi(4) = 2$ πρωταρχικές, δηλαδή τους 2 και 3. Εφ' όσον

$$2^{5-1} \equiv 16 \not\equiv 1 \pmod{25} \qquad \text{και} \qquad 3^{5-1} \equiv 6 \not\equiv 1 \pmod{25},$$

οι 2, 3 είναι πρωταρχικές ρίζες του 5^2 και άρα κάθε μεγαλύτερης δύναμης του 5. Η απόδειξη του Πορίσματος 20.1.7 εξασφαλίζει ότι ο 3 είναι πρωταρχική ρίζα κάθε φυσικού της μορφής $2 \cdot 5^k$.

Στο επόμενο θεώρημα συγκεντρώνουμε ό,τι έχουμε καταφέρει.

Θεώρημα 20.1.8 (Gauss). *Ένας φυσικός $n > 1$ έχει πρωταρχικές ρίζες, αν και μόνο αν*

$$n = 2, 4, p^k, \ \text{ή} \ 2p^k,$$

όπου p είναι περιττός πρώτος.

Απόδειξη. Με βάση όσα έχουμε αποδείξει ως τώρα, αρκεί να δείξουμε ότι οι 2 και 4 έχουν πρωταρχικές ρίζες. Αυτό όμως είναι προφανές, αφού ο 1 είναι πρωταρχική ρίζα του 2 και ο 3 είναι πρωταρχική ρίζα του 4. ■

20.2 Ασκήσεις

Άσκηση 20.2.1. Βρείτε τις τέσσερις πρωταρχικές ρίζες του 26 και τις οκτώ πρωταρχικές ρίζες του 25.

Λύση. Σύμφωνα με τον Πίνακα 18.1.1, οι πρωταρχικές ρίζες του 13 είναι οι $\{2, 6, 7, 11\}$. Η απόδειξη του Πορίσματος 20.1.7 εξασφαλίζει ότι οι 7 και 11 είναι πρωταρχικές ρίζες του 26, ενώ πρωταρχικές ρίζες είναι επίσης οι $15 = 13 + 2$ και $19 = 13 + 6$.

Για να βρούμε τις πρωταρχικές ρίζες του 25 μπορούμε να δουλέψουμε ως εξής. Σύμφωνα με το Θεώρημα 20.1.4 και εφ' όσον μπορούμε εύκολα να δούμε ότι ο 2 είναι πρωταρχική ρίζα του 5, ένας τουλάχιστον εκ των 2, 7 είναι πρωταρχική ρίζα του 25. Θα δείξουμε ότι ο 2 είναι πρωταρχική ρίζα του 25 και για να το πετύχουμε αυτό αρκεί να παρατηρήσουμε ότι $2^{10} = 1024 \equiv -1 \pmod{25}$ και άρα $2^{20} \equiv 1 \pmod{25}$, ενώ $2^5 = 32 \equiv 7 \pmod{25}$. (Μπορούμε φυσικά και να συμβουλευτούμε τον Πίνακα 19.2.1.) Οι υπόλοιπες πρωταρχικές ρίζες είναι

οι $2^k \pmod{25}$ για k σχετικά πρώτο με τον $\phi(25) = 20$, δηλαδή $k \in \{1, 3, 7, 9, 11, 13, 17, 19\}$. Αυτές οι τιμές δίνουν αντίστοιχα τους $\{2, 8, 3, 12, 23, 17, 22, 13\}$. ■

Άσκηση 20.2.2. Βρείτε τις πρωταρχικές ρίζες των 3^2, 3^3 και 3^4.

Λύση. Δουλεύουμε όπως και στην προηγούμενη άσκηση και βρίσκουμε ότι οι πρωταρχικές ρίζες του 9 είναι οι 2 και 5, ενώ του 3^3 είναι οι $\{2, 5, 11, 14, 20, 23\}$ και του 3^4 οι $\{2, 5, 11, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56, 59, 65, 68, 74, 77\}$. ■

Άσκηση 20.2.3. Δείξτε ότι ο 2 είναι πρωταρχική ρίζα του 3^k για κάθε φυσικό k.

Απόδειξη. Εφ' όσον ο 2 είναι πρωταρχική ρίζα του και του 3 και του 3^2, είναι πρωταρχική ρίζα κάθε δύναμης του 3 σύμφωνα με το Θεώρημα 20.1.6. ■

Άσκηση 20.2.4. Να δείξετε ότι ο m έχει πρωταρχική ρίζα, αν και μόνο αν οι μόνες λύσεις της ισοτιμίας $x^2 \equiv 1 \pmod{m}$ είναι οι $x \equiv \pm 1 \pmod{m}$.

Απόδειξη. Έστω ότι ο r είναι πρωταρχική ρίζα του m και ότι $x^2 \equiv 1 \pmod{m}$. Έστω $x \equiv r^t \pmod{m}$, όπου $0 \leqslant t \leqslant p-1$. Τότε $r^{2t} \equiv 1 \pmod{m}$. Εφ' όσον ο r είναι πρωταρχική ρίζα, έπεται ότι $\phi(m) \mid 2t$, δηλαδή $2t = k\phi(m)$ και $t = k\phi(m)/2$ για κάποιον ακέραιο k. Έχουμε τώρα ότι

$$x \equiv r^t = r^{k\phi(m)/2} = r^{(\phi(m)/2)k} \equiv (-1)^k \equiv \pm 1 \pmod{m},$$

αφού $r^{\phi(m)/2} \equiv -1 \pmod{m}$.

Αντίστροφα, έστω ότι ο m δεν έχει πρωταρχική ρίζα. Τότε ο m δεν είναι της μορφής $2, 4, p^a$ ή $2p^a$, όπου p περιττός πρώτος. Επομένως είτε 2 περιττοί πρώτοι διαιρούν τον m ή $m = 2^b M$, όπου $M > 1$ περιττός και $b > 1$ ή $m = 2^b$, όπου $b > 3$ ή $m = 8$. Αν $m = 8$, τότε $3^2 \equiv 1 \pmod{8}$, αλλά $3 \not\equiv \pm 1 \pmod{8}$. Σε κάθε μία από τις υπόλοιπες περιπτώσεις έχουμε $\phi(m) = 2^c N$, όπου N περιττός και $c \geqslant 3$. Γνωρίζουμε από την (20.1.1) ότι η ισοτιμία $y^2 \equiv 1 \pmod{2^c}$ έχει τουλάχιστον 3 λύσεις, έστω τις y_1, y_2, y_3. Επίσης η $z \equiv 1 \pmod{N}$ είναι σίγουρα λύση της $x^2 \equiv 1 \pmod{N}$. Από το Κινέζικο Θεώρημα Υπολοίπων, το σύστημα $x \equiv y_i \pmod{2^c}$, $z \equiv 1 \pmod{N}$ έχει μοναδική λύση για $i = 1, 2, 3$. Εφ' όσον αυτές οι λύσεις είναι διακεκριμένες ως προς το μέτρο m, έπεται ότι τουλάχιστον μία είναι διάφορη $\pm 1 \pmod{m}$. ■

Άσκηση 20.2.5. Έστω ότι ο φυσικός n έχει πρωταρχική ρίζα. Δείξτε ότι

$$\prod_{\substack{1 \leqslant j \leqslant n \\ (j,n)=1}} j \equiv -1 \pmod{n}, \qquad \text{όπου} \qquad (j, n) = \gcd(j, n).$$

Απόδειξη. Το ζητούμενο ισχύει προφανώς για $n = 2$, οπότε μπορούμε να υποθέσουμε ότι $n > 2$. Έστω r πρωταρχική ρίζα του n. Από την προηγούμενη άσκηση γνωρίζουμε ότι ο $r^{\phi(n)/2}$ ικανοποιεί την $x^2 \equiv 1 \pmod{n}$ και άρα $r^{\phi(n)/2} \equiv -1 \pmod{n}$. Οι φυσικοί που είναι μικρότεροι ή ίσοι του n και σχετικά πρώτοι με τον n είναι μια αναδιάταξη των $r^i \pmod{n}$, όπου $1 \leqslant i \leqslant \phi(n)$. Επομένως

$$\prod_{\substack{1 \leqslant j \leqslant n \\ (j,n)=1}} j \equiv r^{\sum_{i=1}^{\phi(n)} i} \equiv r^{\phi(n)/2(\phi(n)-1)} \equiv (-1)^{\phi(n)-1} \equiv -1 \pmod{n},$$

όπου η τελευταία ισοτιμία ισχύει λόγω του Θεωρήματος 16.2.7. ■