26-3-2020
Διάλεξη 23

(δ') $F_n^2 - F_{n+3}F_{n-3} = 4(-1)^{n+1}$, για κάθε $n \geq 4$

(ε') $F_{2n-1} = F_n^2 + F_{n-1}^2$, για κάθε $n \geq 2$

7. Αν $p \in \mathbb{P}$, $p = 4k+3$ τότε η $a^2 + b^2 \equiv 0 \bmod p$ συνεπάγεται ότι $p \mid a$ και $p \mid b$ (Αποδείξτε το ή δεχτείτε το!). Να αποδείξετε ότι αν $p \in \mathbb{P}$, $p \equiv 3 \bmod 4$, τότε για κάθε $n \geq 1$ ισχύει $p \nmid F_{2n-1}$.

8. Να αποδείξετε ότι το γινόμενο $F_{2n-1}F_{2n+5}$ γράφεται ως άθροισμα δύο τετραγώνων.

9. Θεωρήστε κατάλληλη υπακολουθία της ακολουθίας Fibonacci και αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $4k+1$.

10. Να αποδείξετε την ταυτότητα

$$(F_nF_{n+3})^2 + (2F_{n+1}F_{n+2})^2 = F_{2n+3}^2.$$

Στη συνέχεια να υπολογίσετε 5 πρωταρχικές πυθαγόρειες τριάδες. Τέλος να αποδείξετε ότι ο αριθμός $F_nF_{n+1}F_{n+2}F_{n+3}$ είναι πάντοτε εμβαδόν ορθογωνίου τριγώνου.

6.4 Ακολουθίες Lucas.

Στην παράγραφο αυτή θα γενικεύσουμε τα προηγούμενα αποτελέσματα. Οι τύποι Binet, τόσο των αριθμών Fibonacci όσο και των αριθμών Lucas, συνδέονται άμεσα με τους αριθμούς $\alpha = \frac{1+\sqrt{5}}{2}$ και $\beta = \frac{1-\sqrt{5}}{2}$, οι οποίοι είναι οι ρίζες του δευτεροβάθμιου πολυωνύμου $x^2 - x - 1$. Θεωρούμε λοιπόν δύο ακέραιους αριθμούς a, b διάφορους του μηδενός. Οι ρίζες του πολυωνύμου $x^2 - ax + b = 0$ είναι $\alpha = \frac{a+\sqrt{D}}{2}$ και $\beta = \frac{a-\sqrt{D}}{2}$, όπου $D = a^2 - 4b$ η διακρίνουσα του πολυωνύμου. Προκειμένου να αποφύγουμε την ιδιάζουσα περίπτωση της διπλής ρίζας, υποθέτουμε ότι η διακρίνουσα $D \neq 0$. Επομένως, $\alpha + \beta = a$, $\alpha - \beta = \sqrt{D}$ και $\alpha\beta = b$. Για κάθε $n \geq 0$ ορίζουμε δύο ακολουθίες, $U_n = U_n(\alpha,\beta)_{n\in\mathbb{N}}$ και $V_n = V_n(\alpha,\beta)_{n\in\mathbb{N}}$ ως εξής:

$$U_n = U_n(\alpha,\beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ και } V_n = V_n(\alpha,\beta) = \alpha^n + \beta^n$$

Οι ακολουθίες $U = (U_n(\alpha,\beta))_{n\in\mathbb{N}}$ και $V = (V_n(\alpha,\beta))_{n\in\mathbb{N}}$ θα λέγονται (πρώτη και δεύτερη αντίστοιχα) *ακολουθίες Lucas* ως προς το ζευγάρι (α,β).

Είναι φανερό ότι, $U_0(\alpha,\beta) = 0$, $V_0(\alpha,\beta) = 2$ και $U_1(\alpha,\beta) = 1$, $V_1(\alpha,\beta) = \alpha + \beta$. Επίσης εύκολα διαπιστώνεται ότι για κάθε $n \geq 2$ ισχύουν:

$$U_n(\alpha,\beta) = aU_{n-1} - bU_{n-2},\ V_n(\alpha,\beta) = aV_{n-1} - bV_{n-2}.$$

Οι συνηθισμένοι αριθμοί Fibonacci και Lucas προκύπτουν ως ειδική περίπτωση (πρώτη και δεύτερη αντίστοιχα) της ακολουθίας Lucas ως προς το ζευγάρι $(a,b) = (1,-1)$.
Επεκτείνουμε τους δείκτες και για αρνητικούς ακέραιους έτσι ώστε οι αναδρομικοί τύποι να συνεχίσουν να ισχύουν: $U_{-n} = -\frac{1}{b^n}U_n$ και $V_{-n} = \frac{1}{b^n}V_n$, για κάθε $n \geq 1$.

Ιδιότητες Στη συνέχεια αναφέρουμε, χωρίς αποδείξεις, μερικές ιδιότητες των ακολουθιών

Πρόταση 6.4.2. *Έστω $U = (U_n(\alpha,\beta))_{n\in\mathbb{N}}$ και $V = (V_n(\alpha,\beta))_{n\in\mathbb{N}}$ οι ακολουθίες Lucas ως προς το ζευγάρι (a, b). Αν $p \in \mathbb{P}$, τέτοιος ώστε ο p να μην διαιρεί τον $2\beta D$, τότε ισχύει,*

$$U_{p-\varepsilon_p} \equiv 0 (mod p),$$

όπου $\varepsilon_p := (\frac{D}{p})$.

Η πρόταση αυτή αποτελεί γενίκευση της πρότασης 6.1.11. Θα την αποδείξουμε σε μία ειδική περίπτωση. Συγκεκριμένα θα αποδείξουμε ότι

Πρόταση 6.4.3. *Αν p περιττός πρώτος τέτοιος ώστε $(\frac{D}{p}) = -1$, τότε $p \mid U_{p+1}$.*

Απόδειξη. Η απόδειξη είναι όμοια με την πρόταση 6.1.8. Υπολογίζουμε τον διωνυμικό τύπο για τις δυνάμεις

$$\alpha^n = \left(\frac{a+\sqrt{D}}{2}\right)^n = 2^{-n}\sum_{k=0}^{n}\binom{n}{k}a^{n-k}\sqrt{D}^k$$

και

$$\beta^n = \left(\frac{a-\sqrt{D}}{2}\right)^n = 2^{-n}\sum_{k=0}^{n}\binom{n}{k}a^{n-k}(-1)^k\sqrt{D}^k.$$

Από τους τύπους του Binet προκύπτει ότι,

$$U_n = \frac{\alpha^n-\beta^n}{\alpha-\beta} = 2^{-n+1}\sum_{\substack{0\le k\le n\\ k\equiv 1 \bmod 2}}\binom{n}{k}a^{n-k}D^{\frac{k-1}{2}}.$$

Πολλαπλασιάζουμε και τα δύο μέλη με 2^{n-1} και θέτουμε $n = p + 1$ οπότε παίρνουμε

$$2^p U_{p+1} = \sum_{\substack{0\le k\le n\\ k\equiv 1 \bmod 2}}\binom{p+1}{k}a^{p+1-k}D^{\frac{k-1}{2}}.$$

Είναι γνωστό ότι $\binom{p+1}{k} \equiv 0 \bmod p$ για κάθε k, $2 \le k \le p-1$. Επομένως, αν το λάβουμε υπόψη και εφαρμόσουμε το (μικρό) Θεώρημα Fermat, έχουμε: $2U_{p+1} \equiv a(1 + D^{\frac{p-1}{2}}) \bmod p$. Υπενθυμίζουμε το Θεώρημα του Euler, και την υπόθεση ότι $(\frac{D}{p}) = -1$ από τα οποία προκύπτει ότι $p \mid U_{p+1}$. □

Το πιο γενικό αποτέλεσμα είναι το ακόλουθο: Θεωρούμε τις ακολουθίες Lucas $U = (U_n(\alpha,\beta))_{n\in\mathbb{N}}$ και $V = (V_n(\alpha,\beta))_{n\in\mathbb{N}}$ ως προς το ζευγάρι (a, b) και έστω p ένας περιττός πρώτος αριθμός.

Πρόταση 6.4.4.

1. *Αν ο p δεν διαιρεί το a και διαιρεί το b, τότε ο p δεν διαιρεί το U_n για κάθε $n \ge 1$.*
2. *Αν ο p διαιρεί το a και δεν διαιρεί το b, τότε ο p διαιρεί το U_n ακριβώς τότε όταν ο n είναι άρτιος.*
3. *Αν ο p δεν διαιρεί το ab και διαιρεί το D, τότε ο p διαιρεί το U_n ακριβώς τότε όταν $p \mid n$.*
4. *Αν ο p δεν διαιρεί το abD, τότε ο p διαιρεί το $U_{p-\varepsilon(p)}$.*

Σημείωση. Οι συγγραφείς Crandall, Pomerance [8] και Song Y. Yan [9] θεωρούν ότι για την τελευταία σχέση αρκεί ο περιορισμός ο p να είναι περιττός πρώτος ο οποίος να μη διαιρεί το γινόμενο bD.

Αν τώρα $s > \sqrt{n}+1$ τότε, για κάθε πρώτο διαιρέτη p του n έχουμε

$$p+1 \geq p-\left(\frac{D}{p}\right) \geq s > \sqrt{n}+1,$$

δηλαδή $p > \sqrt{n}$. Αν ο n ήταν σύνθετος τότε θα είχε έναν τουλάχιστον πρώτο παράγοντα $p \leq \sqrt{n}$. Συνεπώς ο n είναι πρώτος. □

Θα κλείσουμε την παράγραφο με ένα πολύ πρακτικό και ντετερμινιστικό test πιστοποίησης πρώτων που αφορά στους αριθμούς Mersenne. Ο Lucas είχε τη βασική ιδέα το 1876 και ο Lehmer απλοποίησε τη μέθοδοτο 1930.

Ορισμός 6.5.7. Η ακολουθία $(S_n)_n \in \mathbb{N}$ η οποία ορίζεται από τον αναδρομικό τύπο $S_1 = 4$ και $S_{n+1} = S_n^2 - 2$ θα λέγεται *ακολουθία των Lucas-Lehmer*.

Πρόταση 6.5.8 (*Test των Lucas-Lehmer για τους πρώτους αριθμούς Mersenne M_n*). *Αν p είναι ένας περιττός πρώτος, τότε ο*

$$M_p := 2^p - 1 \text{ είναι πρώτος ακριβώς τότε όταν ο } M_p \mid S_{p-1}.$$

Απόδειξη. Η ιδέα της απόδειξης είναι να αναγάγουμε το πρόβλημα στη μελέτη μιας ακολουθίας Lucas. Το πλεονέκτημα είναι ότι γνωρίζουμε αρκετές ιδιότητες αυτών των ακολουθιών. Η ακολουθία αυτή θα είναι η $(U_n)_{n\in\mathbb{N}}$, $(V_n)_{n\in\mathbb{N}}$ ως προς το ζευγάρι $(\alpha,\beta) = (2,-2)$. Επομένως, $D = 12$, $a = 1+\sqrt{3}$ και $b = 1-\sqrt{3}$. Ισχύει ότι

$$U_p \equiv \left(\frac{3}{p}\right) \mathrm{mod} p$$

και

$$V_p \equiv 2 \mathrm{mod} p,$$

δείτε [7, σελ. 49]. Υποθέτουμε τώρα ότι για $p \geq 3$ ο αριθμός $M_p = 2^p - 1$ είναι πρώτος. Θα αποδείξουμε ότι ο $S_{p-1} \equiv 0 \mathrm{mod} M_p$. Επειδή ο M_p είναι περιττός, η τελευταία ισοτιμία είναι ισοδύναμη προς την

$$2^{2^{p-2}} S_{p-1} \equiv 0 \mathrm{mod} M_p.$$

Για κάθε $i \geq 1$ ορίζουμε $T_i = 2^{(2^{i-1})} S_i$. Συνεπώς, $T_1 = 2^{2^0} S_1 = 2 \cdot 4 = 8$ και

$$T_{i+1} = 2^{(2^{(i+1)-1})} S_{i+1} = (2^{2^{i-1}})^2 [S_i^2 - 2] = (2^{2^{i-1}} S_i)^2 - 2^{(2^i+1)} = T_i^2 - 2^{(2^i+1)}.$$

Επομένως, αρκεί να αποδείξουμε ότι

$$T_{p-1} = 2^{(2^{p-2})} S_{p-1} \equiv 0 \mathrm{mod} M_p.$$

Αλλά $T_p = T_{p-1}^2 - 4 \cdot 2^{(2^{p-1}+1)}$. Επειδή $M_p = 2^p - 1 \equiv 7 \mathrm{mod} 8)$ έπεται ότι $(\frac{2}{M_p}) = 1$. Από το θεώρημα του Euler προκύπτει ότι

$$2^{2^{p-1}-1} = 2^{\frac{M_p-1}{2}} \equiv \left(\frac{2}{M_p}\right) \equiv 1 \mathrm{mod} M_p.$$

Επομένως αρκεί να αποδείξουμε ότι $T_p \equiv -4 \mathrm{mod} M_p$.

Το οποίο σημαίνει ότι ο $M_{11} = 2^{11} - 1 = 2047$ δεν είναι πρώτος. Πράγματι $2047 = 23 \times 89$. Για $p = 13$ έχουμε

(1, 14)
(2, 194)
(3, 4870)
(4, 3953)
(5, 5970)
(6, 1857)
(7, 36)
(8, 1294)
(9, 3470)
(10, 128)
(11, 0)

Το οποίο σημαίνει ότι ο $M_{13} = 8191$ είναι πρώτος.

Παρατηρήσεις:

- Όλοι οι πρώτοι αριθμοί Mersenne έχουν υπολογιστεί σύμφωνα με το παραπάνω κριτήριο. Πρώτος ο Lucas απέδειξε στα 1876 ότι ο M_{127} είναι πρώτος, ενώ ο M_{67} είναι σύνθετος. Λίγο αργότερα ο Perwuschin, απέδειξε ότι ο M_{61} είναι πρώτος, ενώ ο Lehmer στα 1932 απέδειξε ότι ο M_{257} είναι σύνθετος. Η εικασία του Mersenne ήταν ότι είναι πρώτος.

- Η διαδικασία που εφαρμόζεται είναι η εξής: Επιλέγουμε τυχαία έναν πρώτο αριθμό q και στη συνέχεια ελέγχουμε με βάση το κριτήριο αν ο αντίστοιχος αριθμός Mersenne $M_q = 2^q - 1$ είναι πρώτος. Φυσικά μπορούμε να εργασθούμε πιο συστηματικά και να πάρουμε όλους τους πρώτους τους μικρότερους από κάποια συγκεκριμένη τιμή. Πριν από την εποχή των ηλεκτρονικών υπολογιστών αυτό είχε γίνει μέχρι το ≤ 127. Σήμερα, το αποτέλεσμα αυτό είναι γνωστό, τουλάχιστον για 12830000. Φυσικά αν συμβεί για κάποιο πρώτο q να ισχύει $p := 2q + 1$, τότε, ως γνωστό, ισχύει $p \mid M_q$, δηλαδή ο M_q είναι σύνθετος.

  Το Project "The GIMPS", Great Mersenne Prime Search είναι ένα πρόγραμμα κατανεμημένου υπολογισμού που χρησιμοποιεί την υπολογιστική των υπολογιστών εθελοντών προκειμένου να αναζητήσει πρώτους αριθμούς του Mersenne.

Παραδείγματα:

- Για $q = 7$. υπολογίζουμε την ακολουθία S_i για $i = 1, 2, ..., q - 1 = 6$ και έχουμε: $S_1 = 4$, $S_2 \equiv 14 \mathrm{mod} 127$, $S_3 \equiv 67 \mathrm{mod} 127$, $S_4 \equiv 42 \mathrm{mod} 127$ $S_5 \equiv 111 \mathrm{mod} 127$, $S_6 \equiv 0 \mathrm{mod} 127$. Επομένως ο M_7 είναι πρώτος.

- Για $q = 11$ έχουμε $M_{11} = 2047$. Υπολογίζουμε $S_{10} \equiv 1736 (mod 2047)$ και συμπεραίνουμε ότι ο M_{11} δεν είναι πρώτος.

- Για $q = 13$. Επειδή οι αριθμοί μεγαλώνουν είναι πιο εύκολο να εργαζόμαστε στο δυαδικό σύστημα. Εδώ αποδεικνύεται ότι $S_{12} \equiv 0 \mathrm{mod} M_{13})$ ή ότι ο αριθμός M_{13} είναι πρώτος.

  Σημείωση: Σύμφωνα με το δελτίο τύπου της Γερμανικής Μαθηματικής Εταιρείας της με ημερομηνία 27/9/2008, στα πλαίσια του προγράμματος (GIMPS), έχουν βρεθεί

Βιβλιογραφία

[1] E. Cohn, J. H.: *On square Fibonacci numbers.* J. London Math. Soc., 39:537-540, 1964.

[2] E. Cohn, J. H.: *Eight Diophantine equations.* Proc. London Math. Soc., (3):16:153-166, 1966.

[3] E. Hoggatt: *Fibonacci and Lucas numbers.* Houghton Mifflin mathematics enrichment series. Houghton Mifflin, 1969.

[4] Frommer, H. Scheid and A.: *Zahlentheorie.* Spektrum Akademischer Verlag.

[5] Luo Ming: *On triangular Fibonacci Number.* The Fibonacci Quarterly, 27, 1988.

[6] Moss, N. Vorobev and H.: *Fibonacci Numbers.* Popular lectures in mathematics, Pergamon Press, 1961.

[7] Paulo Ribenboim: *The Little Book of Bigger Primes.* Springer, 2004.

[8] R. Crandall, C.B. Pomerance: *Prime Numbers: A Computational Perspective.* 2005.

[9] S. Y. Yan: *Number Theory for Computing.* U.S. Government Printing Office, 2002.

[10] T. Koshy: *Elementary Number Theory with Applications.* Elsevier Science, 2007.

[11] Worobjow, N.: *Die Fibonacci Zahlen.* D.V.W Berlin, 1954.

6.6 Ασκήσεις

1. Να αποδείξετε τις ιδιότητες από (6.3.1) μέχρι (6.3.9)
2. Ομοίως από (6.3.12) μέχρι (6.3.15)
3. Ομοίως για τις (6.3.16) με (6.3.19)
4. Να αποδείξετε ότι για κάθε $n \geq 2$ ισχύει η ισοτιμία
$$L_{2^n} \equiv 7 \mathrm{mod} 10$$
5. Να αποδειχτεί ότι για κάθε $n \geq 1$
$$2^n L_n \equiv 2 \mathrm{mod} 10$$
6. Να αποδείξετε ότι $L_{n+1} + L_{n-1} = 5F_n$ για $n \geq 2$. Συμπεράνετε ότι $5 \nmid L_n$ για $n \geq 1$.
7. Αν $m = n^{13} - n$ και $n > 1$ να αποδείξετε ότι $30290 \mid F_m$. (Υπόδειξη: Να αποδείξετε πρώτα ότι $a^{13} \equiv a \mathrm{mod} 2730$).
8. Για κάθε $n \geq 1$ να αποδείξετε ότι $18 \mid F_{n+11} + F_{n+7} + 8F_{n+5} + F_{n+3} + 2F_n$.

Ασκήσεις

1. Αν $q \in \mathbb{P}$, $q \equiv 7 \pmod 8$ να αποδείξετε ότι $\left(\frac{2}{q}\right) = 1$

2. Έστω $n > 1$. Αν για κάθε πρώτο διαιρέτη p του $(n-1)$, υπάρχει κάποιος ακέραιος $a := a(p)$ τ.ω
$a^{n-1} \equiv 1 \pmod n$ και $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$
τότε ο n είναι πρώτος αριθμός.
(Υπόδειξη: Αρκεί να αποδείξουμε ότι $\varphi(n) = n-1$)

3. Έστω $p \in \mathbb{P}$, $p \equiv 3 \pmod 4$ να αποδείξετε ότι ο $[(2p+1) \mid M_p] \Leftrightarrow [(2p+1) \in \mathbb{P}]$
Αν τώρα ισχύει επιπλέον $p > 3$, τότε ο M_p είναι σύνθετος.
(Υπόδειξη: Χρησιμοποιείστε τις 1. και 2.)

4. Να αποδείξετε ότι οι M_{11} και M_{23} είναι σύνθετοι.

5. Τις ασκήσεις του Βιβλίου 1, 4, 5, 6