ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
Τμήμα Μαθηματικών και
Εφαρμοσμένων Μαθηματικών

Εαρινό Εξάμηνο 2017-18
Θεόδουλος Γαρεφαλάκης

ΜΕΜ 204 ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Φυλλάδιο Ασκήσεων 4

Άσκηση 4.1 Έστω p περιττός πρώτος και $a \in \mathbb{Z}$ με $(a,p)=1$. Αποδείξτε ότι

$$\text{Είτε} \quad a^{p-1} \not\equiv 1 \pmod{p^2} \quad \text{ή} \quad (a+p)^{p-1} \not\equiv 1 \pmod{p^2}.$$

Άσκηση 4.2 Έστω p περιττός πρώτος και $a \in \mathbb{Z}$ με $(a,p)=1$. Υποθέστε ότι $a^{p-1} \not\equiv 1 \pmod{p^2}$. Αποδείξτε ότι $a^{p(p-1)} \not\equiv 1 \pmod{p^3}$.

Άσκηση 4.3 Σε ένα σχολείο με όχι περισσότερα από 500 παιδιά, όταν τα παιδιά παραταχθούν σε 7άδες περισσεύει ένα παιδί, όταν παραταχθούν σε οκτάδες περισσεύουν δύο παιδιά, ενώ όταν παραταχθούν σε εννιάδες υπολείπεται ένα παιδί. Πόσα παιδιά έχει το σχολείο;

Άσκηση 4.4 Έστω p πρώτος και $f(X) = (X+1)^p - X^p - 1 \in \mathbb{Z}[X]$.

α′. Δείξτε ότι ο βαθμός του $f(X)$ είναι $< p$.

β′. Δείξτε ότι οι αριθμοί $0, 1, \ldots, p-1$ είναι (ανά δύο ανισότιμες) ρίζες της ισοτιμίας $f(X) \equiv 0 \pmod{p}$.

γ′. Δείτε ότι $p \mid \binom{p}{k}$ για $1 \leq k \leq p-1$.

Άσκηση 4.5 Υπολογίστε τις τετραγωνικές ρίζες της μονάδας $\bmod 15$. Δηλαδή υπολογίστε όλους τους (ανά δύο ανισότιμους $\bmod 15$) ακεραίους που ικανοποιούν την $x^2 \equiv 1 \pmod{15}$. Πόσες λύσεις βρήκατε; Πόσες είναι οι λύσεις της $x^2 \equiv 1 \pmod{n}$, όταν η κανονική ανάλυση του n σε πρώτους είναι $n = p_1 \cdots p_k$, με $p_i \neq p_j$ για $i \neq j$;

Άσκηση 4.6 Έστω ότι ο αριθμός n είναι ίσος με το γινόμενο δύο διακεκριμένων πρώτων, ας τους ονομάσουμε p και q, τους οποίους δε γνωρίζετε. Σας δίνεται μία μη-τετριμμένη τετραγωνική ρίζα της μονάδας $\bmod n$, δηλαδή ένας αριθμός $x \in \mathbb{Z}$ τέτοιος ώστε $x^2 \equiv 1 \pmod{n}$, αλλά $x \not\equiv \pm 1 \pmod{n}$. Περιγράψτε πώς μπορείτε να βρείτε εύκολα την παραγοντοποίηση του n, δηλαδή τους p, q.