ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἑξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

Ἀσκήσεις τῆς $13^{\eta\varsigma}$ ἑβδομάδας

Ασκησεις Επαναληψης
(συνέχεια αὐτῶν τῆς $12^{\eta\varsigma}$ ἑβδομάδας)

6. Ἂν $a \neq 1$ καὶ $m \geq 1$, ἀποδεῖξτε ὅτι $\left(\dfrac{a^m - 1}{a-1}\,,\, a-1\right) = (m\,,\, a-1)$.

   Ὑπόδειξη. Παρατηρῆστε ὅτι ἀρκεῖ νὰ δείξετε τὸ ἑξῆς: Ἂν d εἶναι διαιρέτης τοῦ $a-1$, τότε ὁ d διαιρεῖ τὸν $(a^m-1)/(a-1)$ ἂν καὶ μόνο ἂν διαιρεῖ τὸν m.

7. Ὑπολογῖστε ὅλα τὰ ζεύγη θετικῶν ἀκεραίων (a, b), γιὰ τὰ ὁποῖα ἰσχύει $ab = 480$ καὶ $[a, b] = 240$.

   Ὑπόδειξη. Ἔστω $(a, b) = d$ (ἄγνωστος), $a = da_1$, $b = db_1$, ὁπότε $(a_1, b_1) = 1$. Θυμηθεῖτε τὴ σχέση $ab = (a, b) \cdot [a, b]$.

8. Ἔστω $p_1 < p_2 < p_3 < \cdots$ ἡ ἄπειρη ἀκολουθία τῶν πρώτων ἀριθμῶν (δηλαδή, $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ κλπ). Ἀποδεῖξτε τὰ ἑξῆς:
   (α′) Γιὰ κάθε $n \geq 2$ ἰσχύει $p_n \leq p_1 p_2 \cdots p_{n-1} + 1$.
   (β′) Μὲ τὴ βοήθεια τοῦ (α′) ἀποδεῖξτε ἐπαγωγικὰ ὅτι γιὰ κάθε $n \geq 1$ ἰσχύει $p_n \leq 2^{2^{n-1}}$ καὶ τὸ $=$ ἰσχύει μόνο γιὰ $n = 1$.

   Ὑπόδειξη γιὰ τὸ (α′). Ἔστω p_i κάποιος διαιρέτης τοῦ $p_1 p_2 \cdots p_{n-1} + 1$. Ἀποδεῖξτε ὅτι $i \geq n$.

9. Ἔστω ὅτι ὁ p εἶναι πρῶτος, τέτοιος ὥστε καὶ ὁ $8p-1$ νὰ εἶναι πρῶτος (π.χ. $p = 3, 13, 19, 61, 79, \ldots$), τότε ὁ $8p + 1$ εἶναι σύνθετος.

   Ὑπόδειξη. Γιὰ $p = 3$ διαπιτωστε ὅτι ὁ ἰσχυρισμὸς ἰσχύει. Γιὰ $p > 3$ ξεχωρῖστε τὶς περιπτώσεις $p \equiv 1 \pmod 3$ καὶ $p \equiv 2 \pmod 3$. Στὴ δεύτερη περίπτωση δεῖξτε ὅτι ὁ $8p - 1$ δὲν μπορεῖ νὰ εἶναι πρῶτος, ἄρα θὰ σᾶς μείνει ἡ πρώτη περίπτωση· ἀλλὰ τότε δεῖξτε ὅτι ὁ $8p + 1$ διαιρεῖται διὰ 3, ἄρα εἶναι σύνθετος.

10. Γιὰ ποιὲς τιμὲς τοῦ γνήσιου κλάσματος λ (δηλαδή, κλάσματος, στὴν ἀνάγωγη μορφὴ τοῦ ὁποίου ὁ παρονομαστής του εἶναι > 1) ὁ ἀριθμὸς $3\lambda^2 - 5\lambda$ εἶναι ἀκέραιος;

11. Ἂν $(a, b) = (b, c) = (c, a) = 1$, ἀποδεῖξτε ὅτι $(ab + bc + ca\,,\, abc) = 1$.

12. Ἂν ὁ p εἶναι περιττὸς πρῶτος, ἀποδεῖξτε ὅτι $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$ (οἱ προσθετέοι τοῦ ἀθροίσματος εἶναι σύμβολα Legendre).
   Ὑπόδειξη. Πόσα τετραγωνικὰ ἰσοϋπολοιπα περιέχονται στὸ σύνολο $\{1, 2, \ldots, p-1\}$;

13. Ἀποδεῖξτε ὅτι, ἂν ὁ p εἶναι πρῶτος $\neq 2, 5$, τότε

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{ἂν } p \equiv \pm 1 \pmod{10} \\ -1 & \text{ἂν } p \equiv \pm 3 \pmod{10}. \end{cases}$$

14. Ἀποδεῖξτε ὅτι, ἂν ὁ p εἶναι πρῶτος $\neq 2, 3$, τότε

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{ἂν } p \equiv 1 \pmod 6 \\ -1 & \text{ἂν } p \equiv -1 \pmod 6. \end{cases}$$

15. Ἔστω πρῶτος $p \equiv 3 \pmod 4$ καὶ a πρῶτος πρὸς τὸν p, τετραγωνικὸ ἰσοϋπόλοιπο $\pmod p$. Ἀποδεῖξτε ὅτι οἱ λύσεις τῆς ἰσοτιμίας $x^2 \equiv a \pmod p$ εἶναι οἱ $x \equiv \pm a^{(p+1)/4} \pmod p$.

16. Ἔστω περιττὸς πρῶτος p. Θεωροῦμε τὴν ἰσοτιμία $ax^2 + bx + c \equiv 0 \pmod p$, ὅπου $p \nmid a$. Ἀποδεῖξτε τὰ ἑξῆς:
(α′) Ἂν $b^2 - 4ac \equiv 0 \pmod p$, τότε ἡ ἰσοτιμία ἔχει ἀκριβῶς μία λύση.
(β′) Ἂν $b^2 - 4ac \not\equiv 0 \pmod p$, τότε ἡ ἰσοτιμία ἔχει δύο, ἀκριβῶς, λύσεις ἂν ὁ $b^2 - 4ac$ εἶναι τετραγωνικὸ ἰσοϋπόλοιπο $\pmod p$ καὶ καμμία λύση ἂν ὁ $b^2 - 4ac$ εἶναι τετραγωνικὸ ἀνισοϋπόλοιπο $\pmod p$.
Ὑπόδειξη καὶ γιὰ τὰ δύο ερωτήματα. Ἡ ἰσοτιμία $ax^2+bx+c \equiv 0 \pmod p$ εἶναι ἰσοδύναμη μὲ τὴν $4a(ax^2+bx+c) \equiv 0 \pmod p$. Παρατηρῆστε ὅτι $4a(ax^2 + bx + c) = (2ax)^2 + 2(2ax)b + 4ac = (2ax + b)^2 - b^2 + 4ac$, ἄρα ἡ ἀρχικὴ ἰσοτιμία εἶναι ἰσοδύναμη μὲ τὴν ....

17. Νὰ λυθεῖ ἡ ἰσοτιμία $3x^2 + 7x - 2 \equiv 0 \pmod{23}$.
Ὑπόδειξη. Δεῖτε τὴν προηγούμενη ἄσκηση, κυρίως τὴν ὑπόδειξη.

18. Ἔστω περιττός πρῶτος p καὶ $a_1, a_2, \ldots, a_{p'}$ ἐκεῖνοι ἀπὸ τοὺς ἀριθμοὺς $1, 2, \ldots, p-1$ ποὺ εἶναι τετραγωνικὰ ἰσοϋπόλοιπα $\pmod p$. (Ἀπὸ τὴ θεωρία, $p' = (p-1)/2$). Ἀποδεῖξτε ὅτι $a_1 a_2 \cdots a_{p'} \equiv (-1)^{(p+1)/2} \pmod p$.
Ὑπόδειξη. Ἔστω g ἕνας ὁποιοσδήποτε γεννήτορας $\pmod p$ καὶ $(a, p) = 1$. Ἀποδεῖξτε ὅτι ὁ a εἶναι τετραγωνικὸ ἰσοϋπόλοιπο $\pmod p$ ἂν καὶ μόνο ἂν ὁ διακριτὸς λογάριθμος $\mathrm{ind}_g(a)$ εἶναι ἄρτιος. Ἐπειδὴ $\mathrm{ind}_g(a) \in \{0, 1, 2, \ldots, p-2\}$, οἱ διακριτοὶ λογάριθμοι τῶν τετραγωνικῶν ἰσοϋπολοίπων εἶναι $0, 2, 4, \ldots, p-3$ ($p-3$ εἶναι ὁ μεγαλύτερος ἄρτιος $\leq p-2$), ἄρα τὸ γινόμενο ὅλων τῶν ἰσοϋπολοίπων εἶναι $\equiv g^0 g^2 g^4 \cdots g^{p-3} \equiv g^{0+2+4+\cdots+(p-3)} \pmod p$. Μετά, παρατηρῆστε τὰ ἑξῆς: (1) $0 + 2 + 4 + \cdots (p-3) = \frac{p-3}{2} \cdot \frac{p-1}{2}$. (2) $g^{(p-1)/2} \equiv -1 \pmod p$. (3) $(-1)^{(p-3)/2} = (-1)^{(p+1)/2}$.