ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἑξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

Ἀσκήσεις τῆς $7^{\eta\varsigma}$ ἑβδομάδας

1. Ποιὸς εἶναι ὁ ἐλάχιστος θετικὸς ἀκέραιος, ὁ ὁποῖος, διαιρούμενος διὰ 3 ἀφήνει ὑπόλοιπο 1, διαιρούμενος διὰ 5 ἀφήνει ὑπόλοιπο 2, διαιρούμενος διὰ 7 ἀφήνει ὑπόλοιπο 3 καὶ διαιρούμενος διὰ 11 ἀφήνει ὑπόλοιπο 4; Ἀποδεῖξτε, μετά, ὅτι ἀριθμὸς μὲ τέτοια ἰδιότητα, ποὺ νὰ βρίσκεται μεταξὺ 1000 καὶ 1500, δὲν ὑπάρχει.

2. Λύσετε χωριστὰ κάθε μία ἀπ' τὶς ἰσοτιμίες $412x \equiv 108 \pmod{34}$ καὶ $843x \equiv 1131 \pmod{105}$. Μετά, μὲ χρήση τοῦ "Κινέζικου Θεωρήματος" ὑπολογῖστε ὅλα τὰ ἀνισότιμα $x \pmod{34\cdot 105}$ ποὺ ἐπαληθεύουν συγχρόνως καὶ τὶς δύο ἰσοτιμίες.
   Ἀπάντηση: $x \equiv 27, 622, 1217, 1812, 2407, 3002 \pmod{34 \cdot 105}$.

3. Θεωροῦμε τοὺς πρώτους ἀριθμοὺς $p_1 = 7$, $p_2 = 13$ καὶ $p_3 = 17$. Σὲ ὅ,τι ἀκολουθεῖ, οἱ δεῖκτες i, j, k παίρνουν τιμὲς ἀπὸ τὸ $\{1, 2, 3\}$ καὶ εἶναι διαφορετικοὶ ἀνὰ δύο.
   Νὰ βρεθεῖ ἀκέραιος a ἀνάμεσα στὸ 12500 καὶ τὸ 13500, μὲ τὴν ἑξῆς ἰδιότητα: Γιὰ κάθε $i = 1, 2, 3$, τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ a διὰ p_i ἰσοῦται μὲ τὸ ὑπόλοιπο τῆς διαίρεσης τοῦ $p_j p_k$ διὰ p_i.
   Ὑπόδειξη: Ὁ a ἱκανοποιεῖ, συγχρόνως, τρεῖς ἰσοτιμίες, οἱ ὁποῖες πρέπει νὰ ἐπιλυθοῦν μὲ τὸ "Κινέζικο θεώρημα". Ἡ ἀπάντηση εἶναι: 12807.

4. Νὰ λυθεῖ τὸ σύστημα
$$2x + 11y \equiv 5 \pmod{493}, \quad 3x - 7y \equiv 1 \pmod{493}.$$
   Ὑπόδειξη. Προχωρῆστε σὲ ἀπαλοιφὴ τοῦ ἑνὸς ἀγνώστου, ὅπως θὰ τὸ κάνατε στὸ σχολεῖο, μὲ τὴ διαφορὰ ὅτι τώρα χειρίζεστε ἰσοτιμίες ἀντὶ ἐξισώσεων καὶ οἱ ἀριθμοὶ μὲ τοὺς ὁποίους θὰ πολλαπλασιάζετε γιὰ νὰ κάνετε ἀπαλοιφή, πρέπει νὰ εἶναι πρῶτοι πρὸς τὸν $493 = 17 \cdot 29$. Ἡ λύση εἶναι $x \equiv 473$, $y \equiv 273 \pmod{493}$.

5. Ἀποδεῖξτε τὸ ἀντίστροφο τοῦ θεωρήματος τοῦ Wilson: Ἂν $n > 1$ καὶ $(n-1)! \equiv -1 \pmod{n}$, τότε ὁ n εἶναι πρῶτος.

6. Ἔστω πρῶτος p καὶ πολυώνυμο $f(x)$ βαθμοῦ n (ἐν γένει, φανταζόμαστε ὅτι $n > p$. Ἔστω $f(x) = (x^p - x)q(x) + r(x)$. Ἀποδεῖξτε ὅτι ἡ ἰσοτιμία $f(x) \equiv 0 \pmod{p}$ ἔχει τὶς ἴδιες λύσεις μὲ τὴν ἰσοτιμία $r(x) \equiv 0 \pmod{p}$.

7. (Γιὰ ὅσους ἀγαποῦν τὶς μαθηματικὲς προκλήσεις.) Ἔστω περιττὸς πρῶτος p καὶ $q = (p-1)/2$. Χρησιμοποιώντας τὸ Θεώρημα τοῦ Wilson ἀποδεῖξτε ὅτι $(q!)^2 + (-1)^q \equiv 0 \pmod{p}$.
   Ὑπόδειξη: Στὸ θεώρημα τοῦ Wilson ἐμφανίζεται τὸ $(p-1)! = 1 \cdot 2 \cdots q(q+1)(q+2)\cdots(p-2)(p-1)$. Παρατηρῆστε ὅτι $q+1 \equiv p-q$, $q+2 \equiv p-(q-1), \ldots, p-2 \equiv -2$, $p-1 \equiv -1 \pmod{p}$.
   Παρατηρῆστε ὅτι, ἂν $p \equiv 1 \pmod{4}$, τότε μία λύση τῆς ἰσοτιμίας $x^2 \equiv -1 \pmod{p}$ εἶναι ἡ $x \equiv q! \pmod{p}$. Ἂν $p \equiv 3 \pmod{4}$, τότε $q! \equiv \pm 1 \pmod{p}$. (Πληροφοριακά: Σ' αὐτὴ τὴν περίπτωση δὲν ὑπάρχει κάποιος ἁπλὸς γενικὸς κανόνας ποὺ νὰ μᾶς λέει ποιὸ πρόσημο ἰσχύει στὴν τελευταία ἰσοτιμία.)