ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἑξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

Ἀσκήσεις τῆς $8^{\eta\varsigma}$ ἑβδομάδας

1. (α′) Ἔστω p εἶναι περιττὸς πρῶτος. Δεῖξτε ὅτι τὸ -1 εἶναι τετραγωνικὸ ἰσοϋπόλοιπο mod p ἂν $p \equiv 1 \pmod 4$ καὶ τετραγωνικὸ ἀνισοϋπόλοιπο mod p ἂν $p \equiv 3 \pmod 4$.
(β′) Ὑπολογῖστε ὅλα τὰ στοιχεῖα τοῦ κατ' ἀπόλυτη τιμὴ ἐλαχίστου συστήματος ὑπολοίπων mod p, τὰ ὁποῖα εἶναι τετραγωνικὰ ἰσοϋπόλοιπα mod p, γιὰ $p = 17$ καὶ $p = 19$, ἀντιστοίχως. Ἐξηγεῖστε, βάσει τοῦ (α′), γιατὶ ὅταν $p = 17$ τὰ στοιχεῖα αὐτὰ εἶναι ἀνὰ ζεύγη ἀντίθετα, ἐνῶ ὅταν $p = 19$, δὲν εἶναι.

2. Ἀποδεῖξτε τὴν ἑξῆς πολὺ ἁπλῆ πρόταση, τῆς ὁποίας χρήση γίνεται πολὺ συχνά: Ἂν ὁ $m > 1$ εἶναι περιττὸς καὶ $\epsilon \equiv \eta \pmod m$, ὅπου $\epsilon, \eta \in \{-1, 1\}$, τότε $\epsilon = \eta$.

3. Ἔστω $N = x^2 + y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξύ τους. Ἀποδεῖξτε ὅτι ὅλοι οἱ περιττοὶ πρῶτοι διαιρέτες τοῦ N εἶναι τῆς μορφῆς $4k + 1$.
Ὑπόδειξη. Ἔστω p περιττὸς πρῶτος διαιρέτης τοῦ N. Ἀποδεῖξτε πρῶτα ὅτι ὁ p δὲν διαιρεῖ κανέναν ἀπὸ τοὺς x, y. Ξέροντας μετὰ ὅτι $(y, p) = 1$, θεωρῆστε y' τέτοιον ὥστε $yy' \equiv 1 \pmod p$ καὶ δεῖξτε ὅτι $(xy')^2 \equiv -1 \pmod p$. Μετὰ ἐφαρμόστε τὴν ἄσκηση 1 (α′).

4. Ἔστω $N = x^2 - 2y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξύ τους καὶ ὁ x εἶναι περιττός. Ἀποδεῖξτε ὅτι, ἂν ἕνας πρῶτος p διαιρεῖ τὸν N, τότε ὁ p εἶναι ἢ τῆς μορφῆς $8k + 1$ ἢ τῆς μορφῆς $8k + 7$.
Ὑπόδειξη. Ἔστω p περιττὸς πρῶτος διαιρέτης τοῦ N. Ἀποδεῖξτε πρῶτα ὅτι ὁ p δὲν διαιρεῖ κανέναν ἀπὸ τοὺς x, y. Ξέροντας μετὰ ὅτι $(y, p) = 1$, θεωρῆστε y' τέτοιον ὥστε $yy' \equiv 1 \pmod p$ καὶ δεῖξτε ὅτι $(xy')^2 \equiv 2 \pmod p$. Ἐφαρμόστε μετὰ τὸν "Συμπληρωματικὸ νόμο τετραγωνικῆς ἀντιστροφῆς".

5. Ἔστω $N = x^2 + 2y^2$, ὅπου οἱ x, y εἶναι μὴ μηδενικοὶ ἀκέραιοι, πρῶτοι μεταξύ τους καὶ ὁ x εἶναι περιττός. Ἀποδεῖξτε ὅτι, ἂν ἕνας πρῶτος p διαιρεῖ τὸν N, τότε ὁ p εἶναι ἢ τῆς μορφῆς $8k + 1$ ἢ τῆς μορφῆς $8k + 3$.
Ὑπόδειξη ἐντελῶς ἀνάλογη μὲ αὐτὴν τῆς προηγούμενης ἄσκησης.

6. Ὑπολογῖστε τὴν τιμὴ τοῦ συμβόλου $\left(\frac{7}{13}\right)$. Στὴ συνέχεια, γιὰ $p = 13$ καὶ $a = 7$: Γρᾶψτε τὶς σχέσεις (4.5) (6 ἰσοτιμίες mod 13), καὶ ἐπαληθεῦστε τὶς σχέσεις (4.6) καὶ (4.7) τῶν Σημειώσεων.
Ἐπαναλάβετε τὴν ἄσκηση γιὰ $p = 19$ καὶ $a = 5$.

7. (α′) Ἀποδεῖξτε ὅτι, ἂν ὁ p εἶναι πρῶτος > 3, τότε $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$.
Ὑπόδειξη. Χρησιμοποιεῖστε τὴν Πρόταση 4.2.1 (δ′) καὶ τὸ Θεώρημα 4.2.3 (Νόμος τετραγωνικῆς ἀντιστροφῆς) τῶν Σημειώσεων.
(β′) Μὲ τὴ βοήθεια τοῦ (α′) ἀποδεῖξτε ὅτι ἕνας πρῶτος p τῆς μορφῆς $3k + 2$ δὲν μπορεῖ νὰ διαιρεῖ ἀριθμὸ τῆς μορφῆς $x^2 + 3y^2$, ὅπου οἱ x, y εἶναι ἀκέραιοι καὶ $(x, 3y) = 1$. Ὑπόδειξη ἀνάλογη μὲ αὐτὲς τῶν ἀσκήσεων 3 καὶ 4.

8. Ὑπολογῖστε τὶς τιμὲς τῶν παρακάτω συμβόλων Legendre, ἐργαζόμενοι ὅπως στὸ ἀριθμητικὸ παράδειγμα τῆς σελίδας 61 τῶν Σημειώσεων:

$$\left(\frac{97}{101}\right), \left(\frac{43}{97}\right), \left(\frac{22}{107}\right), \left(\frac{89}{131}\right), \left(\frac{389}{283}\right), \left(\frac{197}{443}\right), \left(\frac{199}{311}\right), \left(\frac{419}{677}\right).$$

Οἱ τιμὲς τῶν παραπάνω συμβόλων εἶναι, ἀντιστοίχως: $1, 1, -1, 1, 1, 1, -1, -1$.

Σημείωση: Οἱ ἀριθμοὶ $43, 89, 97, 101, 107, 131, 197, 199, 283, 311, 389, 419, 443, 677$ εἶναι πρῶτοι.