ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἐξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

Ἀσκήσεις τῆς $10^{\eta\varsigma}$ ἑβδομάδας

1. Δεῖξτε ὅτι καὶ οἱ δύο παρακάτω ἰσοτιμίες εἶναι ἐπιλύσιμες καὶ βρεῖτε τὶς λύσεις κάθε μιᾶς.

$$x^2 \equiv 241 \pmod{2^{10}}, \quad x^2 \equiv 65 \pmod{2^9}.$$

Λύσεις: Τῆς πρώτης ἰσοτιμίας εἶναι $x \equiv 167, 345, 679, 857 \pmod{2^{10}}$, καὶ τῆς δεύτερης $x \equiv 33, 223, 289, 479 \pmod{2^9}$

2. (α′) Λῦστε τὴν ἰσοτιμία $x^2 \equiv 241 \pmod{5^2}$.

Οἱ λύσεις της εἶναι $x \equiv 4, 21 \pmod{5^2}$.

(β′) Λῦστε τὴν ἰσοτιμία $x^2 \equiv 241 \pmod{2^{10} \cdot 5^2}$.

Ὑπόδειξη. Σύμφωνα μὲ τὴ θεωρία, ἡ δοθεῖσα ἰσοτιμία εἶναι ἰσοδύναμη μὲ τὸ σύστημα ἰσοτιμιῶν $x^2 \equiv 241 \pmod{2^{10}}$, $x^2 \equiv 241 \pmod{5^2}$. Στὴν προηγούμενη ἄσκηση ἔχει ἤδη λυθεῖ ἡ ἰσοτιμία $x^2 \equiv 241 \pmod{2^{10}}$. Ἀπὸ αὐτὴ συμπεραίναμε ὅτι $x \equiv 167, 345, 679, 857 \pmod{2^{10}}$, ἐνῶ ἀπὸ τὸ ἐρώτημα (α′) $x \equiv 4, 21 \pmod{5^2}$. Ἄρα ὅλες οἱ λύσεις $x \pmod{2^{10}5^2}$ προκύπτουν ἀπὸ τὴν ἐπίλυση τῶν 8 συστημάτων $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ὅπου $m_1 = 2^{10}$, $m_2 = 5^2$, $a_1 \in \{167, 345, 679, 857\}$ καὶ $a_2 \in \{4, 21\}$. Καθένα ἀπὸ αὐτὰ τὰ 8 συστήματα λύνεται σύμφωνα μὲ τὴ θεωρία τοῦ "Κινέζικου Θεωρήματος Ὑπολοίπων", ἀλλὰ ἐπειδὴ ὁ στόχος αὐτῆς τῆς ἀσκήσεως δὲν εἶναι ἡ ἐξάσκηση στὴ χρήση αὐτοῦ τοῦ θεωρήματος, σᾶς προτείνω νὰ λύσετε καθένα ἀπὸ τὰ συστήματα μὲ τὴ βοήθεια τοῦ Online Magma Calculator. Ἡ σύνταξη τῆς ἐντολῆς εἶναι ὡς ἑξῆς:

Ἂν π.χ. θέλει κανεὶς νὰ λύσει τὸ σύστημα $x \equiv 31 \pmod{125}$, $x \equiv -1 \pmod{49}$, θὰ δώσει τὴν ἐντολή `ChineseRemainderTheorem`([31,-1],[125,49]); (προσοχή, τὸ ; εἶναι ἀπαραίτητο) καὶ θὰ πάρει τὸν ἀριθμὸ 5781, ποὺ σημαίνει ὅτι ἡ λύση τοῦ συγκεκριμένου συστήματος εἶναι $x \equiv 5781 \pmod{125 \cdot 49}$.

Οἱ λύσεις τῆς ἰσοτιμίας τοῦ ἐρωτήματος (β′) ποὺ πρέπει νὰ βρεῖτε εἶναι:

$$x \equiv 679, 3929, 8871, 12121, 13479, 16729, 21671, 24921 \pmod{125 \cdot 49}..$$

Ὅπως εἶναι ἀναμενόμενο, ἀνὰ δύο οἱ λύσεις εἶναι ἀντίθετες $\pmod{125 \cdot 49}$· π.χ. $24921 \equiv -679 \pmod{125 \cdot 49}$.

3. (α′) Ἔστω $m > 1$, τέτοιος ὥστε τὸ σύνολο D τῶν διαιρετῶν τοῦ $\phi(m)$, οἱ ὁποῖοι εἶναι > 1 καὶ $< \phi(m)$ εἶναι νὰ εἶναι μὴ κενό. (Οἱ m γιὰ τοὺς ὁποίους δὲν ἰσχύει αὐτό, εἶναι ἐλάχιστοι καὶ μποροῦμε νὰ τοὺς προσδιορίσομε, ἀλλὰ δὲν μᾶς ἐνδιαφέρει αὐτὸ τώρα.) Ἔστω ὅτι γιὰ κάποιον a πρῶτο πρὸς τὸν m ἰσχύει $a^d \not\equiv 1 \pmod{m}$ γιὰ κάθε $d \in D$. Ἀποδεῖξτε ὅτι ὁ a εἶναι γεννήτορας $\pmod{m}$.

(β′) Μὲ τὴ βοήθεια τοῦ (α′) ἀποδεῖξτε ὅτι, γιὰ $m = 11, 17, 23, 22, 34, 46$ οἱ ἀριθμοὶ $a = 2, 3, 5, 7, 3, 5$ εἶναι γεννήτορες mod m.

4. Ὑπολογῖστε τὴν τάξη τοῦ $a \pmod{m}$ στὶς ἑξῆς περιπτώσεις: (i) $m = 15$, $a = 2$ (ii) $m = 11$, $a = 3$ (iii) $m = 17$, $a = 2$ (iv) $m = 43$, $a = 2$ (v) $m = 86$, $a = 3$.

Σὲ ποιὲς ἀπὸ τὶς παραπάνω περιπτώσεις εἶναι τὰ a γεννήτορας mod m;

Ὑπόδειξη. Θυμηθῆτε ὅτι $\mathrm{ord}_m(a) \mid \phi(m)$.

5. Μὲ χρήση τοῦ θεωρήματος 4.4.3 τῶν Σημειώσεων ὑπολογῖστε τὸ *πλῆθος* τῶν λύσεων τῆς ἰσοτιμίας $x^2 \equiv a \pmod{m}$ σὲ κάθε μία ἀπὸ τὶς παρακάτω περιπτώσεις (ἡ ἀπάντηση μπορεῖ νὰ εἶναι 0): (i) $m = 11^3 \cdot 17^2$, $a = 3$ (ii) $m = 5^{13} \cdot 19^3$, $a = 11$ (iii) $m = 2 \cdot 5^{10} \cdot 23^4$, $a = 29$ (iv) $m = 4 \cdot 5^{10} \cdot 23^4$, $a = 29$ (v) $m = 16 \cdot 5^{10} \cdot 23^4$, $a = 29$ (vi) $m = 16 \cdot 17^2 \cdot 41^3$, $a = 33$ (vii) $m = 32 \cdot 19^2 \cdot 29^3$, $a = 45$.

   Ἀπαντήσεις. (i): 0, (ii): 4, (iii): 4, (iv): 8, (v): 0, (vi): 16, (vii): 0.