ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἑξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

Ἀσκήσεις τῆς $11^{\eta\varsigma}$ ἑβδομάδας

1. Λύσετε τὶς ἀσκήσεις 1, 2, 3, 4 τῆς ἑνότητας 5.3 τῶν Σημειώσεων.

2. Θεωρῆστε τὸν πρῶτο 191. Στὸν πίνακα 5.1 τῶν Σημειώσεων θὰ βρεῖτε ἕνα συγκεκριμένο γεννήτορα $g \pmod{p}$. Ἀποδεῖξτε χρησιμοποιώντας τὴν ἄσκηση 4 τῶν Σημειώσεων, ὅτι ὁ g εἶναι γεννήτορας $\pmod{191^n}$, καθὼς καὶ γεννήτορας $\pmod{2 \cdot 191^n}$ γιὰ κάθε $n \geq 1$. Γιὰ τὸ $\pmod{2 \cdot 191^n}$ θὰ χρειαστεῖτε τὸ Θεώρημα 5.1.5 (γ΄) τῶν Σημειώσεων,

   Ὑπολογιστικὲς ὁδηγίες: Οἱ ὑπολογισμοὶ τῆς μορφῆς $a^n \pmod{m}$ ποὺ θ' ἀπαιτηθοῦν, νὰ γίνουν στὸν ὑπολογιστὴ μὲ χρήση ὁποιουδήποτε ὑπολογιστικοῦ πακέτου θέλετε. Π.χ., ἕνα online ὑπολογιστικὸ πακέτο εἶναι τὸ Online Magma Calculator. Γιὰ γιὰ τὸν ὑπολογισμὸ τοῦ $a^n \pmod{m}$ ἡ σύνταξη τῆς ἐντολῆς εἶναι: `a^n mod m;` (μὴ ξεχάσετε τὸ ; καὶ πατῆστε μετὰ τὸ "κουμπὶ" Submit).

3. Θεωρῆστε τὸν πρῶτο 337. Στὸν πίνακα 5.1 τῶν Σημειώσεων θὰ βρεῖτε ἕνα συγκεκριμένο γεννήτορα $g \pmod{p}$. Ἀποδεῖξτε χρησιμοποιώντας τὴν ἄσκηση 4 τῶν Σημειώσεων, ὅτι ὁ g εἶναι γεννήτορας $\pmod{337^n}$ γιὰ κάθε $n \geq 1$. Κάνοντας χρήση τοῦ Θεωρήματος 5.1.5 (γ΄) τῶν Σημειώσεων, ὑπολογῖστε ἕνα γεννήτορα $g \pmod{2 \cdot 337^5}$. Ὁ g_1 ποὺ θὰ βρεῖτε εἶναι πολὺ μεγάλος. Μπορεῖ νὰ βρεθεῖ κάποιος πιὸ "φιλικός" γεννήτορας $\pmod{2 \cdot 337^n}$ καί, μάλιστα, γιὰ ὁποιοδήποτε $n \geq 1$; Ναί, ὡς ἑξῆς (συνεχίζεται ἡ ἄσκηση): Ὑπολογῖστε τὸν $g_2 \equiv g^{11} \pmod{337}$ καὶ διαπιστῶστε ὅτι ὁ g_2 εἶναι πολὺ μικρός. (α΄) Γιατὶ g_2 εἶναι, ἐπίσης, γεννήτορας $\pmod{337}$; (β΄) Γιατὶ ὁ g_2 εἶναι γεννήτορας $\pmod{337^n}$ καθὼς καὶ $\pmod{2 \cdot 337^n}$ γιὰ κάθε $n \geq 1$;

   Ὑπολογιστικὲς ὁδηγίες ἴδιες μὲ αὐτὲς τῆς προηγούμενης ἄσκησης.

4. Λύσετε τὶς ἀσκήσεις 14 καὶ 15 τῆς ἑνότητας 5.3 τῶν Σημειώσεων.

5. Λύσετε τὶς ἀσκήσεις 16 (β΄), (γ΄), (ε΄) τῆς ἑνότητας 5.3 τῶν Σημειώσεων. (Ἡ ἄσκηση 16 (α΄) λύθηκε στὸ μάθημα.)