# ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἑξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

## Ἀσκήσεις τῆς $5^{\eta\varsigma}$ ἑβδομάδας

1. (α΄) Διαπιστῶστε ὅτι οἱ ἀριθμοὶ 449, 541, 863 εἶναι πρῶτοι κάνοντας χρήση τοῦ Θεωρήματος 1.4.2 (δ΄) τῶν Σημειώσεων.
   (β΄) Γιὰ καθέναν ἀπὸ τοὺς ἀριθμοὺς $m \in \{1800, 3000, 13500\}$ βρεῖτε τὴν κανονικὴ ἀνάλυσή του σὲ πρώτους καὶ τὴν τιμὴ τοῦ $\phi(m)$.
   (γ΄) Γιὰ κάθε μία ἀπὸ τὶς παρακάτω τριάδες $(a, e, m)$ κάνετε τὰ ἑξῆς: Παρατηρῆστε ὅτι ὁ $m$ εἶναι κάποιος ἀπὸ τοὺς ἀριθμοὺς ποὺ ἐμφανίζονται σὲ ἕνα ἀπὸ τὰ ἐρωτήματα (α΄) ἢ (β΄). Ὑπολογῖστε ἀριθμὸ $1 \leq b \leq m-1$ τέτοιον ὥστε $a \equiv b \pmod{m}$. Διαπιστῶστε ὅτι $(b, m) = 1$, ἄρα $(a, m) = 1$ (γιατί;). Μὲ τὴ βοήθεια τοῦ Θεωρήματος Euler, ἢ Fermat (ἀναλόγως τοῦ $m$) ὑπολογῖστε τὸ ὑπόλοιπο τῆς διαίρεσης $b^e : m$. (Γιατὶ αὐτὸ εἶναι ἴσο μὲ τὸ ὑπόλοιπο τῆς διαίρεσης $a^e : m$;) Ὅταν ὑψώνετε σὲ δύναμη μὲ μεγάλο ἐκθέτη θὰ ἐφαρμόζετε τὸν ἀλγόριθμο ποὺ περιγράφεται στὴ σελίδα 35 τῶν Σημειώσεων.

   $$(a, e, m) \in \{(4501, 1383, 449), (9019, 1011, 1800), (4331, 4377, 863), (40543, 10889, 13500)\}$$

   Ἀπάντηση: Τὰ ὑπόλοιπα εἶναι, ἀντιστοίχως, 369, 19, 116, 3343.

2. Λῦστε τὴν ἄσκηση 7 τῆς ἑνότητας 2.5 τῶν τῶν Σημειώσεων.
   Ὑπόδειξη. Τὰ πρῶτα ἐρωτήματα τῶν ἀσκήσεων 1 καὶ 5 τῆς ἴδιας ἑνότητας θὰ σᾶς εἶναι πολὺ χρήσιμα.

3. Ἀποδεῖξτε τὴν ἑξῆς ἐναλλακτικὴ μορφὴ τοῦ θεωρήματος τοῦ Fermat: Γιὰ κάθε πρῶτο $p$ καὶ γιὰ κάθε ἀκέραιο $a$ (δίχως ν' ἀπαιτεῖται ὁ περιορισμὸς $(a, p) = 1$) ἀποδεῖξτε ὅτι ἰσχύει $a^p \equiv a \pmod{p}$.

4. (α΄) Ἔστω πρῶτος $p$, $a$ ὁποιοσδήποτε ἀκέραιος καὶ $n$ θετικὸς ἀκέραιος, $n \equiv 1 \pmod{p-1}$. Ἀποδεῖξτε ὅτι ὁ $a^n - a$ εἶναι διαιρετὸς ἀπὸ τὸν $p$.
   (β΄) Ἐφαρμογὴ τοῦ (α΄): Ἀποδεῖξτε ὅτι, γιὰ κάθε $a$, ὁ $a^{37} - a$ διαιρεῖται ἀπὸ τὸν 383838.
   Ὑπόδειξη. $383838 = 2 \cdot 3 \cdot 7 \cdot 13 \cdot 19 \cdot 37$.

5. (α΄) Ἔστω ἀκέραιος $m > 1$ καὶ $a$ ἀκέραιος πρῶτος πρὸς $m$. Ἔστω θετικὸς ἀκέραιος $e > 1$ πρῶτος πρὸς $\phi(m)$. Ἀποδεῖξτε ὅτι ὑπάρχει θετικός ἀκέραιος $d$, τέτοιος ὥστε $a^{de} \equiv a \pmod{m}$.
   Ὑπόδειξη. Δεῖξτε, κατ' ἀρχάς, ὅτι ἡ ἐξίσωση $ex + \phi(m)y = 1$ ἔχει λύση $(x_0, y_0)$. Μετά, ἀπὸ τὸν τῦπο τῆς γενικῆς λύσης, δεῖξτε ὅτι ὑπάρχει λύση (στὴν πραγματικότητα, ἄπειρες λύσεις) μὲ θετικὸ $x$. Μετά, εἶστε ἕνα βῆμα ἀπὸ τὸ νὰ ὁλοκληρώσετε τὴν ἀπόδειξη.
   (β΄) Ἐφαρμογὴ τοῦ (α΄): Ὑπολογῖστε τὸ $a \pmod{299}$ ἂν γνωρίζετε ὅτι $a^{17} \equiv 209 \pmod{299}$.
   Ὑπόδειξη. Γιὰ νὰ ἐφαρμόσετε τὸ (α΄) ξεκινῆστε τὴ λύση παραγοντοποιώντας τὸν 299.