

# ΥΠΟΛΟΓΙΣΤΙΚΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ  
ΠΑΝ/ΜΙΟΥ ΠΕΙΡΑΙΩΣ  
2020

2η Ομάδα Ασκήσεων (Παράδοση μέχρι την Τετάρτη 27/5/2020)

**Άσκηση 21.** Να αποδειχθεί ότι αν ο 3 δεν διαιρεί τους  $a, b$ , τότε η εξίσωση  $x^2 = a^2 + b^2$  δεν έχει ακέραια λύση.

**Άσκηση 22.** Αν  $a, b, k \in \mathbb{Z}$ ,  $k \neq 0$ , να αποδειχθεί ότι  $ka \equiv kb \pmod{n} \Leftrightarrow a \equiv b \pmod{n/d}$ , όπου  $d = \mu\kappa\delta(n, k)$ .

**Άσκηση 23.** Να αποδειχθεί ότι  $10 \mid 7 \cdot 1968^{1968} - 3 \cdot 68^{78}$ .

**Άσκηση 24.** Να αποδειχθεί ότι  $2730 \mid a^{13} - a$ , για κάθε  $a \in \mathbb{Z}$ .

**Άσκηση 25.** Να αποδειχθεί ότι αν  $a, b$  θετικοί ακέραιοι με  $\mu\kappa\delta(a, b) = 1$ , τότε  $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$ .

**Άσκηση 26.** Να αποδειχθεί ότι για κάθε  $n \in \mathbb{N}$  ισχύει η σχέση  $5^n \equiv 1 + 4n \pmod{16}$ .

**Άσκηση 27.** Ποια είναι τα τελευταία 2 ψηφία του αριθμού  $3^{1000}$ ;

**Άσκηση 28.** Να αποδειχθεί ότι αν  $p$  πρώτος και  $a, b \in \mathbb{Z}$ , τότε

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

**Άσκηση 29.** Να αποδειχθεί ότι αν  $p$  περιττός πρώτος, τότε η ισοτιμία  $x^2 + 1 \equiv 0 \pmod{p}$  έχει λύση αν  $p \equiv 1 \pmod{4}$ .

**Άσκηση 30.** Να λυθούν οι ισοτιμίες

$$21x \equiv 12 \pmod{33}, \quad 7x \equiv 17 \pmod{120}, \quad -671x \equiv 121 \pmod{737}.$$

**Άσκηση 31.** Αν  $a, b, n \in \mathbb{Z}$ ,  $n > 1$ , με  $\mu\kappa\delta(a, n) = \mu\kappa\delta(b, n) = 1$ , να δειχθεί ότι

$$ab \equiv 1 \pmod{n} \Rightarrow \text{ord}([a]_n) = \text{ord}([b]_n)$$

**Άσκηση 32.** Να ευρεθούν όλες οι αρχικές ρίζες  $\text{mod } 49$ .

**Άσκηση 33.** Να ευρεθούν οι λύσεις των παρακάτω ισοτιμιών:

$$x^2 - 6x - 13 \equiv 0 \pmod{127}, \quad x^2 + 6x - 154 \equiv 0 \pmod{399}.$$

**Άσκηση 34.** Να υπολογισθούν τα σύμβολα του Jacobi:

$$(102/231), \quad (131/1999).$$

**Άσκηση 35.** Αν  $p$  περιττός πρώτος, να αποδειχθεί ότι

$$(3/p) = \begin{cases} 1, & p \equiv \pm 1 \pmod{12}, \\ -1, & p \equiv \pm 5 \pmod{12}. \end{cases}$$