

Ασκήσεις Πεπερασμένων Σωμάτων και κρυπτογραφίας  
3 Φυλλάδιο

**Άσκηση 1** Υπολογίστε τα παρακάτω σύμβολα του Legendre:

$$\left(\frac{3}{97}\right), \left(\frac{3}{389}\right), \left(\frac{22}{11}\right), \left(\frac{5!}{7}\right).$$

**Λύση** Παρατηρούμε ότι οι αριθμοί 3, 7, 97, 389 είναι πρώτοι. Θα χρησιμοποιήσουμε τον νόμο αντιστροφής που εξασφαλίζει ότι

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

- $\left(\frac{3}{97}\right) = (-1)^{\frac{96}{2}} \left(\frac{97}{3}\right) = (-1)^{48} \left(\frac{1}{3}\right) = 1.$
- $\left(\frac{3}{389}\right) = (-1)^{\frac{388}{2}} \left(\frac{389}{3}\right) = (-1)^{194} \left(\frac{2}{3}\right) = -1.$
- $\frac{22}{11} = 0$  γιατί  $11 \mid 22.$
- $\left(\frac{5!}{7}\right) = \left(\frac{1}{7}\right) \left(\frac{2}{7}\right) \left(\frac{3}{7}\right) \left(\frac{4}{7}\right) \left(\frac{5}{7}\right).$  Υπολογίζουμε όλα τα τετράγωνα modulo 7

$$(\pm 1)^2 \equiv 1 \pmod{7}, (\pm 2)^2 \equiv 4 \pmod{7}, (\pm 3)^2 \equiv 2 \pmod{7}.$$

Στον παραπάνω υπολογισμό αντί του συστήματος αντιπροσώπων modulo 7  $\{1, 2, 3, 4, 5, 6, 7\}$  έχουμε χρησιμοποιήσει το βολικότερο  $\{0, \pm 1, \pm 2, \pm 3\}.$  Άρα τα σύμβολα του Legendre υπολογίζονται σε

$$\left(\frac{1}{7}\right) = 1, \left(\frac{2}{7}\right) = 1, \left(\frac{3}{7}\right) = -1, \left(\frac{4}{7}\right) = 1, \left(\frac{5}{7}\right) = -1.$$

και συνεπώς

$$\left(\frac{5!}{7}\right) = 1.$$

Ένας διαφορετικός τρόπος να απαντήσουμε στο ερώτημα είναι χρησιμοποιώντας το θεώρημα του Wilson που εξασφαλίζει ότι  $(p-1)! \equiv -1 \pmod{p}.$  Σε αυτή την περίπτωση θα είχαμε

$$6! \equiv -1 \pmod{7} \text{ άρα } 5! \equiv 1 \pmod{7}$$

και το ζητούμενο είναι σαφές.

**Άσκηση 2** Να υπολογιστεί το πλήθος των  $x < 2^{13}$  που ικανοποιούν την εξίσωση

$$x^2 \equiv 5 \pmod{2^{13} - 1}.$$

Δίνεται ότι το  $2^{13} - 1$  είναι πρώτος.

**Λύση:** Η εξίσωση αφού  $2^{13} - 15$  θα έχει καμία ή δύο λύσεις. Υπολογίζουμε

$$\left(\frac{5}{2^{13} - 1}\right) = (-1)^{\frac{(5-1)(2^{13}-2)}{4}} \left(\frac{2^{13} - 1}{5}\right).$$

Θέλουμε να υπολογίσουμε το υπόλοιπο της διαίρεσης του  $2^{13} - 1$  με 5. Αυτό μπορούμε να το κάνουμε υπολογίζοντας το  $2^{13}$ . Αλλά μπορούμε να επιχειρηματολογήσουμε και ως εξής:

$$2^4 \equiv 1 \pmod{5} \text{ άρα } 2^{13} \equiv ((2^4)^3 2 \equiv 2 \pmod{5}.$$

Άρα καταλήγουμε να υπολογίζουμε  $\left(\frac{1}{5}\right) = 1$ .

**Άσκηση 3** Χρησιμοποιήστε το γεγονός ότι η ομάδα των μονάδων του  $\mathbb{F}_p$  είναι κυκλική για να δώσετε μια απόδειξη ότι η

$$x^2 \equiv -3 \pmod{p}$$

όταν  $p \equiv 1 \pmod{3}$ . Υπόδειξη: υπάρχει στοιχείο  $c \in \mathbb{F}_p^*$  τάξης 3. Αποδείξτε ότι  $(2c + 1)^2 = -3$ .

**Λύση** Αν  $g$  είναι ένας γεννήτορας της κυκλικής ομάδας  $\mathbb{F}_p^*$  τότε  $c = g^{\frac{p-1}{3}}$  έχει τάξη 3. Αφού  $c \neq 1$  και  $0 = c^3 - 1 = (c - 1)(c^2 + c + 1)$  έχουμε ότι  $c^2 + c + 1 = 0$ . Άρα

$$(2c + 1)^2 = 4c^2 + 4c + 1 = -3 \pmod{p}$$

και συνεπώς το  $-3$  είναι τετραγωνικό υπόλοιπο.

**Άσκηση 4** Έστω  $(a, b) \in \mathbb{F}_p$ . Αποδείξτε ότι το πλήθος του σύνολου των σημείων  $(x, y) \in \mathbb{F}_p$  τα οποία ικανοποιούν την εξίσωση

$$y^2 = x^3 + ax + b$$

δίνονται από τον τύπο:

$$p + \sum_{x \in \mathbb{F}_p} \left( \frac{x^3 + ax + b}{p} \right).$$

**Λύση:** Για κάθε  $x \in \mathbb{F}_p$  αν το  $x^3 + ax + b \in \mathbb{F}_p$  είναι τετράγωνο αλλά

$px^3 + ax + b$  τότε η εξίσωση μας έχει δύο λύσεις, τις  $(x, y)$  όπου  $y$  είναι μία από τις δύο τετραγωνικές ρίζες του  $x^3 + ax + b$ . Σε αυτή την περίπτωση παρατηρούμε ότι το πλήθος των λύσεων που έχουν την πρώτη συντεταγμένη ίση με  $x$  είναι  $2 = 1 + \left(\frac{x^3 + ax + b}{p}\right)$ .

Αν  $p \mid x^3 + ax + b$  τότε υπάρχει μία μόνο λύση στην εξίσωση που να έχει συντεταγμένη  $x$ . Και σε αυτή την περίπτωση το πλήθος των λύσεων που έχουν την πρώτη συντεταγμένη ίση με  $x$  είναι ίσο με  $1 = 1 + \left(\frac{x^3 + ax + b}{p}\right)$ .

Τέλος αν το  $x^3 + ax + b$  δεν είναι τετράγωνο τότε δεν υπάρχει καμία λύση  $(x, y)$  της εξίσωσης που να έχει ως πρώτη συντεταγμένη το  $x$ . Και σε αυτή την περίπτωση το πλήθος των λύσεων που έχουν την πρώτη συντεταγμένη ίση με  $x$  είναι ίσο με  $0 = 1 + \left(\frac{x^3 + ax + b}{p}\right)$ .

Συνεπώς το συνολικό πλήθος των λύσεων είναι ίσο με

$$\sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) = p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$$