Θεωρία Αριθμών

Ασκήσεις

Μιχάλης Παπαδημητράκης

Τμήμα Μαθηματικών

Πανεπιστήμιο Κρήτης

Τετραγωνικά υπόλοιπα.

1. Με την βοήθεια του Λήμματος του Gauss βρείτε τους
$$\Big(\frac{8}{11}\Big), \quad \Big(\frac{7}{13}\Big), \quad \Big(\frac{5}{19}\Big), \quad \Big(\frac{11}{23}\Big), \quad \Big(\frac{6}{31}\Big).$$

2. Υπολογίστε τους
$$\Big(\frac{1234}{4567}\Big), \quad \Big(\frac{3658}{12703}\Big).$$

3. Έστω πρώτος $p > 2$ και $p \nmid a$, $p \nmid b$. Αποδείξτε ότι είτε όλες οι εξισώσεις
$$x^2 \equiv a \pmod p, \quad y^2 \equiv b \pmod p, \quad z^2 \equiv ab \pmod p$$
έχουν λύση είτε ακριβώς μία έχει λύση.
Με βάση το προηγούμενο, αποδείξτε ότι για κάθε πρώτο p υπάρχει n ώστε
$$p \mid (n^2 - 2)(n^2 - 3)(n^2 - 6).$$

4. Έχει λύση η εξίσωση
$$x^2 + 7y - 2 = 0;$$

5. Έστω πρώτοι p, q ώστε $p \neq q$, $p \equiv q \equiv 3 \pmod 4$. Αν η $x^2 \equiv p \pmod q$ δεν έχει λύση, αποδείξτε ότι η $x^2 \equiv q \pmod p$ έχει λύση.

6. Έστω πρώτος $p > 2$ ώστε $p \nmid a$. Αποδείξτε ότι η εξίσωση
$$ax^2 + bx + c \equiv 0 \pmod p$$
έχει λύση αν και μόνο αν $p \mid b^2 - 4ac$ ή το $b^2 - 4ac$ είναι τετραγωνικό υπόλοιπο $\bmod\, p$.
Λύστε την $x^2 + 7x + 10 \equiv 0 \pmod{11}$.
Αποδείξτε οτι η $6x^2 + 5x + 1 \equiv 0 \pmod p$ έχει λύση για κάθε πρώτο p.

7. Προσδιορίστε τους πρώτους p για τους οποίους η $x^2 \equiv 13 \pmod p$ έχει λύση.

8. Έστω πρώτος p ώστε $p \equiv 3 \pmod 4$. Αν $a^2 + b^2 \equiv 0 \pmod p$, αποδείξτε ότι $a \equiv b \equiv 0 \pmod p$.

9. Χρησιμοποιώντας το ότι $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ για κάθε πρώτο $p > 2$, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $8k - 1$.

10. Έστω πρώτος $p > 2$. Αποδείξτε ότι
$$\Big(\frac{-2}{p}\Big) = \begin{cases} 1, & \text{αν } p \equiv 1 \text{ ή } 3 \pmod 8 \\ -1, & \text{αν } p \equiv 5 \text{ ή } 7 \pmod 8 \end{cases}$$
Με βάση αυτό το συμπέρασμα, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $8k + 3$.

11. Έστω πρώτος $p > 3$. Αποδείξτε ότι
$$\Big(\frac{3}{p}\Big) = \begin{cases} 1, & \text{αν } p \equiv 1 \text{ ή } 11 \pmod{12} \\ -1, & \text{αν } p \equiv 5 \text{ ή } 7 \pmod{12} \end{cases}$$
$$\Big(\frac{-3}{p}\Big) = \begin{cases} 1, & \text{αν } p \equiv 1 \pmod 6 \\ -1, & \text{αν } p \equiv 5 \pmod 6 \end{cases}$$
Με βάση το πρώτο, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $12k \pm 1$ και, με βάση το δεύτερο, αποδείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $6k + 1$.

12. Αν ο $p > 3$ είναι πρώτος, αποδείξτε ότι ο p διαιρεί το άθροισμα των τετραγωνικών υπολοίπων $\bmod\, p$.