Θεωρία Αριθμών

Ασκήσεις

Μιχάλης Παπαδημητράκης

Τμήμα Μαθηματικών

Πανεπιστήμιο Κρήτης

Ισοτιμίες.

1. Αποδείξτε ότι
$$7 \mid 111^{333} + 333^{111}.$$

2. Αποδείξτε ότι
$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}.$$

3. Βρείτε το υπόλοιπο της διαίρεσης του 4444^{4444} από το 9.

4. Βρείτε ένα πλήρες και ένα περιορισμένο σύστημα υπολοίπων mod 17 τα οποία αποτελούνται από πολλαπλάσια του 3.

5. Αποδείξτε ότι το $\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$ είναι περιορισμένο σύστημα υπολοίπων mod 14 και ότι το $\{2, 2^2, 2^3, \ldots, 2^{18}\}$ είναι περιορισμένο σύστημα υπολοίπων mod 27.

6. Γράψτε μία ισοτιμία ισοδύναμη με το σύστημα
$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \end{cases}$$

7. Λύστε την
$$x^3 + 4x + 8 \equiv 0 \pmod{15}.$$

8. Έστω ότι ο $N \geq 1$ είναι γραμμένος στο δεκαδικό σύστημα στη μορφή
$$N = a_m a_{m-1} \ldots a_1 a_0.$$
Αποδείξτε ότι
$$\begin{aligned} &9 \mid N \;\Leftrightarrow\; 9 \mid a_m + a_{m-1} + \cdots + a_1 + a_0. \\ &11 \mid N \;\Leftrightarrow\; 11 \mid (-1)^m a_m + (-1)^{m-1} a_{m-1} + \cdots - a_1 + a_0. \end{aligned}$$

9. Έστω πρώτος p ώστε $1 \leq n < p < 2n$. Αποδείξτε ότι
$$\binom{2n}{n} \equiv 0 \pmod p.$$

10. Έστω περιττός a. Αποδείξτε ότι
$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

11. Έστω $\{a_1, \ldots, a_{\phi(n)}\}$ οποιοδήποτε περιορισμένο σύνολο υπολοίπων mod n. Αν $n \geq 3$, αποδείξτε ότι
$$a_1 + \cdots + a_{\phi(n)} \equiv 0 \pmod n.$$

12. Βρείτε τα δύο τελευταία δεκαδικά ψηφία του αριθμού 9^{9^9}.

13. Αποδείξτε ότι για κάθε a ισχύει
$$a^{21} \equiv a \pmod{15}, \quad a^7 \equiv a \pmod{42}, \quad a^9 \equiv a \pmod{30}, \quad a^{37} \equiv a \pmod{1729}$$
και ότι, αν $(a, 35) = 1$, τότε
$$a^{12} \equiv 1 \pmod{35}.$$

14. Έστω ότι οι p, q είναι πρώτοι και $p \neq q$. Αποδείξτε ότι

$$a^p \equiv a \pmod{q}, \;\; a^q \equiv a \pmod{p} \;\;\Rightarrow\;\; a^{pq} \equiv a \pmod{pq}.$$

15. Αν ο p είναι πρώτος και $p \nmid a$, αποδείξτε ότι το $a^{p-2}b$ είναι λύση της

$$ax \equiv b \pmod{p}.$$

Λύστε τις

$$2x \equiv 1 \pmod{31}, \qquad 3x \equiv 17 \pmod{29}.$$

Αν $(a, n) = 1$, αποδείξτε ότι το $a^{\phi(n)-1}b$ είναι λύση της

$$ax \equiv b \pmod{n}.$$

Λύστε τις

$$3x \equiv 5 \pmod{26}, \qquad 10x \equiv 21 \pmod{49}.$$

16. Αν ο p είναι πρώτος, αποδείξτε ότι:

$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$.
$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$, όταν $p \neq 2$.

17. Αν ο p είναι πρώτος, αποδείξτε ότι

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

18. Αποδείξτε ότι υπάρχουν άπειροι σύνθετοι n για τους οποίους ισχύει

$$a^{n-1} \equiv 1 \pmod{n}.$$

19. Αν $m, n \geq 1$ και $(m, n) = 1$, αποδείξτε ότι

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}.$$

20. Αν ο p είναι πρώτος, $p \nmid a$, $p \nmid b$, αποδείξτε ότι

$$a^p \equiv b^p \pmod{p} \;\;\Rightarrow\;\; a^p \equiv b^p \pmod{p^2}.$$

21. Αν ο $p \neq 2$ είναι πρώτος και $0 \leq k \leq p-1$, αποδείξτε ότι

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

22. Σχηματίζουμε την ακολουθία (a_n) με $a_1 = 3$ και τον αναδρομικό τύπο

$$a_{n+1} = 3^{a_n} \qquad \text{για κάθε } n.$$

Ποιά είναι τα δύο τελευταία δεκαδικά ψηφία του a_n;

23. (Δεύτερη απόδειξη του Θεωρήματος του Fermat.)

Αν ο p είναι πρώτος και $1 \leq k \leq p-1$, αποδείξτε ότι

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Αν ο p είναι πρώτος, αποδείξτε με επαγωγή ότι

$$a^p \equiv a \pmod{p}$$

για κάθε φυσικό a και, κατόπιν, αποδείξτε το ίδιο για κάθε ακέραιο a.

Αν ο p είναι πρώτος και $p \nmid a$, αποδείξτε ότι

$$a^{p-1} \equiv 1 \pmod{p}.$$

24. (Δεύτερη απόδειξη του Θεωρήματος του Euler.) Θεωρήστε γνωστό το Θεώρημα του Fermat.

Αν ο p είναι πρώτος και $p \nmid a$, αποδείξτε με επαγωγή ότι

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^{\alpha}}$$

για κάθε φυσικό α.

Αν $(a, n) = 1$ και $n > 1$, χρησιμοποιήστε την κανονική αναπαράσταση του n για να αποδείξετε ότι

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

25. Έστω $n \geq 2$. Αποδείξτε ότι:

$$\text{ο } n \text{ είναι πρώτος} \;\Leftrightarrow\; (n-2)! \equiv 1 \pmod{n} \;\Leftrightarrow\; (n-1)! \equiv -1 \pmod{n}.$$

26. Αν ο $p \neq 2$ είναι πρώτος, αποδείξτε ότι

$$1^2 3^2 5^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

27. Αν ο $p \neq 2$ είναι πρώτος, αποδείξτε ότι

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Με βάση αυτό το αποτέλεσμα, αποδείξτε ότι

$$p \equiv 1 \pmod{4} \;\Rightarrow\; \text{η } x^2 + 1 \equiv 0 \pmod{p} \text{ έχει λύση.}$$

Ποιά είναι η λύση;

Λύστε τις

$$x^2 + 1 \equiv 0 \pmod{29}, \qquad x^2 + 1 \equiv 0 \pmod{37}.$$

Αντιστρόφως, αποδείξτε ότι

$$\text{η } x^2 + 1 \equiv 0 \pmod{p} \text{ έχει λύση} \;\Rightarrow\; p \equiv 1 \pmod{4}.$$

28. Λύστε τις

$$36x \equiv 8 \pmod{102}, \qquad 5x \equiv 2 \pmod{26}, \qquad 6x \equiv 15 \pmod{21}.$$

29. Λύστε τα συστήματα

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases} \qquad \begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 9 \pmod{6} \\ 4x \equiv 1 \pmod{7} \\ 5x \equiv 9 \pmod{11} \end{cases}$$

30. Αποδείξτε ότι το σύστημα

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

έχει λύση αν και μόνο αν $(m, n) \mid a - b$ και ότι, αν υπάρχει λύση, τότε αυτή είναι μοναδική mod$[m, n]$.

31. Θεωρήστε την εξίσωση

$$ax \equiv b \pmod{15}.$$

Αν επιλέγουμε το a με τυχαίο τρόπο από τα $1, \ldots, 14$ και το b από τα $0, 1, \ldots, 14$, τότε ποιά είναι η πιθανότητα να έχει λύση η εξίσωση και ποιά είναι η πιθανότητα να έχει ακριβώς μία λύση η εξίσωση;

32. Έστω ότι ο p είναι πρώτος, $p \nmid a$, $r > 1$, $s > 1$, $rs > p$.

Θεωρήστε τους rs αριθμούς

$$ax - y$$

όταν το x διατρέχει τους $0, 1, \ldots, r - 1$ και το y διατρέχει τους $0, 1, \ldots, s - 1$. Αποδείξτε ότι υπάρχουν δύο τουλάχιστον επιλογές ζευγαριών x_1, y_1 και x_2, y_2 ώστε

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}.$$

Αποδείξτε ότι υπάρχουν x, y ώστε

$$ax \equiv y \pmod{p}, \quad 1 \leq |x| < r, 1 \leq |y| < s.$$