ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Συμπληρωματικές Ασκήσεις
Εαρινό Εξάμηνο 2025

Χρήστος Α. Αθανασιάδης

Συμβολίζουμε με $\mathbb{N}$ το σύνολο $\{0, 1, 2, \dots\}$ των φυσικών αριθμών και με $\mathbb{Z}_{>0}$ εκείνο των θετικών ακεραίων. Συμβολίζουμε με $\lfloor x \rfloor$ το ακέραιο μέρος του πραγματικού αριθμού x και υπενθυμίζουμε ότι η ακολουθία $(F_n)_{n\in\mathbb{N}}$ των αριθμών Fibonacci ορίζεται θέτοντας $F_0 = 0$, $F_1 = 1$ και $F_n = F_{n-1} + F_{n-2}$ για $n \geq 2$.

Διαιρετότητα και πρώτοι αριθμοί

Για ακεραίους a, b γράφουμε $a \mid b$ όταν ο a διαιρεί τον b και συμβολίζουμε με $\mu\kappa\delta(a, b)$ το μέγιστο κοινό τους διαιρέτη (εκτός αν $a = b = 0$).

1. Έστω $a \in \mathbb{Z}_{>0}$.

(α) Δείξτε ότι ο a γράφεται με μοναδικό τρόπο στη μορφή $a = 2^k \cdot q$, όπου $q, k \in \mathbb{N}$ και ο q είναι περιττός αριθμός.
(β) Ποιες είναι οι δυνατές τιμές του $k \in \mathbb{N}$, αν $a = x^2 + xy + y^2$ για κάποια $x, y \in \mathbb{Z}$;
(γ) Για κάθε θετικό ακέραιο n, βρείτε τη μεγαλύτερη δύναμη του 2 που διαιρεί το γινόμενο $(n + 1)(n + 2) \cdots (2n)$.

2. Έστω $a_n = (1 + \sqrt{3})^{2n+1} + (1 - \sqrt{3})^{2n+1}$ για $n \in \mathbb{N}$.

(α) Δείξτε ότι $a_n = 8a_{n-1} - 4a_{n-2}$ για $n \geq 2$.
(β) Για κάθε $n \in \mathbb{N}$, δείξτε ότι $a_n = 2^{n+1} \cdot q_n$ για κάποιο περιττό αριθμό $q_n \in \mathbb{N}$.
(γ) Συνάγετε ότι η μεγαλύτερη δύναμη του 2 που διαιρεί τον ακέραιο $\lfloor (1 + \sqrt{3})^{2n+1} \rfloor$ είναι ίση με 2^{n+1}.

3. Για ποια $a \in \mathbb{Z}$ ισχύει καθεμιά από τις παρακάτω σχέσεις διαιρετότητας;

(α) $a + 1 \mid a^5 + 1$ (β) $a^2 + a + 1 \mid a^4 + a^2 + 1$
(γ) $a^2 + a + 1 \mid a^6 + a^3 + 1$ (δ) $a^3 + a^2 + a + 1 \mid a^6 + a^4 + a^2 + 1$.

4. Θέτουμε $f(x) = x^2 + x + 1$ και $g(x) = x^4 + x^3 + x^2 + x + 1$.

(α) Για ποια $n \in \mathbb{N}$ ισχύει ότι $f(a) \mid f(a^n)$ για κάθε $a \in \mathbb{Z}$;
(β) Για ποια $n \in \mathbb{N}$ ισχύει ότι $g(a) \mid g(a^n)$ για κάθε $a \in \mathbb{Z}$;

Το (α) γενικεύει τα μέρη (β) και (γ) της Άσκησης 3. Δείξτε πρώτα ότι

(γ) $f(a) \mid f(a^{n+3}) - f(a^n)$ για $a \in \mathbb{Z}$ και $n \in \mathbb{N}$,
(δ) $g(a) \mid g(a^{n+5}) - g(a^n)$ για $a \in \mathbb{Z}$ και $n \in \mathbb{N}$.

5. Για $n \in \mathbb{N}$ και $k \in \{0, 1, \ldots, n\}$ ορίζουμε το διωνυμικό συντελεστή

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!},$$

όπου $0! := 1$.

(α) Δείξτε ότι $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ για $1 \le k \le n-1$.
(β) Συνάγετε ότι $\binom{n}{k} \in \mathbb{N}$ για κάθε $k \in \{0, 1, \ldots, n\}$.
(γ) Συνάγετε ότι για κάθε θετικό ακέραιο k, το γινόμενο οποιωνδήποτε k διαδοχικών ακεραίων διαιρείται με το $k!$.
(δ) Δείξτε ότι $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ για $x, y \in \mathbb{C}$.

6. Σε καθεμιά από τις παρακάτω περιπτώσεις αποφανθείτε αν για κάθε $k \in \mathbb{N}$ υπάρχουν θετικοί ακέραιοι a, b, c μεγαλύτεροι του k, τέτοιοι ώστε:

(α) $a \mid b^2 - 1$, $b \mid c^2 - 1$ και $c \mid a^2 - 1$.
(β) $a \mid bc - 1$, $b \mid ac - 1$ και $c \mid ab - 1$.

7. Βρείτε το υπόλοιπο της διαίρεσης του $1^n + 2^n + 3^n + 4^n$ με το 5 για τις διάφορες τιμές του $n \in \mathbb{N}$.

8. Έστω $a, b \in \mathbb{Z}$.

(α) Δείξτε ότι αν $5 \mid a^2 + ab + b^2$, τότε $5 \mid a$ και $5 \mid b$.
(β) Βρείτε όλα τα ζεύγη $(x, y) \in \mathbb{Z}^2$ για τα οποία $x^2 + xy + y^2 = 7500$.
(γ) Βρείτε όλα τα ζεύγη $(x, y) \in \mathbb{Z}^2$ για τα οποία $x^2 + xy + y^2 = 8000$.

9. Τι υπόλοιπα μπορούν να προκύψουν

(α) όταν η τρίτη δύναμη ενός ακεραίου διαιρεθεί με το 9;
(β) όταν η έκτη δύναμη ενός ακεραίου διαιρεθεί με το 27;
(γ) όταν η δέκατη δύναμη ενός ακεραίου διαιρεθεί με το 25;

10. Για ποιους θετικούς ακεραίους m ισχύει καθεμιά από τις συνεπαγωγές

(α) $9 \mid x_1^3 + x_2^3 + \cdots + x_m^3 \Rightarrow 3 \mid x_1 x_2 \cdots x_m$
(β) $27 \mid x_1^6 + x_2^6 + \cdots + x_m^6 \Rightarrow 3 \mid x_1 x_2 \cdots x_m$
(γ) $25 \mid x_1^{10} + x_2^{10} + \cdots + x_m^{10} \Rightarrow 5 \mid x_1 x_2 \cdots x_m$

για $x_1, x_2, \ldots, x_m \in \mathbb{Z}$;

11. Βρείτε το μέγιστο κοινό διαιρέτη:

(α) των ακεραίων της μορφής $mn(m^4 - n^4)$, όπου $m, n \in \mathbb{Z}$,
(β) των ακεραίων της μορφής $m^2n^2(m^6 - n^6)$, όπου $m, n \in \mathbb{Z}$.

12. Δίνονται ακέραιοι $1 \leq k \leq n$.

(α) Δείξτε ότι $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.
(β) Αν $\mu\kappa\delta(n, k) = 1$, δείξτε ότι $n \mid \binom{n}{k}$ και $k \mid \binom{n-1}{k-1}$.

13. Για την ακολουθία $(F_n)_{n\in\mathbb{N}}$ των αριθμών Fibonacci:

(α) Δείξτε ότι $F_{m+n} = F_{m+1}F_n + F_mF_{n-1}$ για $m \in \mathbb{N}$ και $n \in \mathbb{Z}_{>0}$.
(β) Δείξτε ότι $m \mid n \Rightarrow F_m \mid F_n$ για $m, n \in \mathbb{N}$.
(γ) Δείξτε ότι $\mu\kappa\delta(F_m, F_n) = F_{\mu\kappa\delta(m,n)}$ για $m, n \in \mathbb{Z}_{>0}$.
(δ) Συνάγετε ότι $F_m \mid F_n \Rightarrow m \mid n$ για $m, n \in \mathbb{N}$ με $m \neq 2$.

14. Δίνονται ακέραιοι a και b, όχι και οι δύο ίσοι με μηδέν.

(α) Δείξτε ότι $\mu\kappa\delta(a, b) = 1 \Rightarrow \mu\kappa\delta(a + b, a^2 + b^2) \in \{1, 2\}$.
(β) Χρησιμοποιώντας το (α), βρείτε όλα τα ζεύγη $(x, y) \in \mathbb{Z}^2$ για τα οποία το $x^2 + y^2$ διαιρεί το $(x + y)^3$.

15. Γενικεύοντας την Άσκηση 14 (α), δείξτε ότι για $m, n \in \mathbb{Z}_{>0}$ οι ακόλουθες συνθήκες είναι ισοδύναμες:

(i) Υπάρχει $k \in \mathbb{N}$ και περιττοί αριθμοί p, q τέτοιοι ώστε $m = 2^k \cdot p$ και $n = 2^k \cdot q$.
(ii) Υπάρχει $d \in \mathbb{Z}_{>0}$ για τον οποίο οι m/d και n/d είναι περιττοί ακέραιοι.
(iii) Υπάρχουν $a, b \in \mathbb{Z}_{>0}$ με $\mu\kappa\delta(a, b) = 1$ και $\mu\kappa\delta(a^m + b^m, a^n + b^n) \geq 3$.

16. Δείξτε ότι ο $1 + a^2 + a^4 + \cdots + a^{2n}$ είναι σύνθετος αριθμός για όλους τους ακεραίους $a \geq 2$ και $n \geq 2$.

17. Αν p, q είναι διαδοχικοί περιττοί πρώτοι, δείξτε ότι ο $p + q$ μπορεί να γραφεί σαν γινόμενο τουλάχιστον τριών (όχι αναγκαστικά διαφορετικών) πρώτων αριθμών. Για παράδειγμα, $13+17 = 2\cdot3\cdot5$, $17+19 = 2\cdot2\cdot3\cdot3$ και $19 + 23 = 2 \cdot 3 \cdot 7$.

18. Για ποιους πρώτους αριθμούς p

(α) ο αριθμός $2^p + p^2$ είναι επίσης πρώτος;
(β) ο αριθμός $4^p + p^4$ είναι επίσης πρώτος;

19. Δίνονται διακεκριμένοι πρώτοι $p_1, p_2, \ldots, p_n$. Δείξτε ότι

$$\frac{1}{p_1^m} + \frac{1}{p_2^m} + \cdots + \frac{1}{p_n^m} \notin \mathbb{Z}$$

για κάθε θετικό ακέραιο m.

20. Δίνεται περιττός θετικός ακέραιος m.

(α) Αν p είναι περιττός πρώτος και

$$\frac{1}{1^m} + \frac{1}{2^m} + \frac{1}{3^m} + \cdots + \frac{1}{(p-1)^m} = \frac{a}{b}$$

για κάποια $a, b \in \mathbb{Z}$, δείξτε ότι $p \mid a$.

(β) Αν $n \geq 2$ είναι ακέραιος και

$$\frac{1}{1^m} + \frac{1}{3^m} + \frac{1}{5^m} + \cdots + \frac{1}{(2^n-1)^m} = \frac{a}{b}$$

για κάποια $a, b \in \mathbb{Z}$, δείξτε ότι $2^n \mid a$.

21. Δίνεται πρώτος αριθμός p.

(α) Δείξτε ότι $p \mid \binom{p}{k}$ για κάθε $k \in \{1, 2, \ldots, p-1\}$.

(β) Δείξτε ότι $p^2 \mid \binom{np}{p} - n$ για κάθε $n \in \mathbb{Z}_{>0}$.

(γ) Γενικότερα, δείξτε ότι $p^2 \mid \binom{pa}{pb} - \binom{a}{b}$ για ακεραίους $0 \leq b \leq a$.

22. Έστω $p \in \mathbb{Z}_{>0}$.

(α) Αν ο p είναι περιττός αριθμός, δείξτε ότι

$$\lfloor (\sqrt{5}+2)^p \rfloor = (\sqrt{5}+2)^p - (\sqrt{5}-2)^p = 2 \cdot \sum_{k=0}^{\lfloor p/2 \rfloor} \binom{p}{2k} 5^k 2^{p-2k}.$$

(β) Συνάγετε ότι $p \mid \lfloor (\sqrt{5}+2)^p \rfloor - 2^{p+1}$ για κάθε περιττό πρώτο p.

23. Δείξτε ότι δεν υπάρχουν $m, n \in \mathbb{N}$ για τους οποίους το $2018^m + 3$ διαιρεί το 1885^n.

24. Βρείτε όλους τους θετικούς ακεραίους m που έχουν την ιδιότητα $m \mid n^3 \Rightarrow m \mid n^2$ για $n \in \mathbb{Z}$.

25. Ποιες από τις ακόλουθες προτάσεις είναι σωστές;

(α) Αν m, n, k είναι θετικοί ακέραιοι με $m \leq n$ και $m \mid n^k$, τότε $m^m \mid n^n$.

(β) Αν m, n, k είναι θετικοί ακέραιοι με $m \leq n$ και $m \mid n^k$, τότε $m^{m^m} \mid n^{n^n}$.

26. Δίνεται σύνολο S με στοιχεία $n \geq 2$ θετικούς ακεραίους που έχουν μέγιστο κοινό διαιρέτη ίσο με 1.

(α) Αν το γινόμενο οποιωνδήποτε δύο στοιχείων του S είναι ίσο με το τετράγωνο ενός ακεραίου, δείξτε ότι το ίδιο ισχύει για καθένα από τα στοιχεία του S.

(β) Γενικότερα, έστω ακέραιος $1 \leq k < n$. Αν το γινόμενο οποιωνδήποτε k στοιχείων του S είναι ίσο με το τετράγωνο ενός ακεραίου, δείξτε ότι το ίδιο ισχύει για καθένα από τα στοιχεία του S.

27. Δίνονται θετικοί ακέραιοι n, a, k. Αν ο n διαιρεί το $(a-1)^k$, δείξτε ότι ο n διαιρεί και το $1 + a + a^2 + \cdots + a^{n-1}$.

28. Δίνεται θετικός ακέραιος k.

(α) Θεωρούμε την ακολουθία $(a_n)_{n\in\mathbb{N}}$ που ορίζεται θέτοντας $a_0 = a_1 = 1$ και $a_{n+1} = (a_n^k + 1)/a_{n-1}$ για $n \geq 1$. Δείξτε ότι $a_n \in \mathbb{N}$ για κάθε $n \in \mathbb{N}$.

(β) Συνάγετε ότι για κάθε ακέραιο $k \geq 2$ υπάρχουν άπειρα ζεύγη θετικών ακεραίων (x, y), τέτοια ώστε $x \mid (y^k + 1)$ και $y \mid (x^k + 1)$.

Διοφαντικές εξισώσεις

29. Δίνονται θετικοί ακέραιοι a, b με $\mu\kappa\delta(a, b) = 1$ και η απεικόνιση $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ με $f(x, y) = ax + by$ για $x, y \in \mathbb{Z}$.

(α) Δείξτε ότι αν $f(x, y) = f(u, v)$, τότε $b \mid x - u$ και $a \mid y - v$.

(β) Δείξτε ότι υπάρχουν ακριβώς ab τιμές του $c \in \mathbb{N}$ για τις οποίες η εξίσωση $f(x, y) = c$ έχει μοναδική λύση $(x, y) \in \mathbb{N} \times \mathbb{N}$ και ότι η μέγιστη τιμή με αυτή την ιδιότητα είναι η $c = 2ab - a - b$.

30. Δίνεται θετικός ακέραιος n.

(α) Δείξτε ότι το πλήθος των λύσεων $(x, y) \in \mathbb{Z}^2$ της εξίσωσης $x^2+y^2 = n$ είναι ακέραιο πολλαπλάσιο του 4.

(β) Δείξτε ότι το πλήθος των λύσεων $(x, y) \in \mathbb{Z}^2$ της εξίσωσης $x^2+y^2 = n$ είναι ίσο με εκείνο της $x^2 + y^2 = 2n$.

(γ) Δείξτε ότι το πλήθος των λύσεων $(x, y) \in \mathbb{Z}^2$ της εξίσωσης $x^2 + xy + y^2 = n$ είναι ακέραιο πολλαπλάσιο του 6.

31. Βρείτε όλα τα ζεύγη $(x, y) \in \mathbb{Z}^2$ για τα οποία $x^5 + x^3 = y^2$.

32. Βρείτε όλα τα $n \in \mathbb{N}$ για τα οποία η εξίσωση

$$\binom{x}{n} + \binom{y}{n} = \binom{z}{n}$$

έχει ακέραια λύση $(x, y, z) \in \mathbb{Z}^3$ με $x \geq n$, $y \geq n$ και $z \geq n$.

33. Δίνεται πρώτος αριθμός p. Θεωρούμε τις λύσεις $(x, y, z) \in \mathbb{Z}^3$ της Διοφαντικής εξίσωσης $p(x + y + z) = xyz$ με $1 \leq x \leq y \leq z$.

(α) Βρείτε την ελάχιστη τιμή του z.
(β) Βρείτε τη μέγιστη τιμή του z.
(γ) Βρείτε όλες τις λύσεις $1 \leq x \leq y \leq z$ για $p = 3$.

34. Θεωρούμε τη Διοφαντική εξίσωση $x^2 + y^2 + z^2 = 2xyz + 2$.

(α) Αν (x, y, z) είναι λύση, δείξτε ότι το ίδιο ισχύει για την τριάδα $(x, y, 2xy - z)$.
(β) Βρείτε μια λύση $(x, y, z) \in \mathbb{Z}^3$ με x, y, z μεγαλύτερα του 10.

35. Θεωρούμε τη Διοφαντική εξίσωση $x^2 + y^2 + z^2 = 2\,(xy + yz + zx)$.

(α) Βρείτε όλες τις λύσεις $(x, y, z) \in \mathbb{Z}^3$ της εξίσωσης.
(β) Συνάγετε ότι για κάθε λύση (x, y, z) με $\mu\kappa\delta(x, y, z) = 1$, η απόλυτος τιμή καθενός από τα x, y, z είναι ίση με το τεράγωνο ενός ακεραίου.

Ισοτιμίες και Θεωρήματα Euler και Wilson

36. Σε καθεμιά από τις ακόλουθες περιπτώσεις, βρείτε όλους τους ακεραίους $m \geq 2$ για τους οποίους ισχύει η συνεπαγωγή για $a, b \in \mathbb{Z}$:

(α) $a^2 \equiv 0 \pmod{m} \Rightarrow a \equiv 0 \pmod{m}$.
(β) $a^2 \equiv b^2 \pmod{m} \Rightarrow a \equiv \pm b \pmod{m}$.

37. Βρείτε τον μικρότερο μη αρνητικό ακέραιο της μορφής $23^m - 3^m - 5^n$, όπου $m, n \in \mathbb{N}$.

38. Βρείτε όλα τα ζεύγη $(m, n) \in \mathbb{N}^2$ για τα οποία $3^m \cdot 5^{m+1} - 2^n = 1$.

39. Δείξτε ότι υπάρχουν άπειροι φυσικοί αριθμοί οι οποίοι δεν μπορούν να γραφούν στη μορφή $x^3 + y^4$ με $x, y \in \mathbb{Z}$.

40. Δείξτε ότι

$$3^{2^n} + 3^{2^{n+1}} \equiv -1 \pmod{13}$$

για κάθε $n \in \mathbb{N}$. Για ποια $k \in \mathbb{Z}_{>0}$ το άθροισμα $3^{2^n} + 3^{2^{n+1}} + \cdots + 3^{2^{n+k-1}}$ διαιρείται με το 13 για κάθε $n \in \mathbb{N}$;

41. Δίνονται ακέραιοι a και $m \geq 1$. Αν $a \equiv 1 \pmod{m}$, δείξτε ότι $a^{m^{n-1}} \equiv 1 \pmod{m^n}$ για κάθε θετικό ακέραιο n.

42. Για την ακολουθία $(F_n)_{n\in\mathbb{N}}$ των αριθμών Fibonacci και για κάθε $m \in \mathbb{Z}_{>0}$:

(α) Δείξτε ότι τουλάχιστον ένας από τους $F_1, F_2, \ldots, F_{m^2}$ διαιρείται με το m.

(β) Δείξτε ότι υπάρχει $r \in \{1, 2, \ldots, m^2\}$ για το οποίο ισχύει $F_{r+n} \equiv F_n \pmod{m}$ για κάθε $n \in \mathbb{Z}_{>0}$.

43. Έστω $a \in \mathbb{Z}$.

(α) Βρείτε τα δυνατά υπόλοιπα της διαίρεσης του $a^2 + a + 1$ με το 5.
(β) Βρείτε όλες τις ακέραιες λύσεις της εξίσωσης $x^2 + x + y = y^5 - 1$.

44. Δίνονται ακέραιοι a και $n \geq 1$. Δείξτε ότι υπάρχει θετικός ακέραιος k τέτοιος ώστε $a^k \equiv -1 \pmod{2^n}$ αν και μόνο αν $a \equiv -1 \pmod{2^n}$.

45. Δίνεται ακέραιος $n \geq 2$.

(α) Για $x, y \in \mathbb{Z}$, δείξτε ότι $x \equiv y \pmod{n} \Rightarrow x^n \equiv y^n \pmod{n^2}$.
(β) Δείξτε ότι υπάρχει $r \in \{0, 1, \ldots, n^2 - 1\}$ τέτοιο ώστε $x^n + y^n \not\equiv r \pmod{n^2}$ για όλα τα $x, y \in \mathbb{Z}$.

46. Για $n \in \mathbb{Z}$ δείξτε ότι:

(α) $2^7 - 2^3 \mid n^7 - n^3$.
(β) $2^{15} - 2^3 \mid n^{15} - n^3$.

47. Δίνεται περιττός πρώτος p.

(α) Δείξτε ότι ο αριθμός $(p-1) \cdot 2^{p(p-1)} + 1$ διαιρείται με το p.
(β) Δείξτε ότι ο αριθμός $(p-1) \cdot 2^{p(p-1)} + 1$ δεν είναι ίσος με το τετράγωνο ενός ακεραίου αριθμού.

48. Δίνεται $a \in \mathbb{Z}_{>0}$. Βρείτε όλους τους θετικούς ακεραίους που διαιρούν τουλάχιστον έναν από τους αριθμούς $1, 1+a, 1+a+a^2, 1+a+a^2+a^3, \ldots$

49. Δίνεται πρώτος αριθμός $p \neq 3$ και ο ακέραιος $n = \dfrac{4^p - 1}{3}$. Δείξτε ότι $n \mid 2^n - 2$.

50. Σε καθεμιά από τις παρακάτω περιπτώσεις βρείτε αν υπάρχει περιττός πρώτος p με τη δοσμένη ιδιότητα:

(α) $2^{p-1} \equiv 1 \pmod{p^2}$.
(β) $a^{p-1} \equiv 1 \pmod{p^2}$ για κάθε $a \in \{1, 2, \ldots, p-1\}$.

51. Για κάθε θετικό ακέραιο n, δείξτε ότι:

(α) Υπάρχει $k \in \mathbb{N}$, τέτοιο ώστε $2^k \equiv -1 \pmod{3^n}$.
(β) Υπάρχει $k \in \mathbb{N}$, τέτοιο ώστε $2^k \equiv -1 \pmod{5^n}$.
(γ) Δεν υπάρχει $k \in \mathbb{N}$, τέτοιο ώστε $2^k \equiv -1 \pmod{7^n}$.

52. Βρείτε όλους τους περιττούς πρώτους p για τους οποίους ο $\dfrac{2^{p-1}-1}{p}$ είναι ίσος με το τετράγωνο ενός ακεραίου.

53. Δίνονται θετικοί ακέραιοι x, y, n με $\mu\kappa\delta(x, y) = 1$.

(α) Δείξτε ότι κάθε περιττός διαιρέτης του $x^2 + y^2$ είναι ισότιμος με 1 (mod 4).
(β) Δείξτε, γενικότερα, ότι κάθε περιττός διαιρέτης του $x^{2^n} + y^{2^n}$ είναι ισότιμος με 1 (mod 2^{n+1}).

54. Ποιες από τις παρακάτω προτάσεις είναι σωστές;

(α) Αν ο αριθμός a ισούται με το άθροισμα των τετραγώνων δύο ακεραίων αριθμών, τότε $a \equiv 2^n \pmod{2^{n+2}}$ για κάποιο $n \in \mathbb{N}$.
(β) Αν $a \equiv 2^n \pmod{2^{n+2}}$ για κάποια $a, n \in \mathbb{N}$, τότε ο a ισούται με το άθροισμα των τετραγώνων δύο ακεραίων αριθμών.

55. Δίνεται πρώτος αριθμός $p \equiv 2 \pmod 3$. Γενικεύοντας την Άσκηση 8 (α), δείξτε ότι αν $p \mid (a^2 + ab + b^2)$ για κάποια $a, b \in \mathbb{Z}$, τότε $p \mid a$ και $p \mid b$.

56. Σε καθεμιά από τις παρακάτω περιπτώσεις, δείξτε ότι δεν υπάρχουν θετικοί ακέραιοι a, b τέτοιοι ώστε:

(α) ο αριθμός $4ab - a - 1$ ισούται με το τετράγωνο ενός ακεραίου,
(β) ο αριθμός $3ab - a - 1$ ισούται με το γινόμενο δύο διαδοχικών ακεραίων.

57. Δείξτε ότι:

(α) Μεταξύ πέντε τυχαίων διαδοχικών ακεραίων είναι δυνατόν να επιλεγεί ένας, ο οποίος είναι σχετικά πρώτος προς καθέναν από τους άλλους τέσσερις.
(β) Μεταξύ δέκα τυχαίων διαδοχικών ακεραίων είναι δυνατόν να επιλεγεί ένας, ο οποίος είναι σχετικά πρώτος προς καθέναν από τους άλλους εννέα.
(γ) Ισχύει το ίδιο για είκοσι τυχαίους διαδοχικούς ακεραίους;

58. Βρείτε όλους τους θετικούς ακεραίους n:

(α) για τους οποίους $n \mid (n-1)!$,
(β) για τους οποίους το ακέραιο μέρος $\lfloor \dfrac{(n-1)!}{n} \rfloor$ είναι άρτιος αριθμός,
(γ) για τους οποίους το $(n-1)! + 1$ είναι δύναμη του n.

59. Δίνεται πρώτος αριθμός p.

(α) Δείξτε ότι

$$k!\,(p-k-1)! \;\equiv\; (-1)^{k-1} \pmod{p}$$

για κάθε $k \in \{0, 1, \ldots, p-1\}$.

(β) Δείξτε ότι

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

για κάθε $k \in \{0, 1, \ldots, p-1\}$.

60. Δίνεται πρώτος αριθμός p. Δείξτε ότι $p \mid \binom{p^m}{k}$ για κάθε θετικό ακέραιο m και κάθε $k \in \{1, 2, \ldots, p^m - 1\}$ ως εξής. Για πολυώνυμα $f(x), g(x) \in \mathbb{Z}[x]$ θα γράφουμε $f(x) \equiv_p g(x)$ αν όλοι οι συντελεστές του $f(x) - g(x)$ διαιρούνται με το p.

(α) Δείξτε ότι η $\equiv_p$ είναι σχέση ισοδυναμίας στο $\mathbb{Z}[x]$.

(β) Αν $f(x) \equiv_p g(x)$ και $s(x) \equiv_p t(x)$, δείξτε ότι $f(x)+s(x) \equiv_p g(x)+t(x)$ και ότι $f(x)s(x) \equiv_p g(x)t(x)$. Εδικότερα, $(f(x))^n \equiv_p (g(x))^n$ για κάθε $n \in \mathbb{Z}_{>0}$.

(γ) Δείξτε ότι

$$(f(x) + g(x))^p \;\equiv_p\; (f(x))^p + (g(x))^p$$

για όλα τα $f(x), g(x) \in \mathbb{Z}[x]$.

(δ) Δείξτε ότι $(x+1)^{p^m} \equiv_p x^{p^m} + 1$ για κάθε $m \in \mathbb{Z}_{>0}$ και συνάγετε ότι $p \mid \binom{p^m}{k}$ για κάθε $k \in \{1, 2, \ldots, p^m - 1\}$.

Αριθμητικές συναρτήσεις

Συμβολίζουμε με $d(n)$ το πλήθος των θετικών διαιρετών του n και με $\mu : \mathbb{Z}_{>0} \to \mathbb{Z}$ και $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}$ τις συναρτήσεις των Möbius και Euler, αντίστοιχα.

61. Δίνεται πολλαπλασιαστική αριθμητική συνάρτηση $f : \mathbb{Z}_{>0} \to \mathbb{C}$. Δείξτε ότι

$$f(m)f(n) \;=\; f(d)f(D)$$

για $m, n \in \mathbb{Z}_{>0}$, όπου $d = \mu\kappa\delta(m, n)$ και $D = \varepsilon\kappa\pi(m, n)$.

62. Δίνονται πολλαπλασιαστικές αριθμητικές συναρτήσεις $f, g : \mathbb{Z}_{>0} \to \mathbb{C}$. Δείξτε ότι η αριθμητική συνάρτηση $h : \mathbb{Z}_{>0} \to \mathbb{C}$ που ορίζεται θέτοντας

$$h(n) \;=\; \sum_{k|n} f(k)g\Big(\frac{n}{k}\Big)$$

για $n \in \mathbb{Z}_{>0}$ είναι επίσης πολλαπλασιαστική συνάρτηση.

63. Έστω $n \in \mathbb{Z}_{>0}$.

(α) Δείξτε ότι $d(n) < 2\sqrt{n}$.
(β) Για ποιούς θετικούς ακεραίους n ισχύει ότι $d(2n) = n$;

64. Για $\alpha \in \mathbb{C}$ ορίζουμε την αριθμητική συνάρτηση $\sigma_\alpha : \mathbb{Z}_{>0} \to \mathbb{C}$ θέτοντας

$$\sigma_\alpha(n) \;=\; \sum_{k|n} k^\alpha$$

για $n \in \mathbb{Z}_{>0}$.

(α) Δείξτε ότι η σ_α είναι πολλαπλασιαστική συνάρτηση.
(β) Δείξτε ότι $\sigma_{-\alpha}(n) = \sigma_\alpha(n)/n^\alpha$ για κάθε $n \in \mathbb{Z}_{>0}$.
(γ) Υπολογίστε το άθροισμα $\displaystyle\sum_{k|n} \mu(k)\sigma_\alpha(k)$ για $n \in \mathbb{Z}_{>0}$.
(δ) Δείξτε ότι

$$\sum_{k|n} \varphi(k)\sigma_\alpha\!\left(\frac{n}{k}\right) \;=\; n\sigma_{\alpha-1}(n)$$

για κάθε $n \in \mathbb{Z}_{>0}$. Ποιες ταυτότητες προκύπτουν για $\alpha \in \{0, 1\}$;

65. Για $\alpha \geq 0$ θεωρούμε τη συνάρτηση $\sigma_\alpha : \mathbb{Z}_{>0} \to \mathbb{R}$ της Άσκησης 64.

(α) Δείξτε ότι $\sigma_\alpha(n) \geq d(n) \geq n/\varphi(n) \geq 1$ για κάθε $n \in \mathbb{Z}_{>0}$. Για ποιους θετικούς ακεραίους ισχύουν οι αντίστοιχες ισότητες;
(β) Αν $\alpha \geq 1$, δείξτε ότι

$$n^\alpha \;\leq\; \sigma_\alpha(n) \;\leq\; \frac{n^{\alpha+1}}{\varphi(n)}$$

για κάθε $n \in \mathbb{Z}_{>0}$. Για ποιους θετικούς ακεραίους ισχύουν οι αντίστοιχες ισότητες;

66. Βρείτε όλους τους θετικούς ακεραίους n για τους οποίους το $\varphi(n!)$ είναι ίσο με:

(α) μια δύναμη του 2,
(β) το γινόμενο μιας δύναμης του 2 επί μιας δύναμης του 3.

67. Δίνονται $\alpha, \beta \in \mathbb{C}$, ακέραιος $p \geq 2$ και η αριθμητική συνάρτηση $\varepsilon_p : \mathbb{Z}_{>0} \to \mathbb{C}$ με

$$\varepsilon_p(n) \;=\; \begin{cases} \alpha, & \text{αν } p \mid n, \\ \beta, & \text{διαφορετικά.} \end{cases}$$

Υπολογίστε το άθροισμα

$$\sum_{k|n} \varepsilon_p(k)\mu\!\left(\frac{n}{k}\right).$$

Υπόδειξη: Εφαρμόστε το Θεώρημα αντιστροφής του Möbius.

68. Συμβολίζουμε με $\psi(n)$ το πλήθος των ζευγών $(a, b) \in [n] \times [n]$ με $\mu\kappa\delta(a, b) = 1$.

(α) Δείξτε ότι $\psi(n) = \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2$ για κάθε $n \in \mathbb{Z}_{>0}$.

(β) Υπολογίστε το όριο $\lim_{n\to\infty} \frac{\psi(n)}{n^2}$.

69. Δίνεται πολλαπλασιαστική αριθμητική συνάρτηση $f : \mathbb{Z}_{>0} \to \mathbb{C}$.

(α) Δείξτε ότι $f(2^{2^n} - 1) = \prod_{k=0}^{n-1} f(2^{2^k} + 1)$ για κάθε $n \in \mathbb{Z}_{>0}$.

(β) Για ποιούς θετικούς ακεραίους n ισχύει ότι $\varphi(2^{2^n} - 1) = 2^{2^n - 1}$;

Πολυωνυμικές ισοτιμίες, τάξη και πρωταρχικές ρίζες

70. Λύστε την ισοτιμία

$$x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 1 \equiv 0 \pmod{19}.$$

Υπόδειξη: Παραγοντοποιήστε το αριστερό μέλος ως πολυώνυμο με ακέραιους συντελεστές.

71. Έστω πρώτος αριθμός p.

(α) Δείξτε ότι η ισοτιμία $x^2 + 1 \equiv 0 \pmod{p}$ έχει λύση αν και μόνο αν $p = 2$ ή $p \equiv 1 \pmod 4$.

(β) Δείξτε ότι η ισοτιμία $x^2 + x + 1 \equiv 0 \pmod{p}$ έχει λύση αν και μόνο αν $p = 3$ ή $p \equiv 1 \pmod 6$.

72. Δείξτε ότι για πρώτο αριθμό p και θετικό ακέραιο d, οι ακόλουθες συνθήκες είναι ισοδύναμες:

(i) Η ισοτιμία $x^d \equiv a \pmod{p}$ έχει λύση για κάθε $a \in \mathbb{Z}$.
(ii) $x^d \equiv y^d \pmod{p} \Rightarrow x \equiv y \pmod{p}$ για $x, y \in \mathbb{Z}$.
(iii) $x^d \equiv 1 \pmod{p} \Rightarrow x \equiv 1 \pmod{p}$ για $x \in \mathbb{Z}$.
(iv) $\mu\kappa\delta(p - 1, d) = 1$.

73. Δίνονται πρώτοι αριθμοί p, q, θετικός ακέραιος d και $x, y \in \mathbb{Z}$.

(α) Δείξτε ότι αν $p \mid (1 + x + x^2 + \cdots + x^{d-1})$, τότε $p \mid d$ ή $\mu\kappa\delta(p-1, d) > 1$.

(β) Γενικεύοντας την Άσκηση 55, δείξτε ότι αν $\mu\kappa\delta(p - 1, d) = \mu\kappa\delta(p, d) = 1$, τότε

$$p \mid (x^d - y^d)/(x - y) \;\Rightarrow\; p \mid x,\; p \mid y.$$

(γ) Δείξτε ότι υπάρχουν άπειροι πρώτοι αριθμοί ισότιμοι με $1 \pmod q$.

74. Θεωρούμε την ισοτιμία $x^2 \equiv d \pmod{p^n}$, όπου p είναι περιττός πρώτος και d είναι ακέραιος που δε διαιρείται με το p.

(α) Δείξτε ότι η ισοτιμία έχει μηδέν ή ακριβώς δύο λύσεις $\pmod{p^n}$.

(β) Δείξτε ότι το πλήθος των λύσεων (mod p^n) είναι ανεξάρτητο του n.
(γ) Πόσες λύσεις έχει η ισοτίμία $x^2 \equiv -1 \pmod{125}$; Ποιες είναι αυτές;

75. Για τις διάφορες τιμές των θετικών ακεραίων n και k, βρείτε όλες τις λύσεις των ισοτιμιών:

(α) $x^k \equiv -1 \pmod{2^n}$ (β) $x^3 \equiv -1 \pmod{3^n}$ (γ) $x^{15} \equiv 1 \pmod{6^n}$.

76. Λύστε την ισοτιμία

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{29}.$$

Υπόδειξη: Βρείτε πρώτα μια πρωταρχική ρίζα (mod 29).

77. Για κάθε πρώτο αριθμό p και κάθε $n \in \mathbb{N}$, γενικεύοντας την Άσκηση 7, δείξτε ότι το $1^n + 2^n + \cdots + (p-1)^n$ διαιρείται με το p αν και μόνο αν το n δεν είναι πολλαπλάσιο του $p - 1$.

78. Σε καθεμιά από τις παρακάτω περιπτώσεις, βρείτε όλους τους ακεραίους $m \geq 2$ για τους οποίους:

(α) Υπάρχει $n \in \mathbb{Z}_{>0}$ και πρωταρχική ρίζα (mod m^n) ισότιμη με 1 (mod m).
(β) Υπάρχει $n \in \mathbb{Z}_{>0}$ και πρωταρχική ρίζα (mod m^n) ισότιμη με -1 (mod m).

79. Δίνεται περιττός πρώτος p, ακέραιος a που δε διαιρείται με το p και $n \in \mathbb{Z}_{>0}$.

(α) Δείξτε ότι υπάρχει $k \in \mathbb{N}$ με $a^k \equiv -1 \pmod{p^n}$ αν και μόνο αν η τάξη της κλάσης a (mod p) είναι άρτιος αριθμός (γενικεύοντας έτσι την Άσκηση 51).
(β) Συνάγετε ότι αν ο a είναι πρωταρχική ρίζα (mod p), τότε υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $a^k \equiv -1 \pmod{p^n}$.
(γ) Ισχύει το αντίστροφο της πρότασης στο (β);

80. Έστω ότι για τον ακέραιο $m \geq 2$ δεν υπάρχει πρωταρχική ρίζα (mod m). Δείξτε ότι $a^{\varphi(m)/2} \equiv 1 \pmod{m}$ για κάθε ακέραιο a σχετικώς πρώτο προς τον m.

81. Βρείτε όλα τα ζεύγη $(m, n) \in \mathbb{N}^2$ για τα οποία $(2m^2 + 1)3^m - 2^n = 1$.
Υπόδειξη: Δείξτε πρώτα ότι το 2 είναι πρωταρχική ρίζα (mod 3^m) για κάθε θετικό ακέραιο m.

Τετραγωνικά υπόλοιπα και νόμος αντιστροφής

Υπενθυμίζουμε ότι ένας ακέραιος a σχετικώς πρώτος προς τον m λέγεται τετραγωνικό υπόλοιπο (mod m) αν $a \equiv x^2 \pmod m$ για κάποιο $x \in \mathbb{Z}$ και τετραγωνικό μη υπόλοιπο (mod m) αν $a \not\equiv x^2 \pmod m$ για κάθε $x \in \mathbb{Z}$. Γράφουμε

$$\left(\frac{a}{m}\right) = \begin{cases} 1, & \text{αν ο } a \text{ είναι τετραγωνικό υπόλοιπο (mod } m), \\ -1, & \text{αν ο } a \text{ είναι τετραγωνικό μη υπόλοιπο (mod } m). \end{cases}$$

82. Δίνεται ακέραιος $m \geq 2$.

(α) Δείξτε ότι υπάρχουν το πολύ $\lfloor m/2 \rfloor + 1$ κλάσεις $x^2 \pmod m$ για $x \in \mathbb{Z}$.
(β) Για ποια m υπάρχουν ακριβώς $\lfloor m/2 \rfloor + 1$ τέτοιες κλάσεις (mod m);

83. Δίνεται ακέραιος $m \geq 3$.

(α) Δείξτε ότι $a^{\varphi(m)/2} \equiv 1 \pmod m$ για κάθε τετραγωνικό υπόλοιπο a (mod m).
(β) Δείξτε ότι ισχύει το αντίστροφο, δηλαδή κάθε ακέραιος a με $a^{\varphi(m)/2} \equiv 1 \pmod m$ είναι τετραγωνικό υπόλοιπο (mod m), αν και μόνο αν υπάρχει πρωταρχική ρίζα (mod m).

84. Θεωρούμε ακέραιο $m \geq 2$.

(α) Δείξτε ότι η συνεπαγωγή

$$a^2 \equiv b^2 \pmod m \;\Rightarrow\; a \equiv \pm b \pmod m$$

ισχύει για ακεραίους a, b σχετικώς πρώτους προς τον m αν και μόνο αν υπάρχει πρωταρχική ρίζα (mod m).
(β) Αν $m \geq 3$, δείξτε ότι υπάρχουν το πολύ $\varphi(m)/2$ τετραγωνικά υπόλοιπα (mod m).
(γ) Για ποια $m \geq 3$ υπάρχουν ακριβώς $\varphi(m)/2$ τετραγωνικά υπόλοιπα (mod m);

85. Δίνεται ακέραιος $m \geq 3$.

(α) Δείξτε ότι κάθε πρωταρχική ρίζα (mod m) είναι τετραγωνικό μη υπόλοιπο (mod m).
(β) Βρείτε όλα τα m για τα οποία, αντιστρόφως, κάθε τετραγωνικό μη υπόλοιπο (mod m) είναι πρωταρχική ρίζα (mod m).

86. Δίνεται περιττός πρώτος p. Για ποια $(a, b) \in \mathbb{Z}^2$ η ισοτιμία $ax^2 + by^2 \equiv c \pmod p$ έχει λύση για κάθε $c \in \mathbb{Z}$;

87. Δίνεται πρώτος αριθμός $p \equiv 3 \pmod 4$.

(α) Λύστε την ισοτιμία $x^4 \equiv 1 \pmod{p}$.
(β) Δείξτε ότι η ισοτιμία $x^4 \equiv c \pmod{p}$ έχει λύση για ακριβώς $(p+1)/2$ κλάσεις $c \pmod{p}$.
(γ) Για ποια $(a, b) \in \mathbb{Z}^2$ η ισοτιμία $ax^4 + by^4 \equiv c \pmod{p}$ έχει λύση για κάθε $c \in \mathbb{Z}$;

88. Δίνεται περιττός πρώτος p.

(α) Βρείτε το υπόλοιπο της διαίρεσης του γινομένου των τετραγωνικών υπολοίπων (mod p) με το p.
(β) Βρείτε το υπόλοιπο της διαίρεσης του γινομένου των τετραγωνικών μη υπολοίπων (mod p) με το p.

89. Βρείτε όλους τους πρώτους p για τους οποίους η ισοτιμία

$$x(x+1)(x+2)(x+3) \equiv -1 \pmod{p}$$

έχει λύση.

90. Δίνεται περιττός πρώτος p.

(α) Δείξτε ότι $\displaystyle\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$.
(β) Δείξτε ότι

$$\sum_{k=1}^{p-1} k\left(\frac{k}{p}\right) \equiv \begin{cases} 2 \pmod{p}, & \text{αν } p = 3, \\ 0 \pmod{p}, & \text{αν } p \neq 3. \end{cases}$$

(γ) Αν $p \equiv 3 \pmod 4$ και $p \neq 3$, δείξτε ότι $\displaystyle\sum_{k=1}^{p-1} k^2\left(\frac{k}{p}\right) \equiv 0 \pmod{p^2}$.

91. Για την ακολουθία $(F_n)_{n\in\mathbb{N}}$ των αριθμών Fibonacci:

(α) Δείξτε ότι $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ για κάθε θετικό ακέραιο n.
(β) Δείξτε ότι $p \mid F_{p-1}F_{p+1}$ για κάθε πρώτο $p \neq 5$.
(γ) Έστω πρώτος αριθμός p. Δείξτε ότι $p \mid F_{p-1}$ αν και μόνο αν $p \equiv \pm 1 \pmod 5$.

Διάφορα προβλήματα

92. Έστω ακέραιος $n \geq 2$. Δείξτε ότι το άθροισμα των ρητών αριθμών της μορφής $1/pq$, όπου $p, q \in \{1, 2, \ldots, n\}$ είναι σχετικώς πρώτοι αριθμοί με άθροισμα $p + q > n$, είναι ίσο με $1/2$. Για παράδειγμα, έχουμε

$$\frac{1}{1\cdot 5} + \frac{1}{2\cdot 5} + \frac{1}{3\cdot 5} + \frac{1}{4\cdot 5} + \frac{1}{3\cdot 4} = \frac{1}{2}$$

για $n = 5$.

93. Έστω $a, b \in \mathbb{N}$. Αν ο αριθμός $(a^2+b^2)/(ab+1)$ είναι ακέραιος, δείξτε ότι ο αριθμός αυτός είναι ίσος με το τετράγωνο ενός ακεραίου αριθμού.

94. Δίνονται θετικοί ακεραίοι $m < n$.

(α) Δείξτε ότι ο ρητός αριθμός

$$\frac{1}{m+1} + \frac{1}{m+2} + \cdots + \frac{1}{n}$$

δεν είναι ακέραιος.

(β) Δείξτε, γενικότερα, ότι ο ρητός αριθμός

$$\frac{1}{am+r} + \frac{1}{a(m+1)+r} + \cdots + \frac{1}{an+r}$$

δεν είναι ακέραιος για κάθε περιττό $a \in \mathbb{Z}_{>0}$ και κάθε $r \in \{0, 1, \ldots, a-1\}$.

95. Έστω πρώτος αριθμός p.

(α) Δείξτε ότι ο p μπορεί να γραφεί στη μορφή $p = x^2 + y^2$ για κάποιους ακεραίους x, y αν και μόνο αν $p = 2$ ή $p \equiv 1 \pmod 4$.

(β) Δείξτε ότι ο p μπορεί να γραφεί στη μορφή $p = x^2 + xy + y^2$ για κάποιους ακεραίους x, y αν και μόνο αν $p = 3$ ή $p \equiv 1 \pmod 6$.

96. Για κάθε $k \in \mathbb{N}$ συμβολίζουμε με $\mathcal{M}_k$ το σύνολο των θετικών ακεραίων της μορφής $a^2 + kab + b^2$, όπου $a, b \in \mathbb{Z}$.

(α) Δείξτε ότι $x, y \in \mathcal{M}_k \Rightarrow xy \in \mathcal{M}_k$.

(β) Αντιστρόφως, έστω ότι $k \in \{0, 1\}$ και ότι $u = a^2 + kab + b^2 \in \mathcal{M}_k$, όπου οι a, b είναι σχετικώς πρώτοι. Δείξτε ότι κάθε θετικός διαιρέτης του u ανήκει στο $\mathcal{M}_k$.

(γ) Ισχύει η πρόταση στο (β) για κάθε $k \in \{3, 4, \ldots\}$;

97. Δίνεται πολυώνυμο $p(x)$ με πραγματικούς συντελεστές.

(α) Δείξτε ότι το $p(x)$ έχει την ιδιότητα $x \in \mathbb{Z} \Rightarrow p(x) \in \mathbb{Z}$ (δηλαδή λαμβάνει ακέραιες τιμές για όλες τις ακέραιες τιμές του x) αν και μόνο αν

$$p(x) = c_0 + c_1\binom{x}{1} + c_2\binom{x}{2} + \cdots + c_n\binom{x}{n}$$

για κάποια $n \in \mathbb{N}$ και $c_0, c_1, \ldots, c_n \in \mathbb{Z}$.

(β) Υπάρχει πολυώνυμο $p(x)$ με αυτή την ιδιότητα για το οποίο για $m \in \mathbb{Z}$, το $p(m)$ είναι άρτιος αριθμός αν και μόνο αν $m \equiv 0 \pmod 3$ ή $m \equiv 1 \pmod 3$;

98. Για κάθε πρώτο αριθμό p, υπολογίστε το υπόλοιπο της διαίρεσης των εξής γινομένων με το p:

(α) $\prod_{k=1}^{p}(k^2+1)$,
(β) $\prod_{k=1}^{p}(k^2+k+1)$.

Υποδείξεις - Λύσεις

(1) Το (α) αφήνεται στον αναγνώστη (εργαστείτε με επαγωγή στο a, διακρίνοντας τις περιπτώσεις ο a να είναι άρτιος ή περιττός αριθμός). Για το (β), δείξτε ότι οι δυνατές τιμές του k είναι όλοι οι άρτιοι φυσικοί αριθμοί ως εξής. Δείξτε πρώτα ότι αν το $x^2 + xy + y^2 = 2^k \cdot q$ είναι άρτιος αριθμός, τότε οι x, y είναι και οι δύο άρτιοι. Γράφοντας $x = 2u$ και $y = 2v$ με $u, v \in \mathbb{Z}$, συμπεράνετε ότι $u^2 + uv + v^2 = 2^{k-2} \cdot q$ και χρησιμοποιήστε κατάλληλα την αρχή της επαγωγής για να δείξετε ότι ο k είναι άρτιος. Αντιστρόφως, αν ο k είναι άρτιος, παρατηρήστε ότι $x^2 + xy + y^2 = 2^k$ για $x = 2^{k/2}$ και $y = 0$. Για το (γ), θέτοντας $a(n) = (n+1)(n+2)\cdots(2n)$, βρίσκουμε ότι

$$a(n) \;=\; \frac{(2n)!}{n!} \;=\; \frac{1}{n!} \cdot 2 \cdot 4 \cdots (2n) \cdot 1 \cdot 3 \cdots (2n-1) \;=\; 2^n \cdot q(n),$$

όπου $q(n) = 1 \cdot 3 \cdots (2n-1)$ είναι περιττός αριθμός, και συμπεραίνουμε ότι η μεγαλύτερη δύναμη του 2 που διαιρεί το $a(n)$ είναι ίση με 2^n. Εναλλακτικά, δείχνουμε πρώτα ότι $a(n+1) = 2(2n+1)a(n)$ για κάθε θετικό ακέραιο n και έπειτα, δείχνουμε επαγωγικά ότι $a(n) = 2^n \cdot q(n)$ για κάποιο περιττό $q(n) \in \mathbb{N}$.

(2) Το (α) αφήνεται στον αναγνώστη. Για το (β), θέτοντας $q_n = a_n/2^{n+1}$ για $n \in \mathbb{N}$, επαληθεύστε ότι $q_0 = 1$ και $q_1 = 5$, συνάγετε από το (α) ότι $q_n = 4q_{n-1} - q_{n-2}$ για $n \geq 2$ και δείξτε με επαγωγή στο n ότι το q_n είναι περιττός φυσικός αριθμός για κάθε $n \in \mathbb{N}$. Για το (γ), δείξτε ότι $\lfloor (1+\sqrt{3})^{2n+1} \rfloor = a_n$ για κάθε $n \in \mathbb{N}$ και εφαρμόστε το (β).

(3) Για το (α) έχουμε γενικότερα $a+1 \mid a^n + 1$ για κάθε περιττό $n \in \mathbb{N}$ και κάθε $a \in \mathbb{Z}$, λόγω της ταυτότητας $a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1)$. Το (β) ισχύει επίσης για κάθε $a \in \mathbb{Z}$, λόγω της ταυτότητας $a^4 + a^2 + 1 = (a^2 - a + 1)(a^2 + a + 1)$. Για το (γ), παρατηρούμε ότι το $a^6 + a^3 - 2 = (a^3 - 1)(a^3 + 2)$ διαιρείται από το $a^3 - 1$, άρα και από το $a^2 + a + 1$, και συμπεραίνουμε ότι $a^2 + a + 1 \mid a^6 + a^3 + 1 \Leftrightarrow a^2 + a + 1 \mid 3 \Leftrightarrow a^2 + a \in \{0, 2\}$. Κατά συνέπεια, το (β) ισχύει ακριβώς όταν $a \in \{-2, -1, 0, 1\}$. Για το (δ), παρατηρούμε ότι $a^3 + a^2 + a + 1 = (a+1)(a^2+1)$ για κάθε $a \in \mathbb{Z}$ και συμπεραίνουμε ότι

$$\begin{aligned} a^3 + a^2 + a + 1 \mid a^6 + a^4 + a^2 + 1 \quad &\Leftrightarrow \quad (a+1)(a^2+1) \mid (a^2+1)(a^4+1) \\ &\Leftrightarrow \quad a + 1 \mid a^4 + 1. \end{aligned}$$

Αφού όμως $a + 1 \mid a^4 - 1$ για κάθε $a \in \mathbb{Z}$, έχουμε $a + 1 \mid a^4 + 1 \Leftrightarrow a + 1 \mid 2 \Leftrightarrow a + 1 \in \{\pm 1, \pm 2\}$. Άρα, το (γ) ισχύει ακριβώς όταν $a \in \{-3, -2, 0, 1\}$.

(4) Για το (γ), παρητηρούμε ότι $f(a^n) = a^{2n} + a^n + 1$ και βρίσκουμε ότι το

$$\begin{aligned} f(a^{n+3}) - f(a^n) \;&=\; (a^{2n+6} + a^{n+3} + 1) - (a^{2n} + a^n + 1) \\ &=\; (a^{2n+6} - a^{2n}) + (a^{n+3} - a^n) \;=\; a^{2n}(a^6 - 1) + a^n(a^3 - 1) \\ &=\; a^{2n}(a^3 - 1)(a^3 + 1) + a^n(a^3 - 1) \\ &=\; (a^3 - 1)(a^{2n+3} + a^{2n} + a^n) \end{aligned}$$

διαιρείται με το $a^3 - 1 = (a-1)(a^2 + a + 1)$, άρα και με το $a^2 + a + 1 = f(a)$, για κάθε $a \in \mathbb{Z}$. Από αυτό προκύπτει ότι $f(a) \mid f(a^n) \Leftrightarrow f(a) \mid f(a^r)$, όπου r είναι το υπόλοιπο της διαίρεσης του n με το 3. Αφού $f(a^0) = 3$ και τα $f(a^1) = f(a)$ και $f(a^2) = a^4 + a^2 + 1 = (a^2 - a + 1)(a^2 + a + 1)$ διαιρούνται με το $f(a)$, συμπεραίνουμε ότι η απάντηση στο (α) είναι όλοι οι φυσικοί αριθμοί που δε διαιρούνται με το 3. Εργαζόμαστε ομοίως για τα (β) και (δ) και βρίσκουμε ότι η απάντηση στο (β) είναι όλοι οι φυσικοί αριθμοί που δε διαιρούνται με το 5. Για να επαληθεύσουμε αυτόν τον ισχυρισμό για $n \in \{2, 3, 4\}$, χρησιμοποιούμε

την ταυτότητα $g(a) = (a^5 - 1)/(a - 1)$, τους υπολογισμούς

$$g(a^2) = \frac{a^{10}-1}{a^2-1} = \frac{(a^5-1)(a^5+1)}{(a-1)(a+1)} = g(a)\cdot\frac{a^5+1}{a+1}$$

$$g(a^3) = \frac{a^{15}-1}{a^3-1} = \frac{(a^5-1)(a^{10}+a^5+1)}{(a-1)(a^2+a+1)} = g(a)\cdot\frac{a^{10}+a^5+1}{a^2+a+1}$$

$$g(a^4) = \frac{a^{20}-1}{a^4-1} = \frac{(a^{10}-1)(a^{10}+1)}{(a^2-1)(a^2+1)} = g(a)\cdot\frac{a^5+1}{a+1}\cdot\frac{a^{10}+1}{a^2+1}$$

και τις σχέσεις διαιρετότητας $a+1 \mid a^5+1$ και $a^2+a+1 \mid a^{10}+a^5+1$ για $a \in \mathbb{Z}$, οι οποίες μας είναι ήδη γνωστές. Γενικότερα, έστω $n \in \mathbb{N}$, πρώτος αριθμός p και $f_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$. Χρησιμοποιώντας στοιχειώδεις γνώσεις για ρίζες πολυωνύμων μπορεί να δείξει κανείς ότι $f_p(a) \mid f_p(a^n)$ για κάθε $a \in \mathbb{Z}$ αν και μόνο αν ο n δε διαιρείται με το p.

(5) Το (α) αφήνεται στον αναγνώστη. Για το (β) εφαρμόστε επαγωγή στο n, χρησιμοποιώντας το (α) και τις ισότητες $\binom{n}{0} = \binom{n}{n} = 1$ για $n \in \mathbb{N}$. Για το (γ), παρατηρήστε ότι το γινόμενο k διαδοχικών ακεραίων είτε ισούται με μηδέν, είτε είναι της μορφής

$$(n+1)(n+2)\cdots(n+k) = k!\binom{n+k}{k},$$

ή

$$(-n-1)(-n-2)\cdots(-n-k) = (-1)^k k!\binom{n+k}{k},$$

για κάποιο $n \in \mathbb{N}$ και χρησιμοποιήστε το (β). Για το (δ) εφαρμόστε επαγωγή στο n, γράφοντας $(x+y)^{n+1} = (x+y)^n(x+y)$, και χρησιμοποιήστε το (α).

(6) Για το (α), δείξτε ότι μια τέτοια τριάδα (a, b, c) είναι η $a = 4k$, $b = 2k+1$ και $c = 4k+1$. Μια άλλη είναι εκείνη με $a = 4k$, $b = 2k-1$ και $c = 4k-1$. Το ερώτημα (β) έχει αρνητική απάντηση: θα δείξουμε ότι οι τριάδες με τις δοσμένες ιδιότητες είναι η $(2, 3, 5)$, εκείνες με $a = b = 1$ και $c \in \mathbb{Z}_{>0}$ και οι μεταθέσεις αυτών. Πράγματι, μπορούμε να υποθέσουμε ότι $a \le b \le c$ και $b \ge 2$. Αφού $b \le c$ και $c \mid ab - 1$, έχουμε επίσης $a \ge 2$. Γράφοντας $ab = cm + 1$ με $m \in \mathbb{N}$, έχουμε $1 \le m < a$ (εξηγήστε γιατί). Πολλαπλασιάζοντας την ισότητα $ab = cm + 1$ με a και b, αντίστοιχα, βρίσκουμε ότι $a^2b = (ac-1)m + (a+m)$ και $ab^2 = (bc-1)m + (b+m)$. Από αυτές τις ισότητες και τις σχέσεις $b \mid ac - 1$ και $a \mid bc - 1$ έπεται ότι $b \mid (a+m)$ και $a \mid (b+m)$. Αφού όμως $m < a \le b$, έχουμε $a + m < 2b$ και συνεπώς $b = a + m$. Από την ισότητα αυτή και τη σχέση $a \mid (b+m)$ βρίσκουμε ότι $a \mid 2m$ και, αφού $2m < 2a$, συμπεραίνουμε ότι $a = 2m$, οπότε και $b = 3m$. Εν όψη της $ab = cm + 1$, βρίσκουμε ότι $m = 1$ και καταλήγουμε στην τριάδα $(a, b, c) = (2, 3, 5)$.

(7) Έστω $f(n)$ το υπόλοιπο της διαίρεσης του $a_n = 1^n + 2^n + 3^n + 4^n$ με το 5. Αν ο n είναι περιττός, τότε $5 \mid 1^n + 4^n$ και $5 \mid 2^n + 3^n$ (εξηγήστε γιατί), οπότε $5 \mid a_n$ και $f(n) = 0$. Αν ο n είναι άρτιος, τότε $n = 4k$ ή $n = 4k+2$ για κάποιο $k \in \mathbb{N}$. Θα δείξουμε ότι $f(n) = 4$ στην πρώτη περίπτωση και $f(n) = 0$ στη δεύτερη. Έστω ότι το n είναι ακέραιο πολλαπλάσιο του 4. Τότε, τα $2^n - 1$, $3^n - 1$ και $4^n - 1$ διαιρούνται (εξηγήστε γιατί) με τους $2^4 - 1 = 15$, $3^4 - 1 = 80$ και $4^4 - 1 = 255$, αντίστοιχα, άρα διαιρούνται και με το 5. Κατά συνέπεια, το $a_n - 4 = (2^n - 1) + (3^n - 1) + (4^n - 1)$ διαιρείται επίσης με το 5 και συνεπώς $f(n) = 4$. Ομοίως βρίσκουμε ότι αν $n = 4k+2$, τότε το $a_n - (1^2 + 2^2 + 3^2 + 4^2) = (2^n - 2^2) + (3^n - 3^2) + (4^n - 4^2)$ διαιρείται με το 5. Αφού $1^2 + 2^2 + 3^2 + 4^2 = 30$, συμπεραίνουμε ότι $5 \mid a_n$ οπότε και $f(n) = 0$. Εναλλακτικά, στην περίπτωση που ο $n = 2m$ είναι άρτιος αριθμός, έχουμε

$a_n = 1^m + 4^m + 9^m + 16^m \equiv 2 + 2 \cdot (-1)^m \pmod 5$ και συνεπώς $f(n) = 4$, αν ο m είναι άρτιος και $f(n) = 0$, αν ο m είναι περιττός.

(8) Για το (α) γράφουμε $a = 5q + r$ και $b = 5t + s$ με $q, t \in \mathbb{Z}$ και $r, s \in \{0, 1, 2, 3, 4\}$. Εκτελώντας τις πράξεις, βρίσκουμε ότι διαιρούμενο με το 5, το $a^2 + ab + b^2$ αφήνει το ίδιο υπόλοιπο με το $r^2 + rs + t^2$ και ότι το τελευταίο είναι ακέραιο πολλαπλάσιο του 5 μόνο για $r = s = 0$. Για το (β), συμπεραίνουμε από το (α) διαδοχικά ότι θα πρέπει $x = 5u$ και $y = 5v$ για κάποια $u, v \in \mathbb{Z}$ με $u^2 + uv + v^2 = 300$ και ότι $u = 5p$ και $v = 5q$ για κάποια $p, q \in \mathbb{Z}$ με $p^2 + pq + q^2 = 12$. Αφού οι p και q θα πρέπει να είναι και οι δύο άρτιοι, βρίσκουμε ότι $p = q = \pm 2$ και συμπεραίνουμε ότι τα ζητούμενα ζεύγη είναι τα $(x, y) = (50, 50)$ και $(x, y) = (-50, -50)$. Εργαζόμενοι ομοίως βρίσκουμε ότι η εξίσωση στο (γ) δεν έχει ακέραιες λύσεις.

(9) Τα δυνατά υπόλοιπα είναι τα $0, 1, 8$ για το (α), τα $0, 1, 10, 19$ για το (β) και τα $0, 1, 24$ για το (γ). Πράγματι, για το (α), αν το a είναι ακέραιο πολλαπλάσιο του 3, τότε το a^3 διαιρείται με το 27, άρα και με το 9. Διαφορετικά, έχουμε $a = 3q \pm 1$ για κάποιο $q \in \mathbb{Z}$ και συνεπώς

$$a^3 \;=\; (3q \pm 1)^3 \;=\; (3q)^3 \pm 3(3q)^2 + 3(3q) \pm 1 \;=\; 9t \pm 1$$

με $t \in \mathbb{Z}$. Ομοίως, για το (γ), αν το a δε διαιρείται με το 5, τότε $a^2 = 5q \pm 1$ για κάποιο $q \in \mathbb{Z}$ (εξηγήστε γιατί) και συνεπώς

$$a^{10} \;=\; (5q \pm 1)^5 \;=\; (5q)^5 \pm 5(5q)^4 + 10(5q)^3 \pm 10(5q)^2 + 5(5q) \pm 1 \;=\; 25t \pm 1$$

με $t \in \mathbb{Z}$. Τέλος, για το (β), αν το a δε διαιρείται με το 3, τότε $a^2 = 9q + r$ για κάποια $q \in \mathbb{Z}$ και $r \in \{1, -2, 4\}$ (εξηγήστε γιατί) και συνεπώς

$$a^6 \;=\; (9q + r)^3 \;=\; (9q)^3 + 3r(3q)^2 + 3r^2(3q) + r^3 \;=\; 27t + s$$

με $s \in \{1, 10, 19\}$.

(10) Το (α) ισχύει αν και μόνο αν $m \in \{1, 3, 5, 7\}$. Πράγματι, για αυτές τις τιμές του m η ισοτιμία $x_1^3 + x_2^3 + \cdots + x_m^3 \equiv 0 \pmod 9$ δεν έχει λύση όταν τα x_i δε διαιρούνται με το 3, αφού τότε καθένα από τα x_i^3 αφήνει υπόλοιπο 1 ή -1 διαιρούμενο με το 9 (Άσκηση 9). Αντιστρόφως, αν ο m είναι άρτιος, ή περιττός ≥ 9, τότε η $x_1^3 + x_2^3 + \cdots + x_m^3 \equiv 0 \pmod 9$ έχει λύση για κατάλληλη επιλογή των $x_i \in \{-1, 1\}$. Χρησιμοποιώντας το αποτέλεσμα της ίδιας άσκησης, βρίσκουμε παρόμοια ότι το (γ) ισχύει αν και μόνο αν $m \in \{1, 3, 5, \ldots, 25\}$. Δείξτε ότι το (β) ισχύει αν και μόνο αν $m \not\equiv 0, 9, 18 \pmod{27}$ ως εξής. Υποθέστε ότι $x_1^6 + x_2^6 + \cdots + x_m^6 \equiv 0 \pmod{27}$ για κάποια $x_1, x_2, \ldots, x_m \in \mathbb{Z}$ που δε διαιρούνται με το 3. Τότε (Άσκηση 9), καθένα από τα x_i^6 αφήνει υπόλοιπο 1, 10 ή 19 διαιρούμενο με το 27. Αφού $10+19 \equiv 1+1 \pmod{27}$, μπορούμε να υποθέσουμε ότι είτε $x_i^6 \equiv 1, 10 \pmod{27}$ για κάθε i, είτε $x_i^6 \equiv 1, 19 \pmod{27}$ για κάθε i. Έστω ότι υπάρχουν ακριβώς p δείκτες $i \in \{1, 2, \ldots, m\}$ με $x_i^6 \equiv 1 \pmod{27}$ και ακριβώς q δείκτες $j \in \{1, 2, \ldots, m\}$ με $x_j^6 \equiv 10 \pmod{27}$ (αντίστοιχα, $x_j^6 \equiv 19 \pmod{27}$). Τότε, $p + q = m$ και $p + 10q \equiv 0 \pmod{27}$ (αντίστοιχα, $p + 19q \equiv 0 \pmod{27}$). Από τις σχέσεις αυτές προκύπτει (εξηγήστε πώς) ότι $m \equiv 0 \pmod 9$, οπότε το m αφήνει υπόλοιπο 0, 9 ή 18 διαιρούμενο με το 27. Το αντίστροφο αφήνεται στον αναγνώστη.

(11) Έστω d ο ζητούμενος μέγιστος κοινός διαιρέτης στο (β). Αφού $m^2n^2(m^6 - n^6) = 252$ για $m = 2$ και $n = 1$, έχουμε $d \mid 252$. Αντιστρόφως, δείξτε ότι ο ακέραιος $m^2n^2(m^6 - n^6)$ διαιρείται με καθέναν από τους 4, 7 και 9 για όλα τα $m, n \in \mathbb{Z}$ και συμπεράνετε ότι $d = 252$. Για παράδειγμα, σύμφωνα με τη λύση της Άσκησης 9, αν οι m, n δεν είναι ακέραια πολλαπλάσια του 3, τότε τα m^3 και n^3 αφήνουν υπόλοιπο 1 ή 8 διαιρούμενα με το 9 και συνεπώς το $m^6 - n^6 = (m^3 - n^3)(m^3 + n^3)$ διαιρείται με το 9. Απάντηση για το (α): $d = 30$.

(12) Το (α) αφήνεται στον αναγνώστη. Για το (β), γράψτε την ταυτότητα του (α) ως $k\binom{n}{k} = n\binom{n-1}{k-1}$ και εφαρμόστε γνωστές ιδιότητες της διαιρετότητας.

(13) Για το (α), εφαρμόζουμε επαγωγή στο m (τετριμμένο για $m = 0$). Υποθέτοντας ότι ισχύει για το $m \in \mathbb{N}$ και για κάθε $n \in \mathbb{Z}_{>0}$, βρίσκουμε ότι

$$\begin{aligned} F_{(m+1)+n} &= F_{m+(n+1)} = F_{m+1}F_{n+1} + F_mF_n = F_{m+1}(F_n + F_{n-1}) + F_mF_n \\ &= (F_{m+1} + F_m)F_n + F_{m+1}F_{n-1} = F_{m+2}F_n + F_{m+1}F_{n-1}. \end{aligned}$$

Αυτό δείχνει ότι το ζητούμενο ισχύει και για το $m + 1$ και ολοκληρώνει το επαγωγικό βήμα. Εναλλακτικά, δείχνουμε με επαγωγή στο n ότι

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

για κάθε $n \in \mathbb{Z}_{>0}$ και συνδυάζουμε την ισότητα αυτή με την ταυτότητα

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{m+n} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^m \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

για να συνάγουμε το ζητούμενο. Για το (β), θέτοντας πρώτα $n = km$ στο (α) παίρνουμε $F_{(k+1)m} = F_{m+1}F_{km} + F_mF_{km-1}$ και έπειτα, χρησιμοποιώντας την ισότητα αυτή, δείχνουμε με επαγωγή στο k ότι $F_m \mid F_{km}$ για $m, k \in \mathbb{N}$. Για το (γ) εφαρμόζουμε επαγωγή στο μέγιστο των m, n. Αφού το ζητούμενο είναι τετριμμένο για $m = n$, μπορούμε να υποθέσουμε ότι $m < n$. Θεωρούμε την Ευκλείδεια διαίρεση $n = mq + r$ του n με το m και, εφαρμόζοντας κατάλληλα το (α), βρίσκουμε ότι $F_n = F_{r+1}F_{mq} + F_rF_{mq-1}$. Από την ισότητα αυτή, αφού $F_m \mid F_{mq}$ από το (β) και $\mu\kappa\delta(F_m, F_{mq-1}) = F_{\mu\kappa\delta(m,mq-1)} = 1$ από την υπόθεση της επαγωγής, προκύπτει (εξηγήστε πώς) ότι $\mu\kappa\delta(F_m, F_n) = \mu\kappa\delta(F_r, F_m)$. Όμως, αφού $r < m < n$, έχουμε $\mu\kappa\delta(F_r, F_m) = F_{\mu\kappa\delta(r,m)}$ από την υπόθεση της επαγωγής και προφανώς $\mu\kappa\delta(r, m) = \mu\kappa\delta(m, n)$. Από τα προηγούμενα έπεται ότι $\mu\kappa\delta(F_m, F_n) = F_{\mu\kappa\delta(m,n)}$. Για το (δ), υποθέτουμε ότι $F_m \mid F_n$. Τότε, σύμφωνα με το (γ), έχουμε $F_m = F_{\mu\kappa\delta(m,n)}$. Αφού $m \neq 2$, από αυτό έπεται (εξηγήστε γιατί) ότι $m = \mu\kappa\delta(m, n)$, δηλαδή ότι $m \mid n$.

(14) Για το (α), υποθέτουμε ότι $\mu\kappa\delta(a, b) = 1$. Παρατηρούμε ότι κάθε πρώτος p που διαιρεί τα $a + b$ και $a^2 + b^2$ διαιρεί και το $(a + b)^2 - (a^2 + b^2) = 2ab$. Αποκλείουμε (εξηγήστε πώς) την περίπτωση $p \mid ab$ και συμπεραίνουμε ότι $p = 2$. Τότε, ο $\mu\kappa\delta(a + b, a^2 + b^2)$ είναι δύναμη του 2 και οι a και b είναι και οι δύο περιττοί αριθμοί. Αφού όμως το $a^2 + b^2$ δε διαιρείται με το 4 (εξηγήστε γιατί), έχουμε υποχρεωτικά $\mu\kappa\delta(a + b, a^2 + b^2) = 2$. Για το (β), παρατηρούμε πρώτα ότι κάθε ζεύγος $(x, y) \in \mathbb{Z}^2$ με $xy = 0$ έχει τη ζητούμενη ιδιότητα. Θα δείξουμε ότι τα ζεύγη (x, y) για τα οποία $xy \neq 0$ είναι εκείνα με

$$\begin{aligned} x &= \lambda u(u^2 + v^2) \\ y &= \lambda v(u^2 + v^2), \end{aligned}$$

όπου λ είναι μη μηδενικός ακέραιος και u, v είναι σχετικώς πρώτοι μη μηδενικοί ακέραιοι, ακριβώς ένας από τους οποίους είναι άρτιος, και εκείνα με

$$\begin{aligned} x &= \lambda u(u^2 + v^2)/2 \\ y &= \lambda v(u^2 + v^2)/2, \end{aligned}$$

όπου λ είναι μη μηδενικός ακέραιος και u, v είναι σχετικώς πρώτοι περιττοί ακέραιοι. Πράγματι, δίνεται ότι $(x + y)^3 = q(x^2 + y^2)$ για κάποιο $q \in \mathbb{Z}$. Ας θέσουμε $d = \mu\kappa\delta(x, y)$ και ας γράψουμε $x = du$ και $y = dv$, όπου $\mu\kappa\delta(u, v) = 1$. Τότε, $d(u + v)^3 = q(u^2 + v^2)$ και, σύμφωνα με το (α), $\mu\kappa\delta(u + v, u^2 + v^2) = 1$ αν ακριβώς ένας από τους u, v είναι άρτιος, και $\mu\kappa\delta(u + v, u^2 + v^2) = 2$ αν και οι δύο είναι περιττοί. Στην πρώτη περίπτωση οι $(u + v)^3$ και $u^2 + v^2$ είναι

σχετικώς πρώτοι και συνεπώς από την ισότητα $d(u+v)^3 = q(u^2+v^2)$ προκύπτει ότι $u^2+v^2 \mid d$. Γράφοντας $d = \lambda(u^2+v^2)$ με $\lambda \in \mathbb{Z}$, δεδομένου ότι $x = du$ και $y = dv$, καταλήγουμε στο πρώτο σύνολο λύσεων που αναφέρθηκε στην αρχή. Εργαζόμαστε ομοίως στη δεύτερη περίπτωση, γράφοντας $d(u+v)^3/2 = q(u^2+v^2)/2$ και παρατηρώντας (εξηγήστε πώς) ότι οι $(u+v)^3/2$ και $(u^2+v^2)/2$ είναι σχετικώς πρώτοι.

(15) Για τη συνεπαγωγή (i) $\Rightarrow$ (ii) αρκεί να θέσει κανείς $d = 2^k$. Ας υποθέσουμε ότι ισχύει η (ii). Τότε, αφού οι m/d και n/d είναι περιττοί και ο $x+y$ διαιρεί το x^k+y^k για κάθε περιττό $k \in \mathbb{N}$ και όλα τα $x, y \in \mathbb{Z}$, έχουμε ότι οι a^m+b^m και a^n+b^n διαιρούνται από το a^d+b^d και συνεπώς ότι $\mu\kappa\delta(a^m+b^m, a^n+b^n) \geq a^d+b^d \geq 3$, εκτός αν $a = b = 1$. Δείξαμε ότι (ii) $\Rightarrow$ (iii). Για τη συνεπαγωγή (iii) $\Rightarrow$ (i), υποθέτουμε ότι δεν ισχύει το (i) και θεωρούμε θετικούς ακεραίους a, b με $\mu\kappa\delta(a,b) = 1$. Θα δείξουμε ότι $\mu\kappa\delta(a^m+b^m, a^n+b^n) \leq 2$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $m = 2^k \cdot p$ και $n = 2^\ell \cdot q$ για κάποιους περιττούς αριθμούς p, q και $k, \ell \in \mathbb{N}$ με $k < \ell$. Θέτοντας $d = 2^k$, αφού $\mu\kappa\delta(a^d, b^d) = 1$, μπορούμε να αντικαταστήσουμε τους a και b με τους a^d και b^d και έτσι να έτσι να ανάγουμε το πρόβλημα στην περίπτωση $k = 0$. Δηλαδή, μπορούμε να υποθέσουμε χωρίς βλάβη της γενικότητας ότι ο m είναι περιττός και ο n είναι άρτιος. Ας θεωρήσουμε τώρα έναν κοινό πρώτο διαιρέτη t των a^m+b^m και a^n+b^n. Αφού ο m είναι περιττός, έχουμε $a^n+b^n \mid a^{mn}+b^{mn}$. Επίσης, αφού ο n είναι άρτιος, έχουμε $(a^m+b^m)(a^m-b^m) = a^{2m}-b^{2m} \mid a^{mn}-b^{mn}$ και συνεπώς $a^m+b^m \mid a^{mn}-b^{mn}$. Άρα, ο t διαιρεί τους $a^{mn}+b^{mn}$ και $a^{mn}-b^{mn}$ και επομένως και τους $2a^{mn}$ και $2b^{mn}$. Αφού όμως οι a^{mn} και b^{mn} είναι σχετικώς πρώτοι, θα πρέπει $t = 2$. Από αυτό συμπεραίνουμε ότι $\mu\kappa\delta(a^m+b^m, a^n+b^n) = 2^r$ για κάποιο $r \in \mathbb{N}$. Αφού όμως ο n είναι άρτιος και ένας τουλάχιστον από τους a, b είναι περιττός, ο a^n+b^n δε διαιρείται με το 4 (εξηγήστε γιατί) και επομένως $r = 0$ ή $r = 1$, όπως το θέλαμε.

(16) Αν ο n είναι περιττός, τότε ο δοσμένος ακέραιος έχει γνήσιο διαιρέτη τον a^2+1. Διαφορετικά, γράφοντας $n = 2m$, βρίσκουμε ότι

$$\begin{aligned} 1+a^2+a^4+\cdots+a^{2n} &= \frac{a^{4m+2}-1}{a^2-1} = \frac{(a^{2n+1}-1)(a^{2n+1}+1)}{(a-1)(a+1)} \\ &= (1+a+a^2+\cdots+a^{2m})(1-a+a^2-\cdots+a^{2m}), \end{aligned}$$

ο οποίος είναι επίσης σύνθετος αριθμός.

(17) Αν όχι, τότε ο $p+q$ γράφεται ως γινόμενο δύο το πολύ πρώτων αριθμών. Όμως, αφού οι p, q είναι περιττοί, ο $p+q$ είναι άρτιος και συνεπώς $p+q = 2r$ για κάποιο πρώτο r. Τότε $r = (p+q)/2$ και συνεπώς έχουμε είτε $p < r < q$, είτε $q < r < p$, σε αντίθεση με την υπόθεση ότι οι p και q είναι διαδοχικοί πρώτοι.

(18) Ο μόνος πρώτος με την ιδιότητα του (α) είναι ο $p = 3$. Πράγματι, δείξτε ότι $3 \mid 2^p+1$ για κάθε περιττό $p \in \mathbb{N}$ και ότι $3 \mid p^2-1$ για κάθε ακέραιο p που δε διαιρείται με το 3 και συμπεράνετε ότι $3 \mid 2^p+p^2$ για κάθε πρώτο $p \geq 5$. Ομοίως, δείξτε ότι $5 \mid 4^p+1$ για κάθε περιττό $p \in \mathbb{N}$ και ότι $5 \mid p^4-1$ για κάθε ακέραιο p που δε διαιρείται με το 5. Συμπεράνετε ότι $5 \mid 4^p+p^4$ για κάθε πρώτο $p \neq 2, 5$ και ότι δεν υπάρχει πρώτος αριθμός p με την ιδιότητα του (β).

(19) Υποθέστε ότι το δοσμένο άθροισμα ισούται με $q \in \mathbb{Z}$. Πολλαπλασιάστε αυτή την ισότητα με $(p_1 p_2 \cdots p_n)^m$ και δείξτε ότι ο πρώτος p_n διαιρεί το ένα σκέλος της ισότητας που προέκυψε αλλά όχι το άλλο, για να καταλήξετε σε άτοπο (θα χρειαστεί να εφαρμόσετε γνωστές ιδιότητες της διαιρετότητας και ιδιότητες των πρώτων αριθμών).

(20) Για το (α) παρατηρούμε ότι

$$\frac{1}{k^m} + \frac{1}{(p-k)^m} = \frac{k^m + (p-k)^m}{k^m\,(p-k)^m}$$

και, αφού ο m είναι περιττός, ότι το $k^m + (p-k)^m$ διαιρείται με το p για κάθε $k \in \{1, 2, \ldots, p-1\}$. Προσθέτοντας αυτές τις ισότητες για $1 \le k \le (p-1)/2$ βρίσκουμε ότι $a/b = px/q$ για κάποιο $x \in \mathbb{Z}$, όπου $q = ((p-1)!)^m$. Γράφοντας την τελευταία ισότητα ως $aq = pbx$ παίρνουμε ότι $p \mid aq$. Δεδομένου ότι $\mu\kappa\delta(p, q) = 1$, συμπεραίνουμε ότι $p \mid a$. Εργαζόμαστε ομοίως για το (β), προσθέτοντας τις ισότητες

$$\frac{1}{(2k-1)^m} + \frac{1}{(2^n - 2k + 1)^m} = \frac{(2k-1)^m + (2^n - 2k + 1)^m}{(2k-1)^m\,(2^n - 2k + 1)^m}$$

για $1 \le k \le 2^{n-2}$.

(21) Για το (α), γνωρίζουμε από την Άσκηση 5 (β) ότι το $k!\,(p-k)!$ διαιρεί το $p! = p \cdot (p-1)!$. Αφού ο p είναι πρώτος αριθμός, ο $k!\,(p-k)!$ είναι σχετικώς πρώτος προς το p (εξηγήστε γιατί) και επομένως ο $k!\,(p-k)!$ διαιρεί το $(p-1)!$. Έχουμε, ισοδύναμα, $\frac{1}{p}\binom{p}{k} \in \mathbb{Z}$. Για το (β), θεωρούμε την ταυτότητα

$$(1+x)^{pn} = \left(\sum_{k=0}^{p} \binom{p}{k} x^k\right)^n.$$

Εξισώνοντας τους συντελεστές του x^p στα δύο μέλη, βρίσκουμε ότι

$$\binom{pn}{p} = \sum_{k_1+k_2+\cdots+k_n=p} \binom{p}{k_1}\binom{p}{k_2}\cdots\binom{p}{k_n}.$$

Από το (α) γνωρίζουμε ότι οι διωνυμικοί συντελεστές $\binom{p}{k}$ διαιρούνται με το p όταν $1 \le k < p$. Επομένως, ακριβώς n όροι του αθροίσματος στο δεξιό μέλος είναι ίσοι με 1 και οι υπόλοιποι διαιρούνται με το p^2 (εξηγήστε γιατί). Το ζητούμενο έπεται. Εργαζόμαστε με παρόμοιο τρόπο για το (γ).

(22) Για τη δεύτερη ισότητα στο (α), εφαρμόστε την Άσκηση 5 (δ). Για την πρώτη ισότητα, συνάγετε ότι $(\sqrt{5}+2)^p - (\sqrt{5}-2)^p \in \mathbb{Z}$ και παρατηρήστε ότι $0 < (\sqrt{5}-2)^p < 1$. Για το (β), χρησιμοποιήστε το (α) και την Άσκηση 21 (α).

(23) Παρατηρούμε ότι για $m \ge 2$ ο ακέραιος $2018^m + 3$ είναι της μορφής $4k+3$ και συνεπώς έχει τουλάχιστον ένα πρώτο διαιρέτη της ίδιας μορφής (εξηγήστε γιατί), ενώ ο $1885^n = 5^n \cdot 13^n \cdot 29^n$ δεν έχει τέτοιους διαιρέτες. Το ίδιο ισχύει για $m \in \{0, 1\}$ αφού $2021 = 43 \cdot 47$.

(24) Θεωρήστε την κανονική ανάλυση των m, n και δείξτε ότι η συνθήκη που δίνεται είναι ισοδύναμη με την εξής: αν p είναι πρώτος διαιρέτης του m και p^α είναι η μεγαλύτερη δύναμη του p που διαιρεί το m, τότε $p^\alpha \mid p^{3\beta} \Rightarrow p^\alpha \mid p^{2\beta}$ για $\beta \in \mathbb{N}$. Δείξτε ότι η τελευταία συνεπαγωγή ισχύει αν και μόνο αν $\alpha \in \{1, 2, 4\}$ και συνάγετε ότι οι θετικοί ακέραιοι m με την επιθυμητή ιδιότητα είναι εκείνοι που έχουν κανονική ανάλυση της μορφής $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ με $\alpha_i \in \{1, 2, 4\}$ για κάθε i.

(25) Σωστή είναι μόνο η πρόταση στο (β). Για το (α), αρκεί να θέσει κανείς $m = 12$, $n = 18$ και $k = 2$. Για το (β), θα δείξουμε ότι κάθε δύναμη πρώτου που διαιρεί το m^{m^m} διαιρεί επίσης και το n^{n^n}. Πράγματι, ας θεωρήσουμε πρώτο διαιρέτη p του m και ας γράψουμε $m = p^\alpha \cdot s$ για κάποιο θετικό ακέραιο α και κάποιο θετικό ακέραιο s που δε διαιρείται με το p. Αφού $m \mid n^k$, έχουμε $p \mid n$ και συνεπώς μπορούμε επίσης να γράψουμε $n = p^\beta \cdot t$ για κάποιο θετικό ακέραιο β και κάποιο θετικό ακέραιο t που δε διαιρείται με το p. Τότε

$$m^{m^m} = p^{\alpha m^m} s^{m^m}, \quad n^{n^n} = p^{\beta n^n} t^{n^n},$$

οπότε πρέπει να δείξουμε ότι $\alpha m^m \le \beta n^n$. Αυτό είναι προφανές αν $\alpha \le \beta$, δεδομένου ότι $m \le n$. Διαφορετικά, έχουμε $\alpha \ne \beta$ και επομένως $m \ne n$, δηλαδή $m < n$. Αφού $m \ge p^\alpha \ge 2^\alpha > \alpha$, συμπεραίνουμε ότι $\alpha m^m < m^{m+1} < n^n \le \beta n^n$. Θεωρούμε τώρα την ανάλυση του $m^{m^m} = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ σε γινόμενο δυνάμεων διακεκριμένων πρώτων $p_1, \ldots, p_r$. Δείξαμε ότι το n^{n^n} διαιρείται με καθέναν από τους $p_i^{\alpha_i}$. Αφού αυτοί είναι ανά δύο σχετικώς πρώτοι, το n^{n^n} διαιρείται επίσης με το γινόμενό τους, δηλαδή με το m^{m^m}.

(26) Ας δείξουμε τα (α) και (β) ταυτόχρονα. Το πρόβλημα είναι τετριμμένο για $k = 1$, οπότε μπορούμε να υποθέσουμε ότι $k \ge 2$. Έστω τυχαίος πρώτος p που διαιρεί το γινόμενο των n στοιχείων του S και έστω $p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_n}$ οι μεγαλύτερες δυνάμεις του p που διαιρούν τα στοιχεία αυτά. Ισχυριζόμαστε ότι οι φυσικοί αριθμοί $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι άρτιοι. Από την υπόθεση γνωρίζουμε ότι το άθροισμα οποιωνδήποτε k από τους $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι άρτιος αριθμός. Για $n = k = 2$, αυτό σημαίνει ότι οι α_1 και α_2 είναι είτε και οι δύο άρτιοι, είτε και οι δύο περιττοί. Αφού όμως τα δύο στοιχεία του S είναι πρώτα μεταξύ τους, οι α_1 και α_2 δεν μπορεί να είναι και οι δύο περιττοί και συνεπώς είναι άρτιοι. Έστω τώρα ότι $2 \le k < n$. Για δύο τυχαίους αριθμούς α_i, α_j μεταξύ των $\alpha_1, \alpha_2, \ldots, \alpha_n$ έχουμε ότι οι $\alpha_i + \beta_1 + \cdots + \beta_{k-1}$ και $\alpha_j + \beta_1 + \cdots + \beta_{k-1}$ είναι άρτιοι, όπου $\beta_1, \ldots, \beta_{k-1}$ είναι $k-1$ τυχαίοι μεταξύ των υπολοίπων. Έπεται ότι $\alpha_i \equiv \alpha_j \pmod 2$ και, αφού η επιλογή των α_i, α_j ήταν τυχαία, οι $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι είτε όλοι άρτιοι, είτε όλοι περιττοί. Όπως και στην περίπτωση $n = k = 2$, το δεύτερο ενδεχόμενο αποκλείεται και συνεπώς δείξαμε τον ισχυρισμό μας. Αφού η επιλογή του p ήταν τυχαία, η κανονική ανάλυση των στοιχείων του S δείχνει ότι καθένα από αυτά είναι γινόμενο τετραγώνων πρώτων αριθμών, άρα τετράγωνο ακεραίου και ισχύει το ζητούμενο.

(27) Όπως και στην Άσκηση 25, αρκεί να δείξουμε ότι κάθε δύναμη p^r πρώτου αριθμού p που διαιρεί το n διαιρεί επίσης και το $1 + a + \cdots + a^{n-1}$. Πράγματι, αφού το n διαιρεί το $(a-1)^k$, ο πρώτος p διαιρεί το $(a-1)^k$ και συνεπώς διαιρεί επίσης το $a-1$, δηλαδή $a \equiv 1 \pmod p$. Γράφοντας $n = p^r m$ για κάποιο θετικό ακέραιο m και θέτοντας $b = a^m$, έχουμε

$$\begin{aligned} 1 + a + \cdots + a^{n-1} &= \frac{a^n - 1}{a - 1} = \frac{a^m - 1}{a - 1} \frac{a^n - 1}{a^m - 1} = \frac{a^m - 1}{a - 1} \frac{a^{p^r m} - 1}{a^m - 1} \\ &= \frac{a^m - 1}{a - 1} \frac{b^{p^r} - 1}{b - 1} = \frac{a^m - 1}{a - 1} \prod_{i=1}^{r} \frac{b^{p^i} - 1}{b^{p^{i-1}} - 1} \\ &= \frac{a^m - 1}{a - 1} \prod_{i=1}^{r} \left(1 + b^{p^{i-1}} + b^{2p^{i-1}} + \cdots + b^{(p-1)p^{i-1}}\right). \end{aligned}$$

Αφού $b = a^m \equiv 1 \pmod p$, καθένας από τους όρους του γινομένου στον τύπο στον οποίο καταλήξαμε διαιρείται με το p και συνεπώς

$$1 + b^{p^{i-1}} + b^{2p^{i-1}} + \cdots + b^{(p-1)p^{i-1}} \equiv 1 + 1 + \cdots + 1 = p \equiv 0 \pmod p$$

για κάθε $i \in \{1, 2, \ldots, p\}$. Συμπεραίνουμε ότι το $1 + a + \cdots + a^{n-1}$ διαιρείται με το p^r.

(28) Για το (α) παρατηρούμε ότι $a_0 = a_1 = 1$, $a_2 = 2$ και $a_3 = 2^k + 1$. Εφαρμόζοντας επαγωγή στο n, ας υποθέσουμε ότι $n \ge 3$ και ότι $a_0, a_1, \ldots, a_n \in \mathbb{N}$. Θα δείξουμε ότι $a_{n+1} \in \mathbb{N}$. Από τις ισότητες $a_{n-1}a_{n-3} = a_{n-2}^k + 1$ και $a_n a_{n-2} = a_{n-1}^k + 1$ προκύπτει ότι

$$\begin{aligned} (a_n^k + 1)a_{n-2}^k &= (a_n a_{n-2})^k + a_{n-2}^k = (a_{n-1}^k + 1)^k + a_{n-2}^k = (qa_{n-1} + 1) + a_{n-2}^k \\ &= qa_{n-1} + (a_{n-2}^k + 1) = qa_{n-1} + a_{n-1}a_{n-3} = (a_{n-3} + q)a_{n-1}, \end{aligned}$$

για κάποιο $q \in \mathbb{N}$, και συνεπώς ότι $a_{n-1} \mid (a_n^k+1)a_{n-2}^k$. Αφού όμως $\mu\kappa\delta(a_{n-1}, a_{n-2}) = 1$, όπως προκύπτει από την ισότητα $a_n a_{n-2} = a_{n-1}^k + 1$, συμπεραίνουμε ότι $a_{n-1} \mid (a_n^k + 1)$, δηλαδή ότι $a_{n+1} = (a_n^k + 1)/a_{n-1} \in \mathbb{N}$. Για το (β), αν $k \geq 2$, δείξτε ότι η ακολουθία $(a_n)_{n\geq 1}$ είναι γνησίως αύξουσα και συνάγετε από το (α) ότι τα ζεύγη (a_n, a_{n+1}) για $n \in \mathbb{N}$ έχουν τις απαιτούμενες ιδιότητες.

(29) Για το (α) παρατηρούμε ότι $f(x, y) = f(u, v) \Leftrightarrow a(x - u) = b(v - y)$. Τότε, $b \mid a(x-u)$ και $a \mid b(y-v)$ οπότε, αφού $\mu\kappa\delta(a, b) = 1$, έχουμε $b \mid x-u$ και $a \mid y-v$. Για το (β), ισχυριζόμαστε ότι η $f(x, y) = c$ έχει μοναδική λύση στο $\mathbb{N} \times \mathbb{N}$ αν και μόνο αν $c = f(x_0, y_0)$ για κάποιο $(x_0, y_0) \in \{0, 1, \ldots, b-1\} \times \{0, 1, \ldots, a-1\}$. Το ζητούμενο είναι άμεση συνέπεια του ισχυρισμού διότι, λόγω του (α), ο περιορισμός της f στο $\{0, 1, \ldots, b-1\} \times \{0, 1, \ldots, a-1\}$ είναι 1–1 και η μέγιστη τιμή που λαμβάνει στο σύνολο αυτό η $f(b-1, a-1) = a(b-1) + b(a-1) = 2ab - a - b$. Για να δείξουμε τον ισχυρισμό παρατηρούμε ότι για να έχει η $f(x, y) = c$ μοναδική λύση στο $\mathbb{N} \times \mathbb{N}$, θα πρέπει να έχει τουλάχιστον μια λύση $(x_0, y_0) \in \mathbb{N} \times \mathbb{N}$, οπότε $c = f(x_0, y_0)$. Αφού όλες οι ακέραιες λύσεις της $f(x, y) = c$ δίνονται από τους τύπους $x = x_0 + bt$ και $y = y_0 - at$ για $t \in \mathbb{Z}$, για να είναι η λύση $(x_0, y_0) \in \mathbb{N} \times \mathbb{N}$ μοναδική πρέπει και αρκεί οι $(x_0 - b, y_0 + a)$ και $(x_0 + b, y_0 - a)$ να μην ανήκουν στο $\mathbb{N} \times \mathbb{N}$, δηλαδή να έχουμε $x_0 < b$ και $y_0 < a$.

(30) Το (α) προκύπτει άμεσα από το γεγονός ότι το (a, b) είναι λύση της $x^2 + y^2 = n$ αν και μόνο αν το ίδιο ισχύει για τα $(\pm a, \pm b)$. Για το (β) παρατηρήστε ότι αν το $(a, b) \in \mathbb{Z}^2$ είναι λύση της $x^2 + y^2 = n$, τότε το $(a + b, a - b) \in \mathbb{Z}^2$ είναι λύση της $x^2 + y^2 = 2n$. Αντιστρόφως, δείξτε ότι για κάθε λύση $(c, d) \in \mathbb{Z}^2$ της $x^2 + y^2 = 2n$ έχουμε $(c, d) = (a + b, a - b)$ για μια μοναδική λύση $(a, b) \in \mathbb{Z}^2$ της $x^2 + y^2 = n$ και συμπεράνετε το ζητούμενο. Για το (γ), γράφουμε τις λύσεις της εξίσωσης ως διανύσματα-στήλες $(a\ b)^t \in \mathbb{Z}^2$ και παρατηρούμε ότι αν $z = (a\ b)^t \in \mathbb{Z}^2$ είναι λύση, τότε το ίδιο ισχύει για το διάνυσμα

$$Pz = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -b \\ a+b \end{pmatrix},$$

όπου

$$P = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Θεωρούμε τώρα δύο λύσεις $z, w \in \mathbb{Z}^2$ ισοδύναμες αν $w = P^k z$ για κάποιο $k \in \mathbb{Z}$ και παρατηρούμε (εξηγήστε πώς) ότι η σχέση αυτή είναι μια καλά ορισμένη σχέση ισοδυναμίας στο σύνολο των λύσεων, αφού ο P είναι αντιστρέψιμος. Βρίσκουμε τέλος ότι $P^6 = I$ και ότι ο πίνακας $P^k - I$ είναι αντιστρέψιμος για κάθε $k \in \{1, 2, 3, 4, 5\}$ και συμπεραίνουμε ότι κάθε κλάση ισοδυναμίας αποτελείται από ακριβώς έξι στοιχεία $z, Pz, P^2z, P^3z, P^4z, P^5z$, δηλαδή διανύσματα της μορφής

$$\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} -b \\ a+b \end{pmatrix}, \begin{pmatrix} -a-b \\ a \end{pmatrix}, \begin{pmatrix} -a \\ -b \end{pmatrix}, \begin{pmatrix} b \\ -a-b \end{pmatrix}, \begin{pmatrix} a+b \\ -a \end{pmatrix}.$$

Έπεται ότι το πλήθος των ακέραιων λύσεων (το οποίο είναι πεπερασμένο) είναι ίσο με έξι φορές το πλήθος των κλάσεων ισοδυναμίας και επομένως διαιρείται με το 6.

(31) Μοναδική λύση είναι η τετριμμένη $x = y = 0$. Γράψτε τη δοσμένη εξίσωση ως $x^3(x^2 + 1) = y^2$. Δείξτε ότι $\mu\kappa\delta(x^3, x^2 + 1) = 1$ και συμπεράνετε το $x^2 + 1$ είναι τετράγωνο ακεραίου και συνεπώς ότι $x = 0$.

(32) Δείξτε ότι για κάθε θετικό ακέραιο n υπάρχει η λύση $x = y = 2n-1$ και $z = 2n$. Προφανώς, δεν υπάρχουν λύσεις για $n = 0$.

(33) Για τα (α) και (β), θα δείξουμε ότι η μέγιστη τιμή του z είναι ίση με $p(p + 2)$ και η ελάχιστη ίση με 4 αν $p = 2$, και με p διαφορετικά. Πράγματι, η εξίσωση

γράφεται ισοδύναμα

$$z = \frac{p(x+y)}{xy-p}$$

και αφού $xyz = p(x+y+z) \leq 3pz$, έχουμε $p+1 \leq xy \leq 3p$. Διακρίνουμε τις περιπτώσεις $p \mid xy$ και $p \mid z$. Στην πρώτη περίπτωση έχουμε είτε $xy = 2p$ και $z = x+y$, είτε $xy = 3p$ και $z = (x+y)/2$. Προκύπτουν οι τριάδες $(x,y,z) = (1,2p,2p+1)$ και $(x,y,z) = (2,p,p+2)$, καθώς και η $(3,3,3)$ για $p = 3$ (εξηγήστε γιατί). Στη δεύτερη περίπτωση θέτουμε $z = np$ για κάποιο θετικό ακέραιο n, οπότε $x+y = n(xy-p)$. Γράφοντας την τελευταία ισότητα ως

$$(n-1)xy + (x-1)(y-1) = np+1$$

και λαμβάνοντας υπόψην ότι $p+1 \leq xy$ συμπεραίνουμε ότι $(n-1)(p+1) \leq np+1$, από όπου προκύπτει ότι $n \leq p+2$, δηλαδή $z \leq p(p+2)$. Η μέγιστη τιμή του z πιστοποιείται από τη λύση $x = 1$, $y = p+1$ και $z = p(p+2)$. Για την ελάχιστη τιμή $z = p$ θα πρέπει $(x-1)(y-1) = p+1$ και πράγματι, υπάρχει η λύση $x = 3$, $y = (p+3)/2$ και $z = p$ με $x \leq y \leq z$, με την προϋπόθεση ότι $p \geq 3$. Για το (γ), από την ανάλυσή μας προκύπτουν οι λύσεις $(3,3,3)$, $(2,3,5)$, $(1,6,7)$, $(1,5,9)$, $(2,2,12)$ και $(1,4,15)$.

(34) Το (β) μπορεί να απαντηθεί χρησιμοποιώντας το (α) και την παρατήρηση ότι κάθε μετάθεση των συντεταγμένων μιας λύσης της εξίσωσης είναι επίσης λύση. Έτσι, αρχίζοντας από την προφανή λύση $(1,1,0)$, βρίσκουμε τις $(1,1,2)$, $(1,2,3)$, $(2,3,11)$, $(3,11,64)$ και $(11,64,1405)$.

(35) Θα δείξουμε ότι οι λύσεις δίνονται από τους τύπους

$$\begin{aligned} x &= \lambda u^2 \\ y &= \lambda v^2 \\ z &= \lambda(u \pm v)^2 \end{aligned}$$

όπου $\lambda, u, v \in \mathbb{Z}$. Ορίζοντας ως λ το μέγιστο κοινό διαιρέτη των x,y,z ή τον αντίθετο αυτού (και παραβλέποντας την τετριμμένη λύση $x = y = z = 0$) ανάγουμε το πρόβλημα στην περίπτωση στην οποία $\mu\kappa\delta(x,y,z) = 1$ και ένας τουλάχιστον από τους x,y,z είναι θετικός ακέραιος. Γράφοντας τη δοσμένη εξίσωση στη μορφή $(z-x-y)^2 = 4xy$ οδηγούμαστε στο συμπέρασμα ότι το xy είναι ίσο με το τετράγωνο ενός ακεραίου. Λόγω συμμετρίας, το ίδιο ισχύει για τα xz και yz. Από αυτά και την Άσκηση 26 (α) προκύπτει καθένας από τους x,y,z είναι μη αρνητικός ακέραιος και μάλιστα ίσος με το τετράγωνο ακεραίου. Γράφοντας $x = u^2$, $y = v^2$ και $z = w^2$, η ισότητα $(z-x-y)^2 = 4xy$ παίρνει τη μορφή $w^2 - u^2 - v^2 = \pm 2uv$ ή, ισοδύναμα, $\pm w = u \pm v$ και δίνει τις λύσεις $x = u^2$, $y = v^2$ και $z = (u \pm v)^2$, όπως το θέλαμε.

(36) Χρησιμοποιώντας το Θεμελιώδες Θεώρημα της Αριθμητικής και βασικές ιδιότητες των πρώτων αριθμών, δείξτε ότι το (α) ισχύει εάνν ο m είναι ελεύθερος τετραγώνων (δηλαδή δε διαιρείται με το τετράγωνο ενός πρώτου αριθμού). Ομοίως, δείξτε ότι το (β) ισχύει αν ο m είναι πρώτος, ή $m = 2p$ για κάποιο περιττό πρώτο p. Διαφορετικά, είτε ο m δεν είναι ελεύθερος τετραγώνων, είτε $m = pqt$ για κάποιους διακεκριμένους περιττούς πρώτους p,q και κάποιο γινόμενο t διακεκριμένων πρώτων διάφορων των p,q. Στην πρώτη περίπτωση δεν ισχύει το (α), άρα ούτε και το (β). Στη δεύτερη περίπτωση δείξτε ότι για $a = (p+q)/2 \cdot t$ και $b = (p-q)/2 \cdot t$, οπότε $a+b = pt$ και $a-b = qt$, έχουμε $a^2 \equiv b^2 \pmod{m}$ αλλά $a \not\equiv \pm b \pmod{m}$ και συμπεράνετε ότι και πάλι δεν ισχύει το (β).

(37) Ο ακέραιος $23^m - 3^m - 5^n$ είναι ισότιμος με 3 (mod 4) για όλα τα $m,n \in \mathbb{N}$ και διαιρείται με το 5 για όλα τα $m,n \in \mathbb{N}$ με $n \geq 1$. Από την πρώτη παρατήρηση προκύπτει ότι ο $23^m - 3^m - 5^n$ δε λαμβάνει τις τιμές 0, 5 ή 10. Αφού για $n = 0$ η

μικρότερη μη αρνητική τιμή του είναι προφανώς το 19, το ζητούμενο ελάχιστο είναι το 15, το οποίο λαμβάνεται για $m = n = 1$.

(38) Το μόνο ζεύγος $(m, n) \in \mathbb{N}^2$ με αυτή την ιδιότητα είναι το $(0, 2)$. Πράγματι, παρατηρούμε ότι $3^m \cdot 5^{m+1} = 5 \cdot 15^m \equiv 5 \cdot (-1)^m \equiv \pm 5 \pmod 8$ και ότι $2^n + 1 \equiv 1 \pmod 8$ για $n \geq 3$. Από αυτά συμπεραίνουμε ότι θα πρέπει $n \leq 2$ και καταλήγουμε στο μοναδική λύση $m = 0$ και $n = 2$.

(39) Για $x, y \in \mathbb{Z}$, τα δυνατά υπόλοιπα της διαίρεσης του x^3 με το 13 είναι τα 0, 1, 5, 8, 12 και του y^4 με το 13 είναι τα 0, 1, 3, 9 (εξηγήστε γιατί). Κατά συνέπεια, τα δυνατά υπόλοιπα της διαίρεσης του $x^3 + y^4$ με το 13 είναι τα 0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12. Άρα, κανένας ακέραιος ισότιμος με 7 modulo 13 δεν μπορεί να γραφεί στη μορφή $x^3 + y^4$.

(40) Παρατηρούμε ότι $2^n \equiv (-1)^n \pmod 3$. Άρα, αν ο n είναι άρτιος, τότε $2^n = 3q+1$ για κάποιο $q \in \mathbb{N}$ και συνεπώς $3^{2^n} = 3^{3q+1} \equiv 3 \pmod{13}$. Αν ο n είναι περιττός, τότε $2^n = 3q + 2$ για κάποιο $q \in \mathbb{N}$ και συνεπώς $3^{2^n} = 3^{3q+2} \equiv 9 \pmod{13}$. Σε κάθε περίπτωση, $3^{2^n} + 3^{2^{n+1}} \equiv 12 \equiv -1 \pmod{13}$. Απάντηση για το δεύτερο ερώτημα: όλα τα θετικά ακέραια πολλαπλάσια του 26.

(41) Χρησιμοποιήστε την ταυτότητα $a^{m^n} - 1 = (a^{m^{n-1}} - 1)(1 + a^{m^{n-1}} + a^{2m^{n-1}} + \cdots + a^{(m-1)m^{n-1}})$ και εφαρμόστε επαγωγή στο n.

(42) Για $n \in \mathbb{N}$, έστω $f(n) \in \{0, 1, \ldots, m-1\}$ το υπόλοιπο της διαίρεσης του F_n με το m. Θεωρούμε τα m^2+1 ζεύγη $(f(1), f(2)), (f(2), f(3)), \ldots, (f(m^2+1), f(m^2+2))$. Αφού υπάρχουν ακριβώς m^2 ζεύγη $(a, b) \in \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, m-1\}$ υπολοίπων (mod m), δύο από τα ζεύγη που θεωρήσαμε πρέπει να είναι ίσα. Δηλαδή, έχουμε $(f(i), f(i+1)) = (f(j), f(j+1))$ για κάποια $1 \leq i < j \leq m^2 + 1$ ή, ισοδύναμα,

$$F_i \equiv F_j \pmod m,$$
$$F_{i+1} \equiv F_{j+1} \pmod m.$$

Μάλιστα μπορούμε να υποθέσουμε ότι $i = 1$, αφού διαφορετικά, από τις δύο παραπάνω ισοτιμίες και από την αναδρομική σχέση $F_{n-1} = F_{n+1} - F_n$ προκύπτει διαδοχικά ότι

$$F_{i-1} \equiv F_{j-1} \pmod m,$$
$$F_{i-2} \equiv F_{j-2} \pmod m,$$

και ούτω καθεξής. Συμπερασματικά, θέτοντας $r = j - i$, οπότε $1 \leq r \leq m^2$, έχουμε $F_{r+1} \equiv F_1 \pmod m$ και $F_{r+2} \equiv F_2 \pmod m$. Με επαγωγή στο n προκύπτει ότι $F_{r+n} \equiv F_n \pmod m$ για κάθε θετικό ακέραιο n και συνεπώς ισχύει το (β). Για το (α), αρκεί να παρατηρήσει κανείς ότι $F_r = F_{r+2} - F_{r+1} \equiv F_2 - F_1 = 0 \pmod m$, δηλαδή ότι το F_r διαιρείται με το m.

(43) Τα δυνατά υπόλοιπα στο (α) είναι τα 1, 2 και 3, αφού για $a \equiv 0, 1, 2, 3, 4 \pmod 5$ έχουμε $a^2 + a + 1 \equiv 1, 3, 2, 3, 1 \pmod 5$, αντίστοιχα. Για το (β), γράψτε τη δοσμένη εξίσωση στη μορφή $x^2 + x + 1 = y^5 - y$ και εφαρμόστε το (α) και το Θεώρημα του Fermat για να δείξετε ότι δεν υπάρχουν ακέραιες λύσεις.

(44) Το ζητούμενο είναι φανερό για $n = 1$. Ας υποθέσουμε ότι $n \geq 2$ και ότι υπάρχει θετικός ακέραιος k με $a^k \equiv -1 \pmod{2^n}$. Τότε, οι a και k είναι περιττοί αριθμοί, αφού $a^k \equiv 0 \pmod 2$ για κάθε άρτιο $a \in \mathbb{Z}$ και $a^2 \equiv 1 \pmod 4$ για κάθε περιττό. Μας δίνεται η σχέση $2^n \mid a^k + 1 = (a+1)(a^{k-1} - a^{k-2} + \cdots - a + 1)$. Αφού όμως ο $a^{k-1} - a^{k-2} + \cdots - a + 1$ είναι περιττός αριθμός (εξηγήστε γιατί), θα πρέπει να έχουμε $2^n \mid (a + 1)$, δηλαδή $a \equiv -1 \pmod{2^n}$. Το αντίστροφο είναι τετριμμένο.

(45) Για το (α) χρησιμοποιήστε την ταυτότητα $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$ και την παρατήρηση ότι αν $x \equiv y \pmod n$, τότε $x^{n-1} + x^{n-2}y + \cdots + y^{n-1} \equiv nx^{n-1} \equiv 0 \pmod n$. Από αυτό συνάγουμε ότι αν $x \equiv a \pmod n$ και $y \equiv b \pmod n$, όπου $a, b \in \{0, 1, \ldots, n-1\}$, τότε $x^n + y^n \equiv a^n + b^n \pmod{n^2}$. Αφού η παράσταση

$a^n + b^n$ λαμβάνει το πολύ $n(n+1)/2 < n^2$ τιμές για $a, b \in \{0, 1, \ldots, n-1\}$ (εξηγήστε γιατί), έπεται το (β).

(46) Για το (α), αφού $2^7 - 2^3 = 2^3 \cdot 3 \cdot 5$, αρκεί να δείξουμε ότι το $n^7 - n^3 = n^3(n^4 - 1)$ διαιρείται με καθέναν από τους 3, 5 και 8. Αυτό προκύπτει από το Θεώρημα του Euler, αφού $\varphi(d) \mid 4$ για $d \in \{3, 5, 8\}$. Για παράδειγμα, έχουμε $8 \mid n^3$ αν ο n είναι άρτιος και $8 \mid n^4 - 1$ αν ο n είναι περιττός. Για το (β) εργαζόμαστε ομοίως με την παραγοντοποίηση $2^{15} - 2^3 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.

(47) Από το Θεώρημα του Euler προκύπτει (εξηγήστε πώς) ότι $(p-1) \cdot 2^{p(p-1)} + 1 \equiv p \pmod{p^2}$. Συμπεραίνουμε ότι ο αριθμός αυτός διαιρείται με το p αλλά όχι με το p^2 και, ειδικότερα, ότι δεν είναι τέλειο τετράγωνο.

(48) Πρόκειται για τους θετικούς ακεραίους που είναι σχετικώς πρώτοι προς τον a. Πράγματι, αν ο $m \in \mathbb{Z}_{>0}$ διαιρεί το $1 + a + a^2 + \cdots + a^{k-1}$ για κάποιο $k \in \mathbb{Z}_{>0}$, τότε προφανώς $\mu\kappa\delta(a, m) = 1$. Αντιστρόφως, έστω ότι $\mu\kappa\delta(a, m) = 1$ και ότι $a \geq 2$. Τότε, $\mu\kappa\delta(a, (a-1)m) = 1$ και συνεπώς, από το Θεώρημα του Euler έχουμε ότι $a^k \equiv 1 \pmod{(a-1)m}$, όπου $k = \varphi((a-1)m)$. Δείξαμε ότι

$$(a-1)m \mid a^k - 1 = (a-1)(1 + a + a^2 + \cdots + a^{k-1})$$

και συμπεραίνουμε ότι $m \mid 1 + a + a^2 + \cdots + a^{k-1}$. Η περίπτωση $a = 1$ είναι τετριμμένη.

(49) Για $p = 2$ έχουμε $n = 5$ και όντως, $5 \mid 2^5 - 2$. Ας υποθέσουμε τώρα ότι $p \geq 5$ και ας δείξουμε ότι $n \mid 2^n - 2$. Αφού $3n = 4^p - 1 = 2^{2p} - 1$, αρκεί να δείξουμε ότι $2^{2p} - 1 \mid 2^{n-1} - 1$. Για αυτό, αρκεί να δείξουμε ότι $2p \mid n - 1$ (εξηγήστε γιατί). Πράγματι, έχουμε $n - 1 = (4^p - 4)/3$ και $p \mid 4^p - 4$ από το θεώρημα του Fermat. Αφού ο p δε διαιρείται με το 3, έπεται ότι $p \mid n - 1$. Επιπλέον, αφού ο p είναι περιττός και ο $n - 1$ είναι άρτιος αριθμός, έπεται ότι $2p \mid n - 1$.

(50) Δεν υπάρχουν περιττοί πρώτοι p με την ιδιότητα (β) διότι

$$(p-1)^{p-1} \;=\; \sum_{k=0}^{p-1} \binom{p-1}{k} (-1)^{p-1-k} p^k \;\equiv\; 1 - (p-1)p \;\equiv\; p + 1 \pmod{p^2}$$

για κάθε τέτοιο p. Αντιθέτως, για το (α) δείξτε ότι $2^{p-1} \equiv 1 \pmod{p^2}$ για $p = 1093$.

(51) Για το (α), ισχυριζόμαστε ότι το $k = 3^{n-1}$ ικανοποιεί τη συνθήκη. Πράγματι, έχουμε $\varphi(3^n) = 2 \cdot 3^{n-1}$ και συνεπώς από το Θεώρημα του Euler παίρνουμε ότι

$$3^n \;\mid\; 2^{\varphi(3^n)} - 1 \;=\; 2^{2 \cdot 3^{n-1}} - 1 \;=\; (2^{3^{n-1}} - 1) \cdot (2^{3^{n-1}} + 1).$$

Αφού όμως $2^m \equiv 2 \pmod 3$ για κάθε περιττό $m \in \mathbb{N}$ (εξηγήστε γιατί), το $2^{3^{n-1}} - 1$ δε διαιρείται με το 3 και συνεπώς το 3^n πρέπει να διαιρεί το $2^{3^{n-1}} + 1$, όπως το ισχυριστήκαμε. Εργαζόμαστε με ανάλογο τρόπο για το (β) με τη διαιρετότητα

$$5^n \;\mid\; 2^{4 \cdot 5^{n-1}} - 1 \;=\; (2^{5^{n-1}} - 1) \cdot (2^{5^{n-1}} + 1) \cdot (2^{2 \cdot 5^{n-1}} + 1).$$

Παρατηρώντας ότι $2^m \equiv \pm 2 \pmod 5$ για κάθε περιττό $m \in \mathbb{N}$, συμπεραίνουμε ότι $5^n \mid (2^k + 1)$ για $k = 2 \cdot 5^{n-1}$. Για το (γ), αρκεί να δείξει κανείς ότι τα 1, 2 και 4 είναι τα μόνα δυνατά υπόλοιπα της διαίρεσης του 2^k με το 7.

(52) Θα δείξουμε ότι οι μόνοι πρώτοι με αυτή την ιδιότητα είναι οι $p = 3$ και $p = 7$. Έστω περιττός πρώτος p για τον οποίο $2^{p-1} - 1 = pm^2$ για κάποιο $m \in \mathbb{N}$. Ας γράψουμε την ισότητα αυτή ως $uv = pm^2$, όπου $u = 2^{\frac{p-1}{2}} - 1$ και $v = 2^{\frac{p-1}{2}} + 1$. Προφανώς, $\mu\kappa\delta(u, v) = 1$. Αφού ο p είναι πρώτος και διαιρεί το uv, θα διαιρεί το u ή το v. Στην πρώτη περίπτωση έχουμε $u/p \cdot v = m^2$ και $\mu\kappa\delta(u/p, v) = 1$. Από γνωστή πρόταση προκύπτει ότι οι u/p και v είναι τέλεια τετράγωνα, άρα $v = x^2$ για κάποιο $x \in \mathbb{N}$. Ομοίως, στη δεύτερη περίπτωση $u = x^2$ για κάποιο $x \in \mathbb{N}$. Αν $2^{\frac{p-1}{2}} + 1 = x^2$, τότε $2^{\frac{p-1}{2}} = x^2 - 1 = (x-1)(x+1)$ και συνεπώς οι $x - 1$

και $x+1$ είναι και οι δύο δυνάμεις του 2. Η μόνη δυνατότητα είναι η $x=3$, οπότε $(p-1)/2=3$ και $p=7$. Έστω τώρα ότι $2^{\frac{p-1}{2}}-1=x^2$. Προφανώς ο x είναι περιττός, άρα $x^2\equiv 1 \pmod 4$. Επομένως, ο $2^{\frac{p-1}{2}}$ δε διαιρείται με το 4 και υποχρεωτικά $(p-1)/2=1$, δηλαδή $p=3$.

(53) Για το (α) αρκεί να δείξουμε ότι κάθε περιττός πρώτος διαιρέτης του x^2+y^2 είναι ισότιμος με 1 (mod 4) (εξηγήστε γιατί). Πράγματι, έστω p ένας περιττός πρώτος διαιρέτης του x^2+y^2. Αφού $\mu\kappa\delta(x,y)=1$, οι x και y δε διαιρούνται με το p. Επομένως, υπάρχει ακέραιος z τέτοιος ώστε $yz\equiv 1 \pmod p$. Πολλαπλασιάζοντας την ισοτιμία $x^2+y^2\equiv 0 \pmod p$ με το z^2 βρίσκουμε ότι $(xz)^2\equiv -1 \pmod p$. Υψώνοντας στη δύναμη $(p-1)/2$ και εφαρμόζοντας το Θεώρημα του Fermat βρίσκουμε ότι $(-1)^{(p-1)/2}\equiv (xz)^{p-1}\equiv 1 \pmod p$ και συμπεραίνουμε ότι ο $(p-1)/2$ είναι άρτιος αριθμός, δηλαδή ότι $p\equiv 1 \pmod 4$. Για το (β) εφαρμόζουμε επαγωγή στο n, όπου το (α) είναι η περίπτωση $n=1$. Για το επαγωγικό βήμα, υποθέτοντας ότι το ζητούμενο ισχύει για το $n-1$, θεωρούμε περιττό πρώτο διαιρέτη p του $x^{2^n}+y^{2^n}$ και παρατηρούμε ότι ο p διαιρεί τον αριθμό $u^{2^{n-1}}+v^{2^{n-1}}$, όπου $u=x^2$ και $v=y^2$. Από την υπόθεση της επαγωγής παίρνουμε ότι $p\equiv 1 \pmod{2^n}$. Έπειτα, εργαζόμενοι όπως στο (α), βρίσκουμε ότι η ισοτιμία $r^{2^n}\equiv -1 \pmod p$ έχει λύση, υψώνουμε στη δύναμη $(p-1)/2^n$ και εφαρμόζουμε το Θεώρημα του Fermat για να δείξουμε ότι $(p-1)/2^n$ είναι άρτιος αριθμός, δηλαδή $p\equiv 1 \pmod{2^{n+1}}$.

(54) Σωστή είναι η πρόταση στο (α), αφού από την Άσκηση 53 προκύπτει ότι $a=2^n(4t+1)$ για κάποια $n,t\in\mathbb{N}$ και συνεπώς ότι $a\equiv 2^n \pmod{2^{n+2}}$. Εναλλακτικά, γράφοντας $a=x^2+y^2$ με $x,y\in\mathbb{N}$, θεωρούμε τη μέγιστη δύναμη 2^k του 2 που διαιρεί τα x και y. Έχουμε $x=2^k u$ και $y=2^k v$ για $u,v\in\mathbb{N}$ που δεν είναι και οι δύο άρτιοι αριθμοί και παρατηρούμε (εξηγήστε πώς) ότι $u^2+v^2\equiv 1 \pmod 4$ αν ένας από τους u,v είναι άρτιος, και ότι $u^2+v^2\equiv 2 \pmod 8$ αν και οι δύο είναι περιττοί για να συμπεράνουμε το ζητούμενο. Ένα αντιπαράδειγμα για το (β) είναι το $n=21$.

(55) Ας υποθέσουμε ότι ο p δε διαιρεί το a. Τότε, αφού $p\mid (a^2+ab+b^2)$, ο p δε διαιρεί ούτε το b. Παρατηρούμε πρώτα ότι $p\mid (a-b)(a^2+ab+b^2)=a^3-b^3$, δηλαδή έχουμε $a^3\equiv b^3 \pmod p$. Από το Θεώρημα του Fermat προκύπτει επίσης ότι $a^{p-1}\equiv b^{p-1}\equiv 1 \pmod p$. Αφού όμως $p-1\equiv 1 \pmod 3$, από τις ισοτιμίες $a^3\equiv b^3 \pmod p$ και $a^{p-1}\equiv b^{p-1} \pmod p$ προκύπτει ότι $a\equiv b \pmod p$. Κατά συνέπεια $3a^2\equiv a^2+ab+b^2\equiv 0 \pmod p$ από όπου έπεται ότι $p=3$, σε αντίθεση με την υπόθεση ότι $p\equiv 2 \pmod 3$. Αυτή η αντίφαση δείχνει ότι τα a και b διαιρούνται με το p.

(56) Για το (α), ας υποθέσουμε ότι $4ab-a-1=x^2$ για κάποιο $x\in\mathbb{Z}$ και ας γράψουμε την ισότητα αυτή ως $a(4b-1)=x^2+1$. Τότε, κάθε πρώτος διαιρέτης του $4b-1$ διαιρεί το x^2+1 και συνεπώς, σύμφωνα με την Άσκηση 53 (α), είναι ισότιμος με 1 (mod 4). Αυτό είναι αδύνατο, αφού $4b-1\equiv -1 \pmod 4$, και οδηγεί στο επιθυμητό συμπέρασμα. Εργαζόμαστε ομοίως για το (β), εφαρμόζοντας το αποτέλεσμα της Άσκησης 55.

(57) Για το (α) παρατηρούμε ότι αν δύο από πέντε διαδοχικούς ακεραίους έχουν κοινό διαιρέτη, τότε αυτός διαιρεί και τη διαφορά τους και συνεπώς είναι ο 2, ο 3 ή ο 4. Όμως, μεταξύ των πέντε διαδοχικών ακεραίων υπάρχουν το πολύ τρεις άρτιοι αριθμοί και ένας το πολύ από τους υπόλοιπους διαιρείται με το 3 (εξηγήστε γιατί). Άρα, μεταξύ των πέντε υπάρχει κάποιος που δε διαιρείται ούτε με το 2 ούτε με το 3. Αυτός είναι σχετικώς πρώτος προς καθέναν από τους άλλους τέσσερις. Το (β) προκύπτει με παρόμοιο σκεπτικό με το (α). Δεν ισχύει το ίδιο για είκοσι τυχαίους ακεραίους. Από το Κινέζικο Θεώρημα, το

γραμμικό σύστημα ισοτιμιών

$$\begin{aligned} x &\equiv 0 \pmod 2 \quad & x+6 &\equiv 0 \pmod 7 \quad & x &\equiv 0 \pmod{17} \\ x &\equiv 0 \pmod 3 \quad & x+7 &\equiv 0 \pmod{11} \quad & x &\equiv 0 \pmod{19} \\ x+1 &\equiv 0 \pmod 5 \quad & x+5 &\equiv 0 \pmod{13} \end{aligned}$$

έχει (μοναδική) λύση $x \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19}$ και για κάθε τέτοια λύση οι $x, x+2, x+4, \ldots, x+18$ διαιρούνται με το 2, οι $x, x+3, x+6, \ldots, x+18$ διαιρούνται με το 3, οι $x+1$, $x+6$, $x+11$ και $x+16$ διαιρούνται με το 5, οι $x+6$ και $x+13$ διαιρούνται με το 7, οι $x+7$ και $x+18$ διαιρούνται με το 11, οι $x+5$ και $x+18$ διαιρούνται με το 13, οι x και $x+17$ διαιρούνται με το 17 και οι x και $x+19$ διαιρούνται με το 19, οπότε καθένας από τους $x, x+1, \ldots, x+19$ έχει κοινό διαιρέτη με κάποιον από τους υπόλοιπους.

(58) Το (α) ισχύει για τους θετικούς ακεραίους εκτός από τους πρώτους αριθμούς και το $n = 4$. Πράγματι, είναι φανερό ότι δεν ισχύει αν ο n είναι πρώτος (εξηγήστε γιατί). Έστω ότι ο n είναι σύνθετος μεγαλύτερος του 4. Τότε, $n = ab$ για κάποιους ακεραίους $2 \le a \le b$ και οι παράγοντες του $(n-1)! = 1 \cdot 2 \cdots (n-1)$ περιέχουν τα a και b, αν $a < b$, ή τα a και $2a$, αν $a = b$. Σε κάθε περίπτωση, το $(n-1)!$ διαιρείται με το $ab = n$. Το (β) ισχύει για όλους τους θετικούς ακεραίους, εκτός των $n = 1$, $n = 4$. Πράγματι, αν ο n είναι σύνθετος μεγαλύτερος του 4, τότε από τα προηγούμενα προκύπτει (εξηγήστε πώς) ότι το $(n-1)!/n$ είναι ακέραιος αριθμός και μάλιστα άρτιος. Έστω τώρα ότι ο n είναι πρώτος. Σύμφωνα με το Θεώρημα του Wilson, έχουμε $(n-1)! = mn - 1$ για κάποιο $m \in \mathbb{N}$. Αφού το $(n-1)!$ είναι άρτιος αριθμός (για $n \neq 2$), ο m είναι περιττός και συνεπώς το ακέραιο μέρος $\lfloor (n-1)!/n \rfloor = m - 1$ είναι άρτιος αριθμός. Το (γ) ισχύει μόνο για $n \in \{2, 3, 5\}$. Πράγματι, έστω ότι $(n-1)! + 1 = n^k$ για κάποιους θετικούς ακεραίους $n \ge 6$ και k. Ας γράψουμε την προηγούμενη ισότητα ως

$$(n-2)! \;=\; n^{k-1} + \cdots + n^2 + n + 1.$$

Αφού ο $(n-1)!$ είναι άρτιος αριθμός, ο $(n-1)! + 1 = n^k$ είναι περιττός και συνεπώς ο n είναι περιττός και ο $m = n - 1$ είναι άρτιος, με $m \ge 6$. Από την απάντησή μας στο ερώτημα (α) προκύπτει ότι $n - 1 = m \mid (m-1)! = (n-2)!$ και επομένως $n-1 \mid n^{k-1} + \cdots + n^2 + n + 1$. Παρατηρώντας ότι $n^i \equiv 1 \pmod{n-1}$ για κάθε i συμπεραίνουμε ότι $n - 1 \mid k$. Τότε όμως $n^k \ge n^{n-1} > (n-1)^{n-1} + 1 > (n-1)! + 1$, σε αντίθεση με την υπόθεση.

(59) Για το (α), χρησιμοποιώντας το Θεώρημα του Wilson βρίσκουμε ότι

$$\begin{aligned} k!\,(p-k-1)! \;&=\; k! \cdot (p-k-1)(p-k-2)\cdots(p-(p-1)) \\ &\equiv\; k! \cdot (-1)^{p-1-k}\,(k+1)(k+2)\cdots(p-1) \;\equiv\; (-1)^k (p-1)! \\ &\equiv\; (-1)^{k-1} \pmod p. \end{aligned}$$

Ομοίως, από το Θεώρημα του Wilson και το (α) συνάγουμε ότι

$$-1 \equiv (p-1)! \;=\; k!\,(p-k-1)! \binom{p-1}{k} \;\equiv\; (-1)^{k-1} \binom{p-1}{k} \pmod p$$

και συμπεραίνουμε ότι ισχύει το (β).

(60) Τα (α) και (β) αφήνονται στον αναγνώστη. Το (γ) προκύπτει αναπτύσσοντας το $(f(x) + g(x))^p$ σύμφωνα με το Διωνυμικό Θεώρημα (βλέπε Άσκηση 5) και εφαρμόζοντας την Άσκηση 21 (α). Το (δ) προκύπτει με επαγωγή στο m, εφαρμόζοντας κατάλληλα τα (β) και (γ).

(61) Ας γράψουμε $m = \prod_{i=1}^r p_i^{\alpha_i}$ και $n = \prod_{i=1}^r p_i^{\beta_i}$, όπου $p_1, p_2, \ldots, p_r$ είναι διακεκριμένοι πρώτοι και $\alpha_i, \beta_i \in \mathbb{N}$. Τότε, $d = \prod_{i=1}^r p_i^{\gamma_i}$ και $D = \prod_{i=1}^r p_i^{\delta_i}$

όπου $\gamma_i = \min(\alpha_i, \beta_i)$ και $\delta_i = \max(\alpha_i, \beta_i)$ για κάθε i. Παρατηρώντας ότι $\{\alpha_i, \beta_i\} = \{\gamma_i, \delta_i\}$ για κάθε i, από την πολλαπλασιαστικότητα της f παίρνουμε

$$f(m)f(n) \;=\; \prod_{i=1}^{r} f(p_i^{\alpha_i}) \prod_{i=1}^{r} f(p_i^{\beta_i}) \;=\; \prod_{i=1}^{r} f(p_i^{\gamma_i}) \prod_{i=1}^{r} f(p_i^{\delta_i}) \;=\; f(d)f(D).$$

(62) Έστω $m, n \in \mathbb{Z}_{>0}$ με $\mu\kappa\delta(m, n) = 1$. Γνωρίζουμε ότι κάθε θετικός διαιρέτης k του mn έχει τη μορφή $k = ab$ για κάποιους θετικούς διαιρέτες a και b των m και n, αντίστοιχα, και ότι $\mu\kappa\delta(a, b) = \mu\kappa\delta(m/a, n/b) = 1$. Κατά συνέπεια,

$$\begin{aligned} h(mn) \;&=\; \sum_{a|m,\, b|n} f(ab)\, g\Big(\frac{mn}{ab}\Big) \;=\; \sum_{a|m,\, b|n} f(a)f(b)\, g\Big(\frac{m}{a}\Big) g\Big(\frac{n}{b}\Big) \\ &=\; \bigg(\sum_{a|m} f(a)\, g\Big(\frac{m}{a}\Big)\bigg)\bigg(\sum_{b|n} f(b)\, g\Big(\frac{n}{b}\Big)\bigg) \;=\; h(m)h(n). \end{aligned}$$

Αυτό δείχνει ότι η h είναι επίσης πολλαπλασιαστική συνάρτηση.

(63) Για το (α) παρατηρούμε ότι αν d είναι θετικός διαιρέτης του n, τότε $d \le \sqrt{n}$ ή $n/d \le \sqrt{n}$ (εξηγήστε γιατί). Άρα, $d \in \{1, 2, \ldots, \lfloor \sqrt{n} \rfloor\}$ ή $n/d \in \{1, 2, \ldots, \lfloor \sqrt{n} \rfloor\}$ και συνεπώς το πλήθος των θετικών διαιρετών του n δεν ξεπερνά το διπλάσιο του πλήθους των στοιχείων του συνόλου $\{1, 2, \ldots, [\sqrt{n}]\}$, δηλαδή $d(n) \le 2\sqrt{n}$. Όπως προκύπτει από τα προηγούμενα, η περίπτωση της ισότητας δεν υφίσταται. Για το (β), εφαρμόζοντας το (α) βρίσκουμε (εξηγήστε πώς) ότι οι μόνες λύσεις είναι οι $n = 4$ και $n = 6$.

(64) Το (α) προκύπτει εφαρμόζοντας την Άσκηση 62 στις συναρτήσεις $f(n) = n^\alpha$ και $g(n) = 1$ για κάθε n. Για το (β), παρατηρούμε ότι

$$\sigma_{-\alpha}(n) \;=\; \sum_{k|n} \frac{1}{k^\alpha} \;=\; \frac{1}{n^\alpha} \sum_{k|n} \Big(\frac{n}{k}\Big)^\alpha \;=\; \frac{1}{n^\alpha} \sum_{k|n} k^\alpha \;=\; \frac{\sigma_\alpha(n)}{n^\alpha},$$

όπου η τρίτη ισότητα οφείλεται στο γεγονός ότι όταν ο k διατρέχει τους θετικούς διαιρέτες του n, το ίδιο συμβαίνει για τον n/k. Για το (γ), εφαρμόζοντας την Άσκηση 62 και το αποτέλεσμα του (α), βρίσκουμε ότι το δοσμένο άθροισμα, έστω $h(n)$, είναι πολλαπλασιαστική συνάρτηση του n. Υπολογίζουμε ότι $h(p^m) = \sigma_\alpha(1) - \sigma_\alpha(p) = -p^\alpha$ για κάθε δύναμη p^m πρώτου αριθμού p και συμπεραίνουμε ότι αν $n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ είναι η κανονική ανάλυση του n σε γινόμενο δυνάμεων πρώτων αριθμών, τότε

$$\sum_{k|n} \mu(k)\sigma_\alpha(k) \;=\; (-1)^r (p_1 p_2 \cdots p_r)^\alpha.$$

Για το (δ) εργαζόμαστε ομοίως, ή υπολογίζουμε απευθείας ότι

$$\begin{aligned} \sum_{k|n} \varphi(k)\sigma_\alpha\Big(\frac{n}{k}\Big) \;&=\; \sum_{k|n} \varphi(k) \sum_{d|(n/k)} d^\alpha \;=\; \sum_{d|n} d^\alpha \sum_{k|(n/d)} \varphi(k) \\ &=\; \sum_{d|n} d^\alpha \cdot \frac{n}{d} \;=\; n\sigma_{\alpha-1}(n), \end{aligned}$$

όπου στην τρίτη ισότητα χρησιμοποιήσαμε τη γνωστή ταυτότητα $\sum_{k|n} \varphi(k) = n$ του Gauss. Για $\alpha = 0$ και $\alpha = 1$ παίρνουμε τις ταυτότητες

$$\sum_{k|n} \varphi(k) d\Big(\frac{n}{k}\Big) \;=\; \sigma(n), \qquad \sum_{k|n} \varphi(k)\sigma\Big(\frac{n}{k}\Big) \;=\; nd(n)$$

αντίστοιχα, όπου $\sigma(n)$ είναι το άθροισμα των θετικών διαιρετών του n.

(65) Για το (α), η ανισότητα $\sigma_\alpha(n) \ge d(n)$ είναι τετριμμένη (και ισχύει ως ισότητα μόνο αν $\alpha = 0$, ή αν $n = 1$ αν $\alpha > 0$) και η $\varphi(n) \le n$ είναι άμεση συνέπεια του

ορισμού του $\varphi(n)$ (η ισότητα ισχύει μόνο για $n = 1$). Αν $n = p^m$ είναι δύναμη πρώτου αριθμού p, τότε

$$\begin{aligned}\varphi(n)d(n) &= \varphi(p^m)d(p^m) = p^{m-1}(p-1)(m+1) \geq p^{m-1}2(p-1)\\ &\geq p^{m-1}\cdot p = n\end{aligned}$$

και ισχύουν παντού ισότητες μόνο για $p = 2$ και $m = 1$. Από αυτό και την πολλαπλασιαστικότητα των συναρτήσεων φ και d προκύπτει ότι $\varphi(n)d(n) \geq n$ για κάθε $n \in \mathbb{Z}_{>0}$. Όπως φαίνεται από τα προηγούμενα, η ισότητα ισχύει μόνο για $n \in \{1, 2\}$. Ομοίως για το (β), η ανισότητα $\sigma_\alpha(n) \geq n^\alpha$ είναι τετριμμένη (η ισότητα ισχύει μόνο για $n = 1$) και αν $n = p^m$ είναι δύναμη πρώτου αριθμού p και $\alpha \geq 1$, τότε

$$\begin{aligned}\varphi(n)\sigma_\alpha(n) &= \varphi(p^m)\sigma_\alpha(p^m) = (p-1)p^{m-1}\,\frac{p^{\alpha(m+1)}-1}{p^\alpha-1}\\ &= (p-1)p^{m-1}\,\frac{p^{\alpha m}-1/p^\alpha}{1-1/p^\alpha} < (p-1)p^{m-1}\frac{p^{\alpha m}}{1-1/p}\\ &= p^m\cdot p^{\alpha m} = n^{\alpha+1}.\end{aligned}$$

Λόγω της πολλαπλασιαστικότητας των φ και σ_α συμπεραίνουμε ότι $\varphi(n)\sigma_\alpha(n) \leq n^{\alpha+1}$ για κάθε $n \in \mathbb{Z}_{>0}$ και ότι η ισότητα ισχύει μόνο για $n = 1$.

(66) Αν $n \geq 6$, τότε το $n!$ διαιρείται με το $3 \cdot 6$ και συνεπώς για τη μεγαλύτερη δύναμη 3^k του 3 που διαιρεί το $n!$ έχουμε $k \geq 2$. Επομένως, το $\varphi(n!)$ διαιρείται με το $2 \cdot 3^{k-1}$ και άρα δεν είναι δύναμη του 2. Ομοίως βρίσκουμε ότι το $\varphi(n!)$ διαιρείται με το 5 για κάθε $n \geq 10$. Απάντηση: $n \in \{1, 2, 3, 4, 5\}$ για το (α) και $n \in \{1, 2, \ldots, 9\}$ για το (β).

(67) Σύμφωνα με το Θεώρημα αντιστροφής του Möbius, έχουμε

$$f(n) = \sum_{k|n} \varepsilon_p(k)\mu\Big(\frac{n}{k}\Big)$$

για κάθε $n \in \mathbb{Z}_{>0}$ αν και μόνο αν

$$\varepsilon_p(n) = \sum_{k|n} f(k)$$

για κάθε $n \in \mathbb{Z}_{>0}$. Αφού η τελευταία συνθήκη επαληθεύεται για

$$f(n) = \begin{cases}\beta, & \text{αν } n = 1,\\ \alpha-\beta, & \text{αν } n = p,\\ 0, & \text{διαφορετικά.}\end{cases}$$

ο τύπος αυτός εκφράζει το ζητούμενο άθροισμα ως συνάρτηση του n.

(68) Εφαρμόζοντας βασική ιδιότητα της συνάρτησης του Möbius βρίσκουμε ότι

$$\begin{aligned}\psi(n) &= \#\{(a,b) \in [n]\times[n] : \mu\kappa\delta(a,b) = 1\}\\ &= \sum_{(a,b)\in[n]\times[n]}\ \sum_{k\,|\,\mu\kappa\delta(a,b)} \mu(k)\\ &= \sum_{k=1}^{n}\mu(k)\,\#\cdot\{(a,b)\in[n]\times[n] : k \mid a,b\}\\ &= \sum_{k=1}^{n}\mu(k)\Big\lfloor\frac{n}{k}\Big\rfloor^2.\end{aligned}$$

Αυτό αποδεικνύει το (α). Για το (β), συνάγουμε από το (α) ότι

$$\lim_{n\to\infty} \frac{\psi(n)}{n^2} \;=\; \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} \;=\; \left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)^{-1} \;=\; \frac{6}{\pi^2}.$$

(69) Για το (α), δείχνουμε πρώτα ότι

$$2^{2^n} - 1 \;=\; \prod_{k=0}^{n-1} (2^{2^k} + 1)$$

με επαγωγή στο n. Από την ισότητα αυτή προκύπτει ότι $\mu\kappa\delta(2^{2^k} + 1, 2^{2^n} + 1) = 1$ για $k < n$ (εξηγήστε γιατί). Επομένως, οι παράγοντες του γινομένου του δεξιού μέλους της ισότητας είναι ανά δύο πρώτοι μεταξύ τους και η προτεινόμενη ισότητα έπεται από την πολλαπλασιαστικότητα της f. Για το (β), συμπεραίνουμε από το (α) ότι η προτεινόμενη εξίσωση είναι ισοδύναμη με την

$$\prod_{k=0}^{n-1} \varphi(2^{2^k} + 1) \;=\; 2^{2^n-1}.$$

Είναι γνωστό ότι το $2^{2^5}+1$ διαιρείται με τον πρώτο αριθμό 641. Κατά συνέπεια, το $\varphi(2^{2^5}+1)$ διαιρείται με το 640, το οποίο δεν είναι δύναμη του 2. Άρα, έχουμε υποχρεωτικά $n \le 5$. Για $k \le 4$ οι ακέραιοι $2^{2^k} + 1$ είναι πρώτοι αριθμοί και συνεπώς, για $n \le 5$

$$\prod_{k=0}^{n-1} \varphi(2^{2^k} + 1) \;=\; \prod_{k=0}^{n-1} 2^{2^k} = 2^{1+2+2^2+\cdots+2^{n-1}} \;=\; 2^{2^n-1}.$$

(70) Το δοσμένο πολυώνυμο παραγοντοποιείται ως $(x^2 + x + 1)(x^4 + x^2 + 1) = (x^2 + x + 1)^2(x^2 - x + 1)$. Οι λύσεις της $x^2 + x + 1 \equiv 0 \pmod{19}$ είναι οι 7 και 11 (mod 19) και εκείνες της $x^2 - x + 1 \equiv 0 \pmod{19}$ είναι οι -7 και -11 (mod 19), δηλαδή οι 8 και 12 (mod 19). Άρα, οι λύσεις της δοσμένης πολυωνυμικής ισοτιμίας είναι οι 7, 8, 11 και 12 (mod 19).

(71) Για το (α), για $p = 2$ υπάρχει η λύση $x \equiv 1 \pmod 2$. Έστω ότι $p \equiv 1 \pmod 4$. Γνωρίζουμε από το Θεώρημα του Fermat ότι η ισοτιμία $x^{p-1} - 1 \equiv 0 \pmod p$ έχει ακριβώς $p - 1$ λύσεις. Αφού όμως το πολυώνυμο $x^2 + 1$ διαιρεί το $x^{p-1} - 1$ (εξηγήστε γιατί), από γνωστή πρόταση προκύπτει ότι η $x^2 + 1 \equiv 0 \pmod p$ έχει ακριβώς δύο λύσεις. Το αντίστροφο αφήνεται στον αναγνώστη. Εργαζόμαστε παρόμοια για το (β), παρατηρώντας ότι το πολυώνυμο $x^2 + x + 1$ διαιρεί το $x^{p-1} - 1$ αν $p \equiv 1 \pmod 6$. Το αντίστροφο προκύπτει από το αποτέλεσμα της Άσκησης 55. Σημειώνουμε ότι το (α) συνήθως αποδεικνύεται ως εφαρμογή του Θεωρήματος του Wilson.

(72) Για την ισοδυναμία (i) $\Leftrightarrow$ (ii) αρκεί να παρατηρήσουμε ότι η απεικόνιση $f : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$ με $f(x) = x^d \pmod p$ είναι επί αν και μόνο αν είναι 1–1 (εξηγήστε γιατί). Η συνεπαγωγή (ii) $\Rightarrow$ (iii) είναι τετριμμένη. Για την (iii) $\Rightarrow$ (iv) ας υποθέσουμε ότι δεν ισχύει η συνθήκη (iv), δηλαδή ότι $\delta := \mu\kappa\delta(p - 1, d) > 1$. Αφού $\delta \mid p - 1$, γνωρίζουμε από τη θεωρία ότι η $x^\delta \equiv 1 \pmod p$ έχει ακριβώς δ λύσεις (mod p). Αφού $\delta \mid d$, αυτές είναι και λύσεις της $x^d \equiv 1 \pmod p$ και επομένως δεν ισχύει η συνθήκη (iii). Τέλος, για την (iv) $\Rightarrow$ (ii), ας υποθέσουμε ότι $\mu\kappa\delta(p - 1, d) = 1$ και ότι $x^d \equiv y^d \pmod p$. Θα δείξουμε ότι $x \equiv y \pmod p$. Αυτό είναι φανερό αν $p \mid x$. Υποθέτοντας το αντίθετο, θεωρούμε $u \in \mathbb{Z}$ με $xu \equiv y \pmod p$, έχουμε ότι $u^d \equiv 1 \pmod p$ και θέλουμε να δείξουμε ότι $u \equiv 1 \pmod p$. Πράγματι, για την τάξη k της κλάσης $u \pmod p$ έχουμε $k \mid d$ και $k \mid p - 1$ (εξηγήστε γιατί). Αφού $\mu\kappa\delta(p - 1, d) = 1$, έχουμε υποχρεωτικά $k = 1$, δηλαδή $u \equiv 1 \pmod p$.

(73) Για το (α) διακρίνετε τις περιπτώσεις $x \equiv 1 \pmod p$ και $x \not\equiv 1 \pmod p$ και εφαρμόστε την Άσκηση 72. Για το (β), υποθέστε ότι τα x, y δε διαιρούνται με το p. Θεωρήστε $u \in \mathbb{Z}$ με $xu \equiv y \pmod p$, δείξτε ότι $1 + u + u^2 + \cdots + u^{d-1} \equiv 0 \pmod p$ και εφαρμόστε το (α) για να καταλήξετε σε άτοπο. Για το (γ) υποθέστε ότι υπάρχουν πεπερασμένου πλήθους πρώτοι αριθμοί ίσοι με q ή ισότιμοι με 1 (mod p), θεωρήστε το γινόμενό τους x, επιλέξτε έναν πρώτο διαιρέτη p του $1 + x + x^2 + \cdots + x^{d-1}$ και εφαρμόστε το (α) με $d = q$ για να καταλήξετε σε άτοπο.

(74) Για το (α) παρατηρούμε ότι αν υπάρχει λύση $a \pmod{p^n}$, τότε $a^2 \equiv d \pmod p$ και συνεπώς

$$\begin{aligned} x^2 \equiv d \pmod{p^n} \quad &\Leftrightarrow \quad x^2 \equiv a^2 \pmod{p^n} \;\Leftrightarrow\; p^n \mid (x^2 - a^2) \\ &\Leftrightarrow \quad p^n \mid (x-a)(x+a). \end{aligned}$$

Τα $x - a$ και $x + a$ δε διαιρούνται και τα δύο με το p, αφού αυτό δε διαιρεί τη διαφορά τους $2a$ (εξηγήστε γιατί). Άρα, ένα από τα $x - a$ και $x + a$ διαιρείται με το p^n και συνεπώς η ισοτιμία έχει δύο ακριβώς λύσεις, τις $\pm a \pmod{p^n}$. Το ζητούμενο στο (β) προκύπτει από γνωστή πρόταση αφού για $f(x) = x^2 - d$, οι ισοτιμίες $f(x) \equiv 0 \pmod{p^n}$ και $f'(x) \equiv 0 \pmod{p^n}$ δεν έχουν κοινή λύση (εξηγήστε γιατί). Σύμφωνα με το (β), η ισοτιμία στο (γ) έχει δύο ακριβώς (αντίθετες) λύσεις, αφού η $x^2 \equiv -1 \pmod 5$ έχει τις λύσεις $x \equiv \pm 2 \pmod 5$. Με δεδομένες τις λύσεις αυτές, με τη γνωστή διαδικασία βρείτε ότι η $x^2 \equiv -1 \pmod{25}$ έχει τις λύσεις $x \equiv \pm 7 \pmod{25}$ και η $x^2 \equiv -1 \pmod{125}$ τις $x \equiv \pm 57 \pmod{125}$.

(75) Για $n = 1$, η ισοτιμία στο (α) έχει μοναδική λύση $x \equiv 1 \pmod 2$ για κάθε $k \in \mathbb{Z}_{>0}$. Για $n \geq 2$, η ισοτιμία είναι αδύνατη για άρτιους k, αφού το x^2 είναι ισότιμο με 0 ή 1 (mod 4) για κάθε $x \in \mathbb{Z}$ και, σύμφωνα με την Άσκηση 44, έχει μοναδική λύση $x \equiv -1 \pmod{2^n}$ για περιττούς k (το τελευταίο προκύπτει και από τη γενική θεωρία της $f(x) \equiv 0 \pmod{p^n}$ για $f(x) = x^k + 1$). Για την ισοτιμία στο (β), για $n = 1$ υπάρχει η μοναδική λύση $x \equiv -1 \pmod 3$. Θα δείξουμε ότι για $n \geq 2$ υπάρχει η μοναδική λύση $x \equiv -1 \pmod{3^{n-1}}$, δηλαδή ακριβώς τρεις λύσεις (mod 3^n), οι κλάσεις -1, $-1 + 3^{n-1}$ και $-1 + 2 \cdot 3^{n-1} \pmod{3^n}$. Αφήνουμε στον αναγνώστη να επαληθεύσει τον ισχυρισμό μας για $n = 2$. Ας υποθέσουμε ότι $n \geq 3$ και ας θεωρήσουμε $x \in \mathbb{Z}$ με $x \equiv -1 \pmod{3^n}$, δηλαδή τέτοιο ώστε

$$3^n \mid x^3 + 1 = (x+1)(x^2 - x + 1).$$

Αφού $x \equiv -1 \pmod 9$, από την περίπτωση $n = 2$ παίρνουμε ότι το x είναι ισότιμο με -1, 2 ή 5 (mod 9). Στις τρεις αυτές περιπτώσεις βρίσκουμε (εξηγήστε πώς) ότι $x^2 - x + 1 \equiv 3 \pmod 9$, οπότε το $x^2 - x + 1$ δε διαιρείται με το 9. Επομένως, υποχρεωτικά το $x + 1$ διαιρείται με το 3^{n-1}, δηλαδή $x \equiv -1 \pmod{3^{n-1}}$. Η ισοτιμίες στο (γ) είναι ισοδύναμη με το σύστημα

$$\begin{cases} x^{15} \equiv 1 \pmod{2^n}, \\ x^{15} \equiv 1 \pmod{3^n}. \end{cases}$$

Χρησιμοποιώντας τη θεωρία της $f(x) \equiv 0 \pmod{p^n}$, ή θεωρώντας τις δυνατές τιμές της τάξης (mod 2^n) και (mod 3^n) του x, ή με άλλο τρόπο, δείξτε ότι η πρώτη ισοτιμία έχει μοναδική λύση $x \equiv 1 \pmod{2^n}$ και η δεύτερη είναι ισοδύναμη με την $x^3 \equiv 1 \pmod{3^n}$. Η τελευταία γράφεται και $(-x)^3 \equiv -1 \pmod{3^n}$ και επομένως, σύμφωνα με το (β), έχει ακριβώς τρεις λύσεις (mod 3^n), τις κλάσεις 1, $1 + 3^{n-1}$ και $1 + 2 \cdot 3^{n-1} \pmod{3^n}$. Οδηγούμαστε στα

συστήματα

$$\begin{cases} x \equiv 1 \pmod{2^n} \\ x \equiv 1 \pmod{3^n} \end{cases} \qquad \begin{cases} x \equiv 1 \pmod{2^n} \\ x \equiv 1 + 3^{n-1} \pmod{3^n} \end{cases}$$

$$\begin{cases} x \equiv 1 \pmod{2^n} \\ x \equiv 1 + 2 \cdot 3^{n-1} \pmod{3^n}. \end{cases}$$

Δείξτε ότι οι λύσεις των συστημάτων αυτών είναι οι $x \equiv 1 \pmod{6^n}$, $x \equiv 1 + 3^{n-1}4^n \pmod{6^n}$ και $x \equiv 1 + 2 \cdot 3^{n-1}4^n \pmod{6^n}$, αντίστοιχα. Αυτές είναι και οι μοναδικές λύσεις της δοσμένης ισοτιμίας.

(76) Οι λύσεις της δοσμένης ισοτιμίας είναι εκείνες της $x^7 \equiv 1 \pmod{29}$ εκτός της $x \equiv 1 \pmod{29}$ και προφανώς το πολύ έξι σε πλήθος. Αφήνουμε στον αναγνώστη να επαληθεύσει ότι το 2 είναι πρωταρχική ρίζα (mod 29). Από αυτό προκύπτει ότι οι κλάσεις ισοτιμίας $2^{4k} \pmod{29}$ για $k \in \{1, 2, \ldots, 6\}$ είναι διακεκριμένες. Αφού $2^{28} \equiv 1 \pmod{29}$, οι κλάσεις αυτές είναι λύσεις της $x^7 \equiv 1 \pmod{29}$. Άρα, οι κλάσεις αυτές, δηλαδή οι 7, 16, 20, 23, 24 και 25 (mod 29), είναι όλες οι λύσεις της δοσμένης ισοτιμίας.

(77) Αν $p - 1 \mid n$, από το Θεώρημα του Fermat έπεται ότι $1^n + 2^n + \cdots + (p-1)^n \equiv p - 1 \pmod{p}$. Έστω ότι το n δεν είναι πολλαπλάσιο του $p - 1$ και έστω ω μια πρωταρχική ρίζα (mod p). Τότε $\omega^n \not\equiv 1 \pmod{p}$ και, αφού το $\{1, \omega, \omega^2, \ldots, \omega^{p-2}\}$ αποτελεί ένα πλήρες σύστημα αντιπροσώπων των μη μηδενικών κλάσεων ισοτιμίας (mod p),

$$\begin{aligned} (\omega^n - 1)(1^n + 2^n + \cdots + (p-1)^n) &\equiv (\omega^n - 1)(1^n + \omega^n + \omega^{2n} + \cdots + \omega^{(p-2)n}) \\ &= \omega^{n(p-1)} - 1 = \omega^{(p-1)n} - 1 \equiv 0 \pmod{p}. \end{aligned}$$

Από τα προηγούμενα έπεται ότι $1^n + 2^n + \cdots + (p-1)^n \equiv 0 \pmod{p}$.

(78) Ο μόνος ακέραιος με την ιδιότητα (α) είναι ο $m = 2$. Πράγματι, έστω ότι το $a \equiv 1 \pmod{m}$ είναι πρωταρχική ρίζα (mod m^n). Τότε, σύμφωνα με την Άσκηση 41, έχουμε $a^{m^{n-1}} \equiv 1 \pmod{m^n}$ και συνεπώς $\varphi(m^n) \leq m^{n-1}$. Δείξτε ότι αυτό ισχύει μόνο για $m = 2$. Εργαζόμαστε ανάλογα για το (β). Αν $a \equiv -1 \pmod{m}$ είναι πρωταρχική ρίζα (mod m^n), τότε $a^2 \equiv 1 \pmod{m}$ και συνεπώς $a^{2m^{n-1}} \equiv 1 \pmod{m^n}$ και $\varphi(m^n) \leq 2m^{n-1}$. Συνάγετε ότι το (β) ισχύει αν και μόνο αν $m \in \{2, 3, 4, 6\}$.

(79) Για το (α), ας υποθέσουμε ότι η τάξη της κλάσης $a \pmod{p}$ είναι άρτιος αριθμός. Από τη θεωρία γνωρίζουμε ότι η τάξη της κλάσης $a \pmod{p^n}$ είναι ακέραιο πολλαπλάσιο εκείνης της $a \pmod{p}$ και επομένως επίσης άρτιος αριθμός, έστω ίσος με $2k$. Τότε, $p^n \mid a^{2k} - 1 = (a^k - 1)(a^k + 1)$. Αφού όμως το p δε μπορεί να διαιρεί και τους δύο παράγοντες αυτού του γινομένου (εξηγήστε γιατί), έχουμε είτε $p^n \mid (a^k - 1)$, είτε $p^n \mid (a^k + 1)$ και η πρώτη περίπτωση αποκλείεται διότι το a θα είχε τάξη (mod p^n) μικρότερη του $2k$. Αντιστρόφως, έστω ότι $a^k \equiv -1 \pmod{p^n}$ για κάποιο $k \in \mathbb{N}$ (υποχρεωτικά θετικό αριθμό) και έστω r η τάξη της κλάσης $a \pmod{p}$. Προφανώς, έχουμε $a^k \equiv -1 \pmod{p}$ και $a^{2k} \equiv 1 \pmod{p}$. Από την πρώτη ισοτιμία προκύπτει ότι το r δε διαιρεί το k και από τη δεύτερη ότι το r διαιρεί το $2k$. Από αυτά έπεται (εξηγήστε γιατί) ότι το r είναι άρτιος αριθμός. Το (β) είναι άμεση συνέπεια του (α), αφού το $\varphi(p) = p - 1$ είναι άρτιος αριθμός. Το αντίστροφο δεν ισχύει, όπως δείχνει το παράδειγμα $a = 2$, $p = 17$ και $n = 1$.

(80) Από την ταξινόμηση των πρωταρχικών ριζών (mod m) προκύπτει (εξηγήστε πώς) ότι είτε $m = 2^k$ για κάποιο $k \geq 3$, είτε για την κανονική ανάλυση $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ του m έχουμε $r \geq 2$ και οι αριθμοί $\varphi(p_i^{\alpha_i})$ είναι όλοι άρτιοι. Στην πρώτη περίπτωση είναι γνωστό (προκύπτει με επαγωγή στο k) ότι $a^{\varphi(m)/2} = a^{2^{k-2}} \equiv 1 \pmod{m}$. Στη δεύτερη περίπτωση, το ελάχιστο κοινό πολλαπλάσιο, έστω q,

των αριθμών $\varphi(p_i^{\alpha_i})$ διαιρεί το $\varphi(m)/2$. Από το Θεώρημα του Euler παίρνουμε ότι $a^q \equiv 1 \pmod{\varphi(p^{\alpha_i})}$ για κάθε i και συμπεραίνουμε ότι $a^q \equiv 1 \pmod{m}$. Αφού το $\varphi(m)/2$ είναι πολλαπλάσιο του q, έπεται πάλι ότι $a^{\varphi(m)/2} \equiv 1 \pmod{m}$.

(81) Το ότι το 2 είναι πρωταρχική ρίζα $\pmod{3^m}$ προκύπτει άμεσα από τη θεωρία του υπολογισμού της τάξης των κλάσεων $\pmod{p^m}$. Θα δείξουμε ότι το μόνα ζεύγη (m, n) με τις επιθυμητές ιδιότητες είναι τα $(1, 3)$ και $(3, 9)$. Πράγματι, για κάθε τέτοιο ζεύγος (μπορούμε να υποθέσουμε ότι $m, n \geq 1$) έχουμε $2^n \equiv -1 \pmod{3^m}$, άρα και $2^{2n} \equiv 1 \pmod{3^m}$. Κατά συνέπεια, το $2n$ διαιρείται με την τάξη $\varphi(3^m) = 2 \cdot 3^{m-1}$ της κλάσης 2 $\pmod{3^m}$. Ειδικότερα, έχουμε $n \geq 3^{m-1}$. Δείχνουμε με επαγωγή στο m ότι $2^{3^{m-1}} \geq (2m^2 + 1)3^m$ για $m \geq 4$ και συμπεραίνουμε ότι η δοσμένη ισότητα είναι δυνατή μόνο για $m \leq 3$. Οι μόνες λύσεις με $m \leq 3$ είναι οι $m = 1$, $n = 3$ και $m = 3$, $n = 9$.

(82) Αφού $(m - x)^2 \equiv (-x)^2 = x^2 \pmod{m}$ για $x \in \{0, 1, \ldots, m - 1\}$, οι κλάσεις της μορφής $x^2 \pmod{m}$ είναι οι $0^2, 1^2, \ldots, \lfloor m/2 \rfloor^2 \pmod{m}$. Οι κλάσεις αυτές είναι ακριβώς $\lfloor m/2 \rfloor + 1$ σε πλήθος αν και μόνο αν $a^2 \equiv b^2 \pmod{m} \Rightarrow a \equiv \pm b \pmod{m}$ για $a, b \in \mathbb{Z}$. Σύμφωνα με τη λύση της Άσκησης 36, αυτό συμβαίνει αν και μόνο αν ο m είναι πρώτος ή το διπλάσιο κάποιου περιττού πρώτου αριθμού.

(83) Για το (α) γράψτε $a \equiv x^2 \pmod{m}$ για κάποιο $x \in \mathbb{Z}$ και εφαρμόστε το Θεώρημα του Euler. Για το (β), ας υποθέσουμε πρώτα ότι υπάρχει πρωταρχική ρίζα $\omega \pmod{m}$ και ας θεωρήσουμε ακέραιο a τέτοιον ώστε $a^{\varphi(m)/2} \equiv 1 \pmod{m}$. Τότε $a \equiv \omega^k \pmod{m}$ για κάποιο $k \in \mathbb{N}$ και επομένως $\omega^{k\varphi(m)/2} \equiv 1 \pmod{m}$. Αφού όμως το ω έχει τάξη $\pmod{m}$ ίση με $\varphi(m)$, θα πρέπει το $k\varphi(m)/2$ να διαιρείται με το $\varphi(m)$. Άρα, το k είναι άρτιος αριθμός και συνεπώς το $a \equiv \omega^k \pmod{m}$ είναι τετραγωνικό υπόλοιπο $\pmod{m}$. Το αντίστροφο είναι άμεση συνέπεια του αποτελέσματος της Άσκησης 80.

(84) Για το (α), επειδή οι κλάσεις των $a, b \pmod{m}$ είναι αντιστρέψιμες, η δοσμένη συνεπαγωγή είναι ισοδύναμη με τη $x^2 \equiv 1 \pmod{m} \Rightarrow x \equiv \pm 1 \pmod{m}$. Από τη γενική θεωρία της ισοτιμίας $x^2 \equiv 1 \pmod{m}$ που γνωρίζουμε προκύπτει ότι η συνεπαγωγή ισχύει εάνν $m \in \{2, 4, p^n, 2p^n\}$ για κάποιο περιττό πρώτο p και $n \in \mathbb{Z}_{>0}$ ή, ισοδύναμα, εάνν υπάρχει πρωταρχική ρίζα $\pmod{m}$. Για το (β), παρατηρούμε ότι τα τετραγωνικά υπόλοιπα $\pmod{m}$ είναι οι κλάσεις $x^2 \pmod{m}$ για τις $\varphi(m)$ τιμές του $x \in \{1, 2, \ldots, m - 1\}$ που είναι σχετικώς πρώτες προς το m. Αφού οι τιμές αυτές χωρίζονται σε ζεύγη $\{x, -x\}$ με $(-x)^2 \equiv x^2 \pmod{m}$ και $x \not\equiv -x \pmod{m}$, το πλήθος των εν λόγω κλάσεων είναι μικρότερο ή ίσο του $\varphi(m)/2$. Η ισότητα ισχύει εάνν ισχύει η συνεπαγωγή του ερωτήματος (α) και επομένως εάνν $m \in \{4, p^n, 2p^n\}$ για κάποιο περιττό πρώτο p και $n \in \mathbb{Z}_{>0}$.

(85) Για το (α) παρατηρούμε ότι αν $a \equiv x^2 \pmod{m}$ είναι τετραγωνικό υπόλοιπο $\pmod{m}$, τότε από το Θεώρημα του Euler παίρνουμε $a^{\varphi(m)/2} \equiv x^{\varphi(m)} \equiv 1 \pmod{m}$. Αυτό δείχνει ότι το a έχει τάξη $\pmod{m}$ μικρότερη ή ίση του $\varphi(m)/2$ και επομένως το a δεν είναι πρωταρχική ρίζα $\pmod{m}$. Θα δείξουμε ότι το αντίστροφο ισχύει εάνν $m \in \{4, p, 2p\}$ για κάποιο περιττό πρώτο p της μορφής $p = 2^k + 1$. Πράγματι, σύμφωνα με το (α), το αντίστροφο ισχύει εάνν το πλήθος των μη τετραγωνικών υπολοίπων $\pmod{m}$ είναι ίσο με εκείνο των πρωταρχικών ριζών $\pmod{m}$, δηλαδή (υπό την προϋπόθεση ότι τέτοιες υπάρχουν) με $\varphi(\varphi(m))$. Από την Άσκηση 84 (β) γνωρίζουμε ότι υπάρχουν τουλάχιστον $\varphi(m)/2$ μη τετραγωνικά υπόλοιπα $\pmod{m}$ και συμπεραίνουμε ότι θα πρέπει $\varphi(\varphi(m)) \geq \varphi(m)/2$. Όμως ο $\varphi(m)$ είναι άρτιος αριθμός (εξηγήστε γιατί) και, όπως προκύπτει από το γνωστό τύπο για το $\varphi(n)$, έχουμε $\varphi(n) \leq n/2$ για κάθε άρτιο θετικό ακέραιο n, όπου η ισότητα ισχύει εάνν ο n είναι δύναμη του 2. Από τα παραπάνω συνάγουμε ότι, αφού υπάρχει πρωταρχική ρίζα

(mod m), έχουμε $m \in \{4, p^n, 2p^n\}$ για κάποιο περιττό πρώτο p και $n \in \mathbb{Z}_{>0}$ και ότι το $\varphi(m)$ είναι δύναμη του 2. Από αυτά συμπεραίνουμε (εξηγήστε πώς) ότι $m \in \{4, p, 2p\}$ για κάποιο περιττό πρώτο p της μορφής $p = 2^k + 1$. Αφήνεται στον αναγνώστη να επαληθεύσει ότι, αντιστρόφως, για κάθε τέτοιο m υπάρχουν ακριβώς $\varphi(m)/2$ μη τετραγωνικά υπόλοιπα (mod m), όσα και πρωταρχικές ρίζες.

(86) Θα δείξουμε ότι ικανή και αναγκαία συνθήκη είναι τα a, b να μη διαιρούνται με το p. Πράγματι, η συνθήκη είναι αναγκαία αφού υπάρχουν μόνο $(p-1)/2$ τετραγωνικά υπόλοιπα (mod p) και συνεπώς οι ισοτιμίες $ax^2 \equiv c \pmod p$ ή $by^2 \equiv c \pmod p$ δεν μπορεί να έχουν λύση για κάθε $c \in \mathbb{Z}$. Αντιστρόφως, έστω ότι τα a, b δε διαιρούνται με το p. Τότε, για $x, y \in \mathbb{Z}$, τα ax^2 και $c - by^2$ λαμβάνουν το καθένα ακριβώς $(p+1)/2$ τιμές (mod p) (εξηγήστε γιατί). Αφού υπάρχουν μόνο p κλάσεις (mod p), έχουμε υποχρεωτικά $ax^2 \equiv c - by^2 \pmod p$ για κάποια $x, y \in \mathbb{Z}$.

(87) Για το (α) παρατηρήστε ότι $x^4 \equiv 1 \pmod p \Leftrightarrow p \mid (x-1)(x+1)(x^2+1)$ και εφαρμόστε την Άσκηση 71 (α) για να συμπεράνετε ότι οι μόνες λύσεις είναι οι $x \equiv \pm 1 \pmod p$. Για το (β), συνάγετε από το (α) ότι $x^4 \equiv y^4 \pmod p \Leftrightarrow x \equiv \pm y \pmod p$ και συμπεράνετε ότι η ισοτιμία $x^4 \equiv c \pmod p$ έχει λύση αν και μόνο αν $c \equiv 0^4, 1^4, \ldots, ((p-1)/2)^4 \pmod p$ και ότι οι κλάσεις αυτές είναι διακεκριμένες. Για το (γ) χρησιμοποιήστε το (β) και μιμηθείται τη λύση της Άσκησης 86.

(88) Θεωρούμε μια πρωταρχική ρίζα $\omega \pmod p$. Για το (α), παρατηρούμε ότι οι κλάσεις των τετραγωνικών υπολοίπων (mod p) είναι οι $\omega^2, \omega^4, \ldots, \omega^{p-1} \pmod p$. Αφού $\omega^{(p-1)/2} \equiv -1 \pmod p$ (εξηγήστε γιατί), για το γινόμενό τους βρίσκουμε ότι

$$\omega^2 \cdot \omega^4 \cdots \omega^{p-1} \;=\; \omega^{(p-1)(p+1)/4} \;\equiv\; (-1)^{(p+1)/2}$$

$$\equiv \begin{cases} 1 \pmod p, & \text{αν } p \equiv 3 \pmod 4, \\ -1 \pmod p, & \text{αν } p \equiv 1 \pmod 4. \end{cases}$$

Για το (β) χρησιμοποιήστε το (α) και την ισοτιμία $\omega \cdot \omega^2 \cdots \omega^{p-1} \equiv -1 \pmod p$, η οποία είναι ισοδύναμη με το Θεώρημα του Wilson (και φυσικά προκύπτει και με υπολογισμό ανάλογο εκείνου στο (α) για το $\omega^2 \cdot \omega^4 \cdots \omega^{p-1}$).

(89) Δείξτε πρώτα ότι η δοσμένη ισοτιμία μπορεί να γραφεί ως $(x^2 + 3x + 1)^2 \equiv 0 \pmod p$ και συμπεράνετε ότι είναι ισοδύναμη με τη $x^2 + 3x + 1 \equiv 0 \pmod p$. Συμπληρώνοντας το τετράγωνο, δείξτε ότι η τελευταία έχει λύση αν και μόνο αν το 5 είναι τετραγωνικό υπόλοιπο (mod p). Απάντηση: $p = 5$ ή $p \equiv \pm 1 \pmod{10}$.

(90) Το (α) προκύπτει άμεσα από το γεγονός ότι υπάρχουν $(p-1)/2$ τετραγωνικα υπόλοιπα (mod p) και $(p-1)/2$ τετραγωνικά μη υπόλοιπα (mod p). Για το (β), ας συμβολίσουμε με S_p το άθροισμα που ζητάμε να υπολογίσουμε (mod p) και ας θέσουμε

$$S_p^+ \;=\; \sum_{\substack{k=1 \\ (k/p)=1}}^{p-1} k, \qquad S_p^- \;=\; \sum_{\substack{k=1 \\ (k/p)=-1}}^{p-1} k.$$

Τότε, $S_p = S_p^+ - S_p^-$. Παρατηρούμε πρώτα ότι $S_p^+ + S_p^- = \sum_{k=1}^{p-1} k = p(p-1)/2 \equiv 0 \pmod p$, οπότε $S_p \equiv 2S_p^+ \pmod p$. Έπειτα, αφού τα τετραγωνικά υπόλοιπα (mod p) είναι οι κλάσεις των $1^2, 2^2, \ldots, ((p-1)/2)^2$, βρίσκουμε ότι

$$S_p \;\equiv\; 2S_p^+ \;\equiv\; 2\sum_{x=1}^{(p-1)/2} x^2 \;=\; \frac{p(p^2-1)}{12} \pmod p,$$

από όπου προκύπτει το ζητούμενο. Για το (γ), παρατηρούμε ότι

$$\left(\frac{p-k}{p}\right) = \left(\frac{-k}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{k}{p}\right) = -\left(\frac{k}{p}\right)$$

για κάθε $k \in \mathbb{Z}$ και συμπεραίνουμε ότι

$$\begin{aligned} 2\sum_{k=1}^{p-1} k^2\left(\frac{k}{p}\right) &= \sum_{k=1}^{p-1} k^2\left(\frac{k}{p}\right) + \sum_{k=1}^{p-1}(p-k)^2\left(\frac{p-k}{p}\right) \\ &= \sum_{k=1}^{p-1} k^2\left(\frac{k}{p}\right) - \sum_{k=1}^{p-1}(p-k)^2\left(\frac{k}{p}\right) \\ &= \sum_{k=1}^{p-1}(2kp-p^2)\left(\frac{k}{p}\right) = 2p\sum_{k=1}^{p-1} k\left(\frac{k}{p}\right), \end{aligned}$$

όπου για την τελευταία ισότητα χρησιμοποιήσαμε το (α). Το ζητούμενο έπεται από αυτό και το (β).

(91) Για το (α) εφαρμόστε επαγωγή στο n, ή εξισώστε τις ορίζουσες των δύο μελών της ταυτότητας

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

που αναφέρθηκε στη λύση της Άσκησης 13. Υπενθυμίζουμε τώρα το γνωστό τύπο

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1+\sqrt{5}}{2}\right)^n\right).$$

Αναπτύσσοντας τις n-οστές δυνάμεις σύμφωνα με το Διωνυμικό Θεώρημα (βλέπε μέρος (δ) της Άσκησης 5) βρίσκουμε ότι

$$\begin{aligned} F_n &= \frac{1}{2^n\sqrt{5}}\left(\sum_{k=0}^{n}\binom{n}{k}(\sqrt{5})^k - \sum_{k=0}^{n}\binom{n}{k}(-\sqrt{5})^k\right) \\ &= \frac{1}{2^{n-1}}\left(\binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \cdots\right). \end{aligned}$$

Για το (β), υποθέτοντας ότι ο p είναι περιττός, συμπεραίνουμε ότι

$$2^{p-1}F_p = \binom{p}{1} + \binom{p}{3}5 + \binom{p}{5}5^2 + \cdots + \binom{p}{p}5^{(p-1)/2}.$$

Από αυτή την ισότητα, λόγω των ισοτιμιών $2^{p-1} \equiv 1 \pmod p$ και $5^{(p-1)/2} \equiv \pm 1 \pmod p$ και του αποτελέσματος της Άσκησης 21 (α) συνάγουμε ότι $F_p \equiv \pm 1 \pmod p$. Από αυτό και την ταυτότητα του ερωτήματος (α) έπεται ότι $p \mid F_{p-1}F_{p+1}$. Για το (γ), με παρόμοιο σκεπτικό βρίσκουμε ότι

$$\begin{aligned} 2^p F_{p+1} &= \binom{p+1}{1} + \binom{p+1}{3}5 + \binom{p+1}{5}5^2 + \cdots + \binom{p+1}{p}5^{(p-1)/2} \\ &\equiv 1 + 5^{(p-1)/2} \equiv 1 + \left(\frac{5}{p}\right) = 1 + \left(\frac{p}{5}\right) \pmod p. \end{aligned}$$

Έπεται ότι $p \mid F_{p+1}$ αν και μόνο αν το p είναι τετραγωνικό μη υπόλοιπο (mod p), δηλαδή αν και μόνο αν $p \equiv \pm 2 \pmod 5$.

(92) Έστω $f(n)$ το άθροισμα αυτό. Έχουμε $f(2) = 1/2$ και συνεπώς αρκεί να δείξουμε ότι $f(n-1) = f(n)$ για κάθε $n \geq 3$. Παρατητούμε ότι το $f(n)$ προκύπτει από το $f(n-1)$ προσθέτοντας τους ρητούς της μορφής $1/pq$ με $p, q \in \{1, 2, \ldots, n\}$, $\mu\kappa\delta(p,q) = 1$ και $p = n$ ή $q = n$ και αφαιρώντας εκείνους

της μορφής $1/pq$, όπου $p, q \in \{1, 2, \ldots, n\}$, $\mu\kappa\delta(p, q) = 1$ και $p + q = n$. Όμως, για $p + q = n$ έχουμε

$$\frac{1}{p \cdot n} + \frac{1}{q \cdot n} = \frac{p+q}{p \cdot q \cdot n} = \frac{1}{p \cdot q}$$

και οι συνθήκες $\mu\kappa\delta(p, n) = 1$, $\mu\kappa\delta(q, n) = 1$ και $\mu\kappa\delta(p, q) = 1$ είναι ανά δύο ισοδύναμες. Έπεται ότι $f(n) = f(n-1)$ για $n \geq 3$.

(93) Το πρόβλημα αυτό τέθηκε στη Διεθνή Μαθηματική Ολυμπιάδα που έγινε στην Αυστραλία το 1988 με το χαρακτηρισμό του εξαιρετικά δύσκολου (και λύθηκε πλήρως από 11 διαγωνιζόμενους). Ας υποθέσουμε ότι $a \geq b > 0$ και ότι $(a^2 + b^2)/(ab + 1) = m \in \mathbb{N}$. Θεωρώντας την ισότητα αυτή ως την εξίσωση $x^2 - mbx + (b^2 - m) = 0$ στον άγνωστο $x = a$, βρίσκουμε μια δεύτερη λύση $x = c$ για την οποία έχουμε $a + c = mb$ και $ac = b^2 - m$. Από την πρώτη ισότητα έπεται ότι $c \in \mathbb{Z}$ και από τη δεύτερη ότι $c < a$, αφού $ac = b^2 - m < b^2 \leq a^2$. Επίσης, έχουμε $(b^2 + c^2)/(bc + 1) = m > 0$, άρα $c \geq 0$. Συμπερασματικά, από το ζεύγος $\{a, b\}$ θετικών ακεραίων που επαληθεύει την ισότητα $(a^2+b^2)/(ab+1) = m$ βρήκαμε ένα νέο ζεύγος $\{b, c\}$ φυσικών αριθμών, με $b + c < a + b$, που επαληθεύει την ίδια ισότητα. Αν λοιπόν, για δοσμένο m, επιλέξουμε το ζεύγος $a \geq b$ φυσικών αριθμών που επαληθεύει την ισότητα και επιτυγχάνει το ελάχιστο δυνατό άθροισμα $a + b$, τότε θα πρέπει $b = 0$, οπότε το $m = a^2$ είναι ίσο με το τετράγωνο ενός ακεραίου.

(94) Ας συμβολίζουμε με $f(m, n)$ το δοσμένο στο (α) ρητό αριθμό και ας υποθέσουμε ότι $n \geq m + 2$. Μεταξύ των ακεραίων $m + 1, m + 2, \ldots, n$ υπάρχει κάποιος, έστω ο $2^k \cdot q$, ο οποίος διαιρείται με τη μέγιστη δυνατή δύναμη 2^k του 2 (οπότε, ο q είναι περιττός). Ο ακέραιος αυτός είναι μοναδικός διότι αν $p < q$ είναι περιττοί αριθμοί, τότε μεταξύ των $2^k \cdot p$ και $2^k \cdot q$ υπάρχει ο ακέραιος $2^k \cdot (p+1)$ ο οποίος διαιρείται με το 2^{k+1}. Ας υποθέσουμε ότι $f(m, n) \in \mathbb{Z}$. Συμβολίζουμε με Q το γινόμενο όλων των περιττών αριθμών που είναι μικρότεροι ή ίσοι του n και θεωρούμε την ισότητα

$$2^k Q \cdot f(m, n) = \frac{2^k Q}{m+1} + \frac{2^k Q}{m+2} + \cdots + \frac{2^k Q}{n}.$$

Τότε, το αριστερό μέλος αυτής της ισότητας είναι άρτιος αριθμός, ενώ μεταξύ των προσθετέων του δεξιού μέλους υπάρχει ένας μόνο περιττός ακέραιος αριθμός (συγκεκριμένα, ο Q/q) και οι υπόλοιποι είναι άρτιοι ακέραιοι (εξηγήστε γιατί). Από αυτή την αντίφαση συμπεραίνουμε ότι $f(m, n) \notin \mathbb{Z}$. Με ανάλογο επιχείρημα, στο οποίο το ρόλο του $2^k \cdot (p + 1)$ παίζει το $2^k \cdot (p + a)$, προκύπτει το (β).

(95) Το (α) είναι γνωστό θεώρημα. Θα μιμηθούμε τη γνωστή του απόδειξη για να αποδείξουμε το (β). Ας υποθέσουμε πρώτα ότι $p \equiv 1 \pmod 6$. Από την Άσκηση 71 γνωρίζουμε ότι υπάρχει $r \in \mathbb{Z}$ τέτοιο $r^2 + r + 1 \equiv 0 \pmod p$. Θεωρούμε τα ζεύγη $(a, b) \in \mathbb{Z}^2$ με $0 \leq a, b \leq \lfloor \sqrt{p} \rfloor$ και τους αντίστοιχους ακεραίους $a + br$. Αφού το πλήθος των ζευγών είναι μεγαλύτερο του p (εξηγήστε γιατί), υπάρχουν δύο διαφορετικά τέτοια ζεύγη, έστω τα (a, b) και (c, d), τέτοια ώστε $a + br \equiv c + dr \pmod p$. Θέτοντας $x = a - c$ και $y = d - b$, έχουμε $x \equiv ry \pmod p$ όπου x και y είναι ακέραιοι, όχι και οι δύο ίσοι με μηδέν. Λαμβάνοντας υπόψην ότι $r^3 \equiv 1 \pmod p$, βρίσκουμε ότι $x^3 \equiv (ry)^3 \equiv y^3 \pmod p$, δηλαδή ότι το p διαιρεί το $x^3 - y^3 = (x-y)(x^2+xy+y^2)$. Παρατηρούμε τώρα ότι το p δε διαιρεί το $x - y = a + b - c - d$, αφού από τις $a + b \equiv c + d \pmod p$ και $a + br \equiv c + dr \pmod p$ προκύπτει (εξηγήστε γιατί) ότι $a \equiv c \pmod p$ και $b \equiv d \pmod p$ και κατά συνέπεια ότι $(a, b) = (c, d)$, σε αντίθεση με την επιλογή των δύο ζευγών. Επομένως, το p διαιρεί το $x^2 + xy + y^2$. Παρατηρούμε τέλος ότι $0 < x^2 + xy + y^2 < 3p$, αφού $|x|, |y| < \sqrt{p}$,

και συμπεραίνουμε ότι $x^2+xy+y^2 = p$, ή $x^2+xy+y^2 = 2p$. Η δεύτερη περίπτωση αποκλείεται λόγω του αδύνατου της ισοτιμίας $x^2 + xy + y^2 \equiv 2 \pmod 4$. Το αντίστροφο είναι άμεση συνέπεια του αποτελέσματος της Άσκησης 55.

(96) Το (α) είναι άμεση συνέπεια της ταυτότητας

$$(a^2 + kab + b^2)(c^2 + kcd + d^2) \;=\; x^2 + kxy + y^2,$$

όπου $x = ac - bd$ και $y = ad + bc + kbd$. Για το (β), θεωρήστε τυχαίο θετικό διαιρέτη d του u. Χρησιμοποιώντας τα αποτελέσματα των Ασκήσεων 53 (α), 55 και 95, δείξτε ότι κάθε πρώτος διαιρέτης του d ανήκει στο $\mathcal{M}_k$ και συνάγετε από το (α) ότι $d \in \mathcal{M}_k$. Το ερώτημα (γ) έχει αρνητική απάντηση. Για παράδειγμα, για $k = 4$, $a = 4$, $b = 5$ έχουμε $a^2 + kab + b^2 = 121 \in \mathcal{M}_4$ αλλά ο διαιρέτης 11 του 121 δεν ανήκει στο $\mathcal{M}_4$ (εξηγήστε γιατί).

(97) Για το (α), παρατηρούμε πρώτα ότι κάθε πολυώνυμο $p(x)$ με πραγματικούς συντελεστές γράφεται στη μορφή

$$p(x) \;=\; c_0 + c_1\binom{x}{1} + c_2\binom{x}{2} + \cdots + c_n\binom{x}{n}$$

για κάποια $n \in \mathbb{N}$ και $c_0, c_1, \ldots, c_n \in \mathbb{R}$ (εξηγήστε γιατί). Έστω ότι το $p(x)$ έχει την ιδιότητα $x \in \mathbb{Z} \Rightarrow p(x) \in \mathbb{Z}$. Τότε, το πολυώνυμο $\Delta p(x) := p(x + 1) - p(x)$ έχει την ίδια ιδιότητα και προφανώς $c_0 = p(0) \in \mathbb{Z}$. Αφού

$$\Delta p(x) \;=\; c_1 + c_2\binom{x}{1} + \cdots + c_n\binom{x}{n-1}$$

(εξηγήστε γιατί), εφαρμόζοντας επαγωγή στο n προκύπτει ότι $c_1, \ldots, c_n \in \mathbb{Z}$. Το αντίστροφο είναι άμεση συνέπεια της Άσκησης 5 (β). Το ερώτημα (β) έχει αρνητική απάντηση. Πράγματι, έστω ότι υπάρχει τέτοιο πολυώνυμο $p(x)$. Τότε, η ακολουθία των $p(m) \pmod 2$ για $m \in \mathbb{N}$ είναι η $(0, 0, 1, 0, 0, 1, \ldots)$. Κατά συνέπεια, για το πολυώνυμο $\Delta p(x)$ η αντίστοιχη ακολουθία είναι η $(0, 1, 1, 0, 1, 1, \ldots)$, για το $\Delta^2 p(x) = \Delta(\Delta p(x))$ είναι η $(1, 0, 1, 1, 0, 1, \ldots)$, για το $\Delta^3 p(x)$ είναι η $(1, 1, 0, 1, 1, 0, \ldots)$ και ούτε καθεξής. Από αυτά συμπεραίνουμε ότι το $\Delta^k p(x)$ είναι μη μηδενικό πολυώνυμο για κάθε $k \in \mathbb{N}$, πράγμα αδύνατο αφού ο τελεστής Δ μικραίνει το βαθμό του πολυωνύμου κατά ένα (εξηγήστε γιατί). Από την αντίφαση αυτή προκύπτει το επιθυμητό συμπέρασμα.

(98) Από την Άσκηση 71 (α) γνωρίζουμε ότι το γινόμενο στο (α) διαιρείται με το p, αν $p = 2$ ή $p \equiv 1 \pmod 4$. Έστω ότι $p \equiv 3 \pmod 4$. Θα χρησιμοποιήσουμε κάποιες γνώσεις άλγεβρας για να δείξουμε ότι το ζητούμενο υπόλοιπο είναι ίσο με 4. Θεωρούμε το δακτύλιο πηλίκο (ο οποίος είναι σώμα) $F = \mathbb{Z}_p[t]\,/\langle t^2 + 1\rangle$ που προκύπτει προσαρτώντας μια ρίζα ω του πολυωνύμου $t^2 + 1$ στο σώμα $\mathbb{Z}_p$ (ώστε ω είναι η κλάση του t στο πηλίκο) και τον πολυωνυμικό δακτύλιο $F[x]$ στη μεταβλητή x (πολυώνυμα με συντελεστές από το F). Αφού το F έχει χαρακτηριστική p, το πολυώνυμο $f(x) = x^p - x \in F[x]$ παραγοντοποιείται στο $F[x]$ κατά τα γνωστά ως

$$f(x) \;=\; x(x-1)\cdots(x-p+1) \;=\; \prod_{k=1}^{p}(x+k).$$

Αφού $\omega^2 = -1$ στο F, οπότε $x^2 + 1 = x^2 - \omega^2 = (x - \omega)(x + \omega)$ στο $F[x]$, υπολογίζουμε ότι

$$\begin{aligned}\prod_{k=1}^{p}(k^2+1) &= \prod_{k=1}^{p}(k-\omega)(k+\omega) = \prod_{k=1}^{p}(k-\omega)\prod_{k=1}^{p}(k+\omega)\\ &= f(-\omega)f(\omega) = ((-\omega)^p+\omega)\cdot(\omega^p-\omega) = -(\omega^p-\omega)^2\\ &= 2+2\omega^{p+1}\end{aligned}$$

στο F, όπου χρησιμοποιήσαμε την ισότητα $\omega^2 = -1$. Αφού $p \equiv 3 \pmod 4$, έχουμε $\omega^{p+1} = 1$ και το γινόμενο είναι ίσο με 4 στο F, άρα και στο $\mathbb{Z}_p$. Για το (β) εργαζόμαστε ομοίως με το δακτύλιο $F = \mathbb{Z}_p[t]/\langle t^2 + t + 1\rangle$ και την παραγοντοποίηση $x^2 + x + 1 = (x - \omega)(x - \omega^2)$ στο $F[x]$, όπου $\omega^2 + \omega + 1 = 0$, και βρίσκουμε ότι το ζητούμενο υπόλοιπο είναι ίσο με μηδέν, αν $p = 3$ ή $p \equiv 1 \pmod 3$ και με 3, αν $p \equiv 2 \pmod 3$.