Λύσεις Θεμάτων Θεωρίας Αριθμών Σεπτεμβρίου

1. **(α)** *Να δειχθεί ότι για οποιουσδήποτε ακεραίους A, B, C ισχύει*

$$\min(A+B, B+C, C+A) + \max(A, B, C) = A + B + C.$$

(β) *Χρησιμοποιώντας το* **(α)** *να δειχθεί ότι*

$$(ab, bc, ca)[a, b, c] = abc.$$

(1+1 μονάδες)

Απόδειξη. **(α)** Χωρίς περιορισμό της γενικότητας θεωρούμε $A \leqslant B \leqslant C$, καθώς και τα δύο μέλη είναι συμμετρικά ως προς A, B, C. Άρα $\min(A+B, B+C, C+A) = A+B$ και $\max(A, B, C) = C$, και το ζητούμενο προκύπτει εύκολα.

(β) Θεωρούμε τις πρωτογενείς αναλύσεις των a, b, c:

$$\begin{aligned} a &= p_1^{\alpha_1} \cdots p_n^{\alpha_n} \\ b &= p_1^{\beta_1} \cdots p_n^{\beta_n} \\ c &= p_1^{\gamma_1} \cdots p_n^{\gamma_n} \end{aligned}$$

όπου $p_1, \ldots, p_n$ είναι *όλοι* οι πρώτοι που διαιρούν τουλάχιστον έναν από τους a, b, c, και τα α_i, β_i, γ_i είναι $\geqslant 0$. Επομένως

$$[a, b, c] = p_1^{\max(\alpha_1, \beta_1, \gamma_1)} \cdots p_n^{\max(\alpha_n, \beta_n, \gamma_n)}.$$

Επίσης

$$\begin{aligned} ab &= p_1^{\alpha_1+\beta_1} \cdots p_n^{\alpha_n+\beta_n} \\ bc &= p_1^{\beta_1+\gamma_1} \cdots p_n^{\beta_n+\gamma_n} \\ ca &= p_1^{\gamma_1+\alpha_1} \cdots p_n^{\gamma_n+\alpha_n} \end{aligned}$$

οπότε

$$(a, b, c) = p_1^{\min(\alpha_1+\beta_1, \beta_1+\gamma_1, \gamma_1+\alpha_1)} \cdots p_n^{\min(\alpha_n+\beta_n, \beta_n+\gamma_n, \gamma_n+\alpha_n)}$$

άρα

$$(ab, bc, ca)[a, b, c] = p_1^{\min(\alpha_1+\beta_1, \beta_1+\gamma_1, \gamma_1+\alpha_1)+\max(\alpha_1, \beta_1, \gamma_1)} \cdots p_n^{\min(\alpha_n+\beta_n, \beta_n+\gamma_n, \gamma_n+\alpha_n)+\max(\alpha_n, \beta_n, \gamma_n)}$$

και χρησιμοποιώντας το **(α)** για τους εκθέτες α_i, β_i, γ_i προκύπτει πως το δεξί μέλος της παραπάνω ισότητας ισούται με

$$p_1^{\alpha_1+\beta_1+\gamma_1} \cdots p_n^{\alpha_n+\beta_n+\gamma_n} = abc.$$

□

2. *Να δειχθεί ότι για κάθε φυσικό n ισχύει*

$$15 \mid 2^{4n+2} + 7^{4n+1} + 4.$$

(1 μονάδα)

Απόδειξη. Θέτουμε $A_n = 2^{4n+2} + 7^{4n+1} + 4$. Ισχύει $A_0 = 15$, οπότε το ζητούμενο ισχύει για $n = 0$. Ας υποθέσουμε πως ισχύει για $n = k$, δηλαδή $15 \mid A_k$, και θέλουμε να δείξουμε πως $15 \mid A_{k+1}$. Ισοδύναμα, αρκεί να δειχθεί πως $15 \mid A_{k+1} - A_k$:

$$\begin{aligned} A_{k+1} - A_k &= 2^{4n+6} + 7^{4n+5} + 4 - 2^{4n+2} - 7^{4n+1} - 4 \\ &= 2^{4n+2}(2^4 - 1) + 7^{4n+1}(7^4 - 1) \\ &= 15 \cdot 2^{4n+2} + 2400 \cdot 7^{4n+1} \end{aligned}$$

$$15 \cdot (2^{4n+2} + 160 \cdot 7^{4n+1}),$$

αποδεικνύοντας το ζητούμενο. □

3. **(α)** *Έστω $\omega : \mathbb{N} \to \mathbb{N}$ η αριθμητική συνάρτηση που ορίζεται ως εξής:*

$$\omega(n) = \text{το πλήθος των πρώτων διαιρετών του } n.$$

Π. χ. $\omega(12) = 2$, αφού οι μόνοι πρώτοι διαιρέτες του 12 είναι οι 2 και 3. Να δειχθεί ότι η συνάρτηση $f(n) = 2^{\omega(n)}$ είναι πολλαπλασιαστική.

(β) *Να δειχθεί ότι για κάθε φυσικό n ισχύει*

$$\tau(n^2) = \sum_{d|n} f(d),$$

όπου $\tau(n)$ το πλήθος των διαιρετών του n.
(1+1 μονάδες)

Απόδειξη. **(α)** Εξ ορισμού, αρκεί να δειχθεί πως για τυχόντες φυσικούς m, n, πρώτους μεταξύ τους ισχύει $f(mn) = f(m)f(n)$. Προς τούτο, θεωρούμε τις πρωτογενείς αναλύσεις των m, n:

$$m = p_1^{a_1} \cdots p_r^{a_r}$$

και

$$n = q_1^{b^1} \cdots q_s^{b_s}.$$

Εφόσον οι m, n είναι πρώτοι μεταξύ τους, οι $p_1, \ldots, p_r$ είναι διάφοροι των $q_1, \ldots, q_s$, άρα η πρωτογενής ανάλυση του mn είναι

$$mn = p_1^{a_1} \cdots p_r^{a_r} q_1^{b^1} \cdots q_s^{b_s}$$

οπότε $\omega(m) = r$, $\omega(n) = s$, και $\omega(mn) = r + s$, άρα

$$f(mn) = 2^{\omega(mn)} = 2^{r+s} = 2^r 2^s = 2^{\omega(m)} 2^{\omega(n)} = f(m)f(n).$$

(β) Το δεξί μέλος μπορεί να γραφεί ως $f * \mathbf{1}(n)$, όπου $\mathbf{1}(n) = 1$ για κάθε n. Αφού οι f και $\mathbf{1}$ είναι πολλαπλασιαστικές, τότε και το δεξί μέλος είναι πολλαπλασιαστική συνάρτηση ως προς n. Τώρα για m, n πρώτους μεταξύ τους, ισχύει

$$\tau((mn)^2) = \tau(m^2 n^2) = \tau(m^2)\tau(n^2),$$

αφού η τ είναι πολλαπλασιαστική και $(m^2, n^2) = 1$ όταν ισχύει $(m, n) = 1$. Άρα και το αριστερό μέλος της δοθείσης ισότητας είναι πολλαπλασιαστική συνάρτηση ως προς n. Αρκεί λοιπόν να δειχθεί η ισότητα για δυνάμεις πρώτων. Ισχύει

$$\tau((p^r)^2) = \tau(p^{2r}) = 2r + 1$$

και

$$\sum_{d|p^r} f(d) = f(1) + f(p) + \cdots + f(p^r) = 1 + \underbrace{2 + \cdots + 2}_{r \text{ φορές}} = 2r + 1,$$

ολοκληρώνοντας την απόδειξη. □

4. **(α)** *Έστω p περιττός πρώτος και $\{a_1, \ldots, a_{p-1}\}$ περιορισμένο σύστημα υπολοίπων $\pmod p$. Να δειχθεί ότι το $\{a_1, 2a_2, \ldots, (p-1)a_{p-1}\}$ δεν αποτελεί περιορισμένο σύστημα υπολοίπων $\pmod p$.*

(β) *Να λυθεί το παρακάτω σύστημα ισοτιμιών:*

$$\begin{aligned} x &\equiv 1 \pmod{12} \\ 3x &\equiv 7 \pmod{13}. \end{aligned}$$

(1+1 μονάδες)

Απόδειξη. **(α)** Για κάθε τέτοιο περιορισμένο σύστημα υπολοίπων, οι $a_1, \ldots, a_{p-1}$ είναι ισότιμοι των $1, 2, \ldots, p-1$ με κάποια σειρά, οπότε από Θεώρημα Wilson προκύπτει

$$\begin{aligned} a_1 \cdots a_{p-1} &\equiv 1 \cdot 2 \cdots (p-1) \pmod p \\ &\equiv -1 \pmod p. \end{aligned}$$

Όμως για το $\{a_1, 2a_2, \ldots, (p-1)a_{p-1}\}$ ισχύει

$$\begin{aligned} a_1 \cdot (2a_2) \cdots ((p-1)a_{p-1}) &\equiv ((p-1)!)^2 \pmod p \\ &\equiv 1 \pmod p \\ &\not\equiv -1 \pmod p \end{aligned}$$

οπότε δεν μπορεί να είναι περιορισμένο σύστημα υπολοίπων $\pmod p$. □

5. **(α)** *Να λυθεί η ισοτιμία*

$$x^4 \equiv 3 \pmod{11}.$$

(β) *Να λυθεί η ισοτιμία*

$$7^x \equiv 4 \pmod{11}.$$

(1+1 μονάδες)

Απόδειξη. **(α)** Ο 11 είναι πρώτος, οπότε υπάρχουν αρχικές ρίζες $\pmod{11}$. Για μια τέτοια αρχική ρίζα, έστω g, θα πρέπει να ισχύει $g, g^2, g^5 \not\equiv 1 \pmod{11}$. Παίρνουμε $g = 2$ και υπολογίζουμε τις αντίστοιχες δυνάμεις:

k	1	2	4	5
$2^k \pmod{11}$	2	4	5	10

Άρα το 2 είναι αρχική ρίζα $\pmod{11}$. Λύνουμε τώρα την ισοτιμία χρησιμοποιώντας δείκτες με βάση 2:

$$\operatorname{ind}_2 x^4 \equiv \operatorname{ind}_2 3 \pmod{10}$$

ή

$$4 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 3 \pmod{10}.$$

Υπολογίζοντας τις δυνάμεις του 2 $\pmod{10}$ βρίσκουμε τον $\operatorname{ind}_2 3$:

k	1	2	3	4	5	6	7	8
$2^k \pmod{11}$	2	4	8	5	10	9	7	3

και διαπιστώνουμε πως $\operatorname{ind}_2 3 = 8$. Η ισοτιμία γίνεται

$$4 \operatorname{ind}_2 x \equiv 8 \pmod{10}.$$

Ισχύει $(4, 10) = 2$ και $2 \mid 8$, οπότε η ισοτιμία έχει λύσεις. Διαιρώντας με 2 και τα δύο μέλη, όπως και το modulo θα έχουμε

$$2 \operatorname{ind}_2 x \equiv 4 \pmod{5}$$

ή

$$\operatorname{ind}_2 x \equiv 2 \pmod{5}$$

και τελικά

$$\operatorname{ind}_2 x \equiv 2, 7 \pmod{10}$$

άρα

$$x \equiv 2^2, 2^7 \pmod{11}$$

ή πιο απλά

$$x \equiv \pm 4 \pmod{11}.$$

(β) Χρησιμοποιώντας και πάλι δείκτες με αρχική ρίζα το 2, η δοθείσα είναι ισοδύναμη της

$$x \operatorname{ind}_2 7 \equiv \operatorname{ind}_2 4 \pmod{10}.$$

Από τον πίνακα που βρήκαμε στο **(α)** προκύπτει $\operatorname{ind}_2 7 = 7$ και $\operatorname{ind}_2 4 = 2$, άρα

$$7x \equiv 2 \pmod{10}.$$

Αφού $7 \cdot 3 = 21 \equiv 1 \pmod{10}$, ένας αντίστροφος του 7 $\pmod{10}$ είναι το 3. Άρα

$$x \equiv 3 \cdot 2 \equiv 6 \pmod{10}.$$

□

6. **(α)** *Να υπολογιστεί το σύμβολο Legendre* $(253/157)$.

(β) *Έστω $p = 4m + 1$ πρώτος και $d \mid m$. Να δειχθεί ότι $(d/p) = 1$.*
(1+1 μονάδες)

Απόδειξη. **(α)** Ισχύει $253 = 157 + 96$, άρα $(253/157) = (96/157) = (2^5 \cdot 3/157) = (2/157)^5(3/157)$. Αφού $157 \equiv -3 \pmod 8$ θα έχουμε (2/157)=-1, άρα $(253/157) = -(3/157)$. Από τον νόμο τετραγωνικής αντιστροφής προκύπτει $(3/157) = (157/3)$, εφόσον $157 \equiv 1 \pmod 4$, και επιπλέον, αφού $157 \equiv 1 \pmod 3$, θα ισχύει $(157/3) = (1/3) = 1$, άρα $(253/157) = -1$.

(β) Αν d περιττός, τότε από τετραγωνική αντιστροφή (έχουμε $p \equiv 1 \pmod 4$) ισχύει $(d/p) = (p/d) = (1/d) = 1$, αφού ο d διαιρεί τον $4m = p - 1$ (δηλαδή $p \equiv 1 \pmod d$). Αν ο d είναι άρτιος, θα ισχύει $d = 2^n d_0$, για κάποιον θετικό ακέραιο n και περιττό d_0. Επομένως $(d/p) = (2/p)^n (d_0/p) = (2/p)^n$, αφού $(d_0/p) = 1$, όπως προηγουμένως. αφού ο d είναι άρτιος, τότε και ο m θα είναι, δηλαδή $m = 2k$ για κάποιο k, άρα $p = 8k + 1$ ή $p \equiv 1 \pmod 8$. Όμως τότε $(2/p) = 1$, οπότε τελικά $(d/p) = 1$.

□