Λύσεις Θεμάτων Θεωρίας Αριθμών

1. **α)** *Να δειχθεί ότι ο πέμπτος αριθμός της μορφής Fermat, δηλαδή ο*

$$F_5 = 2^{2^5} + 1$$

διαιρείται από το 641.

β) *Έστω F_n η ακολουθία των αριθμών Fermat, δηλαδή*

$$F_n = 2^{2^n} + 1,\ n \geqslant 0.$$

Να δειχθεί ότι για κάθε $n \geqslant 0$ ισχύει

$$(F_n, F_{n+1}) = 1.$$

γ) *Να δειχθεί ότι για κάθε φυσικό n ισχύει*

$$31 \mid 5^{3n+1} + 2^{5n+2} + 22.$$

(1+1+1 μονάδες)

Απόδειξη. **α)** Αρκεί να δειχθεί ότι

$$2^{32} \equiv -1 \pmod{641}.$$

Προκειμένου να υπολογίσουμε το υπόλοιπο αυτής της μεγάλης δύναμης ως προς το 641, παίρνουμε τετράγωνα και υπολογίζουμε σε κάθε βήμα το υπόλοιπο. Οπότε προκύπτει ο παρακάτω πίνακας:

k	1	2	4	8	16	32
$2^k \pmod{641}$	2	4	16	256	156	-1

Για παράδειγμα,

$$256^2 = 65536 = 641 \cdot 102 + 154 \equiv 154 \pmod{641},$$

και ομοίως

$$154^2 = 23716 = 641 \cdot 36 + 640 \equiv -1 \pmod{641}.$$

β) Ισχύει

$$F_{n+1} = 2^{2^n \cdot 2} + 1 = (2^{2^n})^2 + 1 = (F_n - 1)^2 + 1 = F_n^2 - 2F_n + 2,$$

άρα

$$(F_n, F_{n+1}) = (F_n, F_{n+1} - (F_n - 2)F_n) = (F_n, 2) = 1,$$

αφού προφανώς ο F_n είναι περιττός.

γ) Θέτουμε $A_n = 5^{3n+1} + 2^{5n+2} + 22$. Θα αποδειχθεί επαγωγικά· για $n = 0$ βλέπουμε πως $A_0 = 5 + 2^2 + 22 = 31$, οπότε ισχύει $31 \mid A_0$. Έστω ότι ισχύει για $n = k$, δηλαδή $31 \mid A_k$. Για να δείξουμε ότι $31 \mid A_{k+1}$, αρκεί να δειχθεί ότι $31 \mid A_{k+1} - A_k$. Έχουμε:

$$\begin{aligned} A_{k+1} - A_k &= 5^{3k+4} + 2^{5k+7} + 22 - 5^{3k+1} - 2^{5k+2} - 22 \\ &= (5^3 - 1)5^{3k+1} + (2^5 - 1)2^{5k+2} \\ &= 124 \cdot 5^{3k+1} + 31 \cdot 2^{5k+2} \\ &= 31(4 \cdot 5^{3k+1} + 2^{5k+2}), \end{aligned}$$

αποδεικνύοντας το ζητούμενο. Ένας άλλος τρόπος λύσης είναι με την χρήση ισοτιμιών. Όπως διαπιστώσαμε και πριν, ισχύει $5^3 = 125 \equiv 1 \pmod{31}$ και $2^5 = 32 \equiv 1 \pmod{31}$, άρα

$$\begin{aligned} 5^{3n+1} + 2^{5n+2} + 22 &\equiv 5^{3n} \cdot 5 + 2^{5n} \cdot 2^2 + 22 \pmod{31} \\ &\equiv 125^n \cdot 5 + 32^n \cdot 2^2 + 22 \pmod{31} \\ &\equiv 1^n \cdot 5 + 1^n \cdot 2^2 + 22 \pmod{31} \\ &\equiv 5 + 4 + 22 \equiv 0 \pmod{31} \end{aligned}$$

□

2. *Έστω $\tau, \sigma : \mathbb{N} \to \mathbb{N}$ οι αριθμητικές συναρτήσεις που δίνουν το πλήθος και το άθροισμα των διαιρετών αντίστοιχα, και $\varphi : \mathbb{N} \to \mathbb{N}$ η συνάρτηση του Euler. Να δειχθεί ότι για κάθε $n \in \mathbb{N}$ ισχύει*

$$n\tau(n) = \sum_{d \mid n} \sigma(d)\varphi(n/d),$$

όπου το d στο παραπάνω άθροισμα διατρέχει τους θετικούς διαιρέτες του n. (2 μονάδες)

Απόδειξη. Έστω $T : \mathbb{N} \to \mathbb{N}$ η ταυτοτική συνάρτηση, δηλαδή $T(n) = n$ για κάθε $n \in \mathbb{N}$. Η δοθείσα ισότητα μπορεί να γραφεί ως εξής:

$$T\tau = \sigma * \varphi.$$

Γνωρίζουμε πως ισχύει $\sigma = T * \mathbf{1}$, $T = \mathbf{1} * \varphi$, και $\tau = \mathbf{1} * \mathbf{1}$, άρα

$$\begin{aligned} \sigma * \varphi &= (T * \mathbf{1}) * \varphi \\ &= T * (\mathbf{1} * \varphi) \\ &= T * T. \end{aligned}$$

Επειδή η T είναι *πλήρως* πολλαπλασιαστική, θα ισχύει

$$\begin{aligned} T(n)\tau(n) &= \sum_{d \mid n} T(n)\mathbf{1}(d)\mathbf{1}(n/d) \\ &= \sum_{d \mid n} T(d)T(n/d) \\ &= T * T(n), \end{aligned}$$

αποδεικνύοντας το ζητούμενο.

(*β΄ τρόπος*) Γνωρίζουμε πως οι T, τ, σ και φ είναι όλες πολλαπλασιαστικές, οπότε και οι $T\tau$ και $\sigma * \varphi$ είναι, καθώς γινόμενα και συνελίξεις πολλαπλασιαστικών συναρτήσεων είναι

επίσης πολλαπλασιαστικές συναρτήσεις. Αρκεί λοιπόν να αποδείξουμε την δοθείσα ισότητα για δυνάμεις πρώτων, π. χ. για p^r, όπου p πρώτος και $r \geqslant 1$. Ισχύει

$$T(p^r)\tau(p^r) = p^r(r+1),$$

και

$$\begin{aligned}
\sigma * \varphi(p^r) &= \sum_{i=0}^{r} \sigma(p^i)\varphi(p^{r-i}) \\
&= \sigma(p^r)\varphi(1) + \sum_{i=0}^{r-1} \frac{p^{i+1}-1}{p-1} p^{r-i-1}(p-1) \\
&= (1 + p + \cdots + p^r) + \sum_{i=0}^{r-1} (p^r - p^{r-i-1}) \\
&= (1 + p + \cdots + p^r) + r \cdot p^r - (1 + p + \cdots + p^{r-1}) \\
&= p^r(r+1),
\end{aligned}$$

ολοκληρώνοντας την απόδειξη. □

3. *Να λυθεί το παρκάτω σύστημα ισοτιμιών:*

$$\begin{aligned}
x &\equiv 9 \pmod{24} \\
3x &\equiv 19 \pmod{20} \\
5x &\equiv 3 \pmod{14}.
\end{aligned}$$

(2 μονάδες)

Λύση. Το σύνολο των ακεραίων που ικανοποιεί την πρώτη ισοτιμία μπορεί να περιγραφεί με την εξής μορφή:

$$\boxed{x = 24y + 9, y \in \mathbb{Z}}$$

Αντικαθιστούμε στις άλλες δύο ισοτιμίες, οπότε προκύπτει το εξής σύστημα ως προς y (μετά από πράξεις):

$$\begin{aligned}
72y &\equiv -8 \pmod{20} \\
120y &\equiv -42 \pmod{14}.
\end{aligned}$$

Έχουμε $72 = 2^3 \cdot 3^2$, $20 = 2^2 \cdot 5$, $120 = 2^3 \cdot 3 \cdot 5$ και $14 = 2 \cdot 7$, οπότε $(72, 20) = 4$ και $(120, 14) = 2$. Αφου $4 \mid -8$ και $2 \mid -42$, η κάθεμια από τις παραπάνω ισοτιμίες έχει λύση, και είναι ισοδύναμες με

$$\begin{aligned}
18y &\equiv -2 \pmod{5} \\
60y &\equiv -21 \pmod{7}.
\end{aligned}$$

Προφανώς $18 \equiv -2 \pmod{5}$, $60 \equiv 4 \pmod{7}$ και $-21 \equiv 0 \pmod{7}$, οπότε το σύστημα παίρνει την εξής πιο απλή μορφή:

$$\begin{aligned}
-2y &\equiv -2 \pmod{5} \\
4y &\equiv 0 \pmod{7}.
\end{aligned}$$

Έχουμε

$$\begin{aligned}
-2y \equiv -2 \pmod{5} &\Rightarrow 2(-2)y \equiv 2(-2) \pmod{5} \\
&\Rightarrow y \equiv 1 \pmod{5},
\end{aligned}$$

οπότε οι ακέραιοι που ικανοποιούν αυτήν την ισοτιμία είναι της μορφής

$$\boxed{y = 5z + 1, z \in \mathbb{Z}}$$

Αντικαθιστώντας στην $4y \equiv 0 \pmod 7$, προκύπτει

$$20z \equiv -4 \pmod 7$$

και επειδή $20 \equiv -1 \pmod 7$, η παραπάνω είναι ισοδύναμη της $z \equiv 4 \pmod 7$, της οποίας οι λύσεις περιγράφονται από την εξής μορφή

$$\boxed{z = 7w + 4, w \in \mathbb{Z}}$$

Αφού έχουμε χρησιμοποιήσει όλες τις ισοτιμίες, δεν υπάρχουν περαιτέρω περιορισμοί για το w. Αντικαθιστόντας διαδοχικά, βρίσκουμε όλες τις ακέραιες τιμές του x:

$$\begin{aligned} x &= 24y + 9 \\ &= 24(5z + 1) + 9 = 120z + 33 \\ &= 120(7w + 4) + 33 = 840z + 513 \end{aligned}$$

άρα η λύση του συστήματος περιγράφεται από την εξής ισοτιμία

$$\boxed{x \equiv 513 \pmod{840}}$$ □

Σημείωση: Το αποτέλεσμα παραμένει σωστό, αν αντί του 513 είχαμε κάποιον άλλο ακέραιο, ισότιμο του 513 modulo 840, όπως για παράδειγμα το -327.

4. **α)** *Να βρεθούν όλες οι αρχικές ρίζες* $\pmod n$ *(αν υπάρχουν!) στο σύνολο* $\{1, 2, \ldots, n-1\}$ *για τις περιπτώσεις* $n = 22$ *και* $n = 221$.

β) *Να βρεθούν όλες οι λύσεις της ισοτιμίας*

$$3x^3 \equiv 17 \pmod{22}.$$

(1+1 μονάδες)

Λύση. **α)** Γνωρίζουμε πως όλοι οι φυσικοί n για τους οποίους υπάρχουν αρχικές ρίζες $\pmod n$ είναι της μορφής $2, 4, p^r, 2p^r$, όπου p περιττός πρώτος και $r \geqslant 1$. Εφόσον $221 = 13 \cdot 17$, δεν υπάρχουν αρχικές ρίζες $\pmod{221}$, αφού το 221 είναι γινόμενο δύο διαφορετικών περιττών πρώτων. Αντιθέτως, το $22 = 2 \cdot 11$ έχει την παραπάνω μορφή για $p = 11$ και $r = 1$, οπότε υπάχουν αρχικές ρίζες $\pmod{22}$.

Βρίσκουμε πρώτα μια αρχική ρίζα $\pmod{11}$, με δοκιμές. Γι'αυτήν την αρχική ρίζα, έστω g, θα πρέπει να ισχύει $\operatorname{ord}_{11} g = \varphi(11) = 10$. Αφού ούτως ή άλλως ισχύει $\operatorname{ord}_{11} g \mid 10$, πρέπει να ελέγξουμε αν ισχύουν οι $g, g^2, g^5 \not\equiv 1 \pmod{11}$. 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 $\pmod{11}$. Επομένως οι υποψήφιες αρχικές ρίζες $\pmod{22}$ είναι οι 2 και $2 + 11 = 13$. Απορρίπτουμε την άρτια, οπότε το 13 είναι αρχική ρίζα $\pmod{22}$. Οι υπόλοιπες αρχικές ρίζες είναι της μορφής 13^k, όπου $1 \leqslant k \leqslant \varphi(22) - 1 = 9$, και $(k, \varphi(22)) = (k, 10) = 1$, δηλαδή οι

$$13, 13^3, 13^7, 13^9.$$

Μας μένει να βρούμε τα υπόλοιπα των δυνάμεων αυτών όταν διαιρεθούν με το 22:

k	1	2	3	6	7	9
$13^k \pmod{22}$	13	15	19	9	7	17

(σε κάθε βήμα παίρνουμε το υπόλοιπο $\pmod{22}$, π. χ. $13^6 \equiv (13^3)^2 \equiv 19^2 \equiv (-3)^2 \equiv 9 \pmod{22}$). Τελικά, οι ζητούμενες αρχικές ρίζες είναι οι $7, 13, 17, 19$.

β) Καταρχήν απαλείφουμε τον συντελεστή του x^3, παρατηρώντας πως $3 \cdot 15 = 45 \equiv 1 \pmod{22}$, οπότε

$$x^3 \equiv 3 \cdot 15x^3 \equiv 15 \cdot 17 \equiv (-7)(-5) \equiv 35 \equiv 13 \pmod{22}.$$

Χρησιμοποιώντας δείκτες με αρχική ρίζα το 13, η παραπάνω είναι ισοδύναμη της

$$3 \operatorname{ind}_{13} x \equiv \operatorname{ind}_{13} 13 \pmod{10}.$$

Όμως $\operatorname{ind}_{13} 13 = 1$, και $3 \cdot 7 = 21 \equiv 1 \pmod{10}$, άρα

$$\operatorname{ind}_{13} x \equiv 7 \cdot 3 \operatorname{ind}_{13} x \equiv 7 \pmod{10},$$

η οποία είναι ισοδύναμη της

$$x \equiv 13^7 \equiv 7 \pmod{10}.$$ □

5. **α)** *Να δειχθεί ότι*

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & \text{όταν } p \equiv \pm 1 \pmod{10} \\ -1, & \text{όταν } p \equiv \pm 3 \pmod{10}. \end{cases}$$

β) *Χρησιμοποιώντας το* **(α)**, *δείξτε ότι αν p περιττός πρώτος με $p \equiv \pm 3 \pmod{10}$ και*

$$p \mid x^2 - 5y^2,$$

τότε θα ισχύει $p \mid x$ και $p \mid y$.
(1+1 μονάδες)

Απόδειξη. **α)** Αφού $5 \equiv 1 \pmod{4}$, από τον νόμο τετραγωνικής αντιστροφής θα ισχύει

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Ισχύει $(1/5) = (-1/5) = 1$, αφού $(-1/5) = (-1)^{(5-1)/2} = (-1)^2 = 1$, και

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{(3-1)/2} = -1,$$

άρα και $(-3/5) = (-1/5)(3/5) = -1$. Επομένως, αν $p = 10k \pm 3$, για κάποιον $k \in \mathbb{Z}$, τότε

$$\left(\frac{5}{10k \pm 3}\right) = \left(\frac{10k \pm 3}{5}\right) = \left(\frac{\pm 3}{5}\right) = -1,$$

ενώ αν $p = 10k \pm 1$, για κάποιον $k \in \mathbb{Z}$, τότε

$$\left(\frac{5}{10k \pm 1}\right) = \left(\frac{10k \pm 1}{5}\right) = \left(\frac{\pm 1}{5}\right) = 1,$$

αποδεικνύοντας το ζητούμενο.

β) Θα ισχύει $x^2 \equiv 5y^2 \pmod{p}$, οπότε αν $p \nmid x$, τότε προφανώς θα έχουμε και $p \nmid y$, άρα

$$1 = \left(\frac{x^2}{p}\right) = \left(\frac{5y^2}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{y^2}{p}\right) = (-1) \cdot 1 = -1,$$

άτοπο (χρησιμοποιήσαμε το $(5/p) = -1$). Άρα αναγκαστικά θα έχουμε $p \mid x$, οπότε και $p \mid y$, αφού $p \neq 5$.

□