1η Πρόοδος Εφαρμοσμένης Άλγεβρας
Λύσεις

1. *Θεωρούμε τον δακτύλιο*

$$R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

την συνήθη νόρμα του $N : R^* \to \mathbb{N}$ *με τύπο*

$$N(a + bi) = a^2 + b^2 = |a + bi|^2$$

(γνωρίζουμε πως ο R *με την* N *είναι Ευκλείδειος). Έστω* $x, y \in R^*$ *και* d *ένας κοινός τους διαιρέτης. Αν ισχύει* $N(d) = ΜΚΔ(N(x), N(y))$*, τότε να δειχθεί ότι*

$$d = ΜΚΔ(x, y).$$

(10 πόντοι)

Απόδειξη. Έστω δ ένας μέγιστος κοινός διαιρέτης των x, y. Εξ ορισμού, $d|\delta$, άρα $\delta = du$, για κάποιο $u \in R$. Εφόσον η νόρμα είναι πολλαπλασιαστική, θα ισχύει $N(\delta) = N(d)N(u)$, δηλαδή $N(d)|N(\delta)$. Επίσης, αφού δ κοινός διαιρέτης των x, y, τότε ξανά από την πολλαπλασιαστική ιδιότητα της νόρμας προκύπτει πως ο $N(\delta)$ είναι κοινός διαιρέτης των $N(x)$, $N(y)$, άρα θα διαιρεί και τον μέγιστο κοινό διαιρέτη τους, που είναι το $N(d)$. Αφού $N(\delta)|N(d)$ και $N(d)|N(\delta)$, τότε $N(d) = N(\delta)$, αφού και οι δύο είναι φυσικοί. Επομένως $N(u) = 1$, δηλαδή το u είναι μονάδα και τα d, δ είναι συνεταιρικά. Τελικά, $d = \text{ΜΚΔ}(x, y)$. □

2. *Να βρεθεί ο μέγιστος κοινός διαιρέτης των* $5 + 4i$ *και* $4 + 3i$ *στον δακτύλιο* $\mathbb{Z}[i]$ *και να γραφεί ως γραμμικός συνδυασμός αυτών των στοιχείων.* (10 πόντοι)

Λύση. Εφαρμόζουμε τον Ευκλείδειο αλγόριθμο. Θέτουμε

$$q_1' = \frac{5 + 4i}{4 + 3i} = \frac{(5 + 4i)(4 - 3i)}{|4 + 3i|^2} = \frac{32 + i}{25} = \frac{32}{25} + \frac{1}{25}i.$$

Αντικαθιστούμε το πραγματικό και φανταστικό μέρος του q_1' με τους πλησιέστερους ακεραίους και προκύπτει το πηλίκο της διαίρεσης $q_1 = 1$. Για το υπόλοιπο r_1 θα ισχύει

$$r_1 = (5 + 4i) - q_1(4 + 3i) = (5 + 4i) - (4 + 3i) = 1 + i.$$

Διαιρούμε στην συνέχεια τα $4 + 3i$ και $1 + i$. Θέτουμε

$$q_2' = \frac{4+3i}{1+i} = \frac{(4+3i)(1-i)}{|1+i|^2} = \frac{7-i}{2} = \frac{7}{2} - \frac{1}{2}i.$$

Υπάρχουν από δύο επιλογές για τον πλησιέστερο ακέραιο στα $\Re(q_2')$ και $\Im(q_2')$. Επιλέγουμε $q_2 = 3$, οπότε το υπόλοιπο r_2 σ'αυτήν την περίπτωση είναι

$$r_2 = (4+3i) - q_2(1+i) = (4+3i) - 3(1+i) = 1.$$

Αφού το 1 είναι μονάδα στον $\mathbb{Z}[i]$ σταματάμε εδώ (η επόμενη διαίρεση θα έβγαζε υπόλοιπο μηδέν), και συμπεραίνουμε πως $1 = \text{ΜΚΔ}(5+4i, 4+3i)$. Για τον γραμμικό συνδυασμό, έχουμε

$$\begin{aligned} 1 &= (4+3i) - 3(1+i) \\ &= (4+3i) - 3[(5+4i) - (4+3i)] \\ &= -3(5+4i) + 4(4+3i). \end{aligned}$$

□

Σημείωση: Στην δεύτερη διαίρεση θα μπορούσαμε να πάρουμε ως πηλίκα τα 4, $3-i$, $4-i$. Οι αντίστοιχοι μέγιστοι κοινοί διαιρέτες θα ήταν οι $-i$, i, -1, και οι αντίστοιχοι γραμμικοί συνδυασμοί

$$\begin{aligned} -i &= -4(5+4i) + 5(4+3i) \\ i &= -(3-i)(5+4i) + (4-i)(4+3i) \\ -1 &= -(4-i)(5+4i) + (5-i)(4+3i). \end{aligned}$$

3. *Να αποδειχθεί ότι το πολυώνυμο X^2+1 είναι ανάγωγο στο $\mathbb{F}_3[X]$, και έπειτα να βρεθούν όλες οι πρωταρχικές ρίζες του σώματος*

$$F = \mathbb{F}_3[X]/(X^2+1).$$

Οι πρωταρχικές ρίζες να γραφούν στην μορφή

$$[a_1X + a_0],\ a_0, a_1 \in \mathbb{F}_3.$$

(10 πόντοι)

Απόδειξη. Αρκεί να δειχθεί πως το πολυώνυμο $P(X) = X^2+1$ δεν έχει ρίζες στο $\mathbb{F}_3$. Αυτό είναι εύκολο να ελεγχθεί:

$$\begin{aligned} P(0) &= 1 \neq 0 \\ P(1) &= 1^2 + 1 = 2 \neq 0 \\ P(2) &= 2^2 + 1 = 5 = 2 \neq 0. \end{aligned}$$

Υπενθυμίζουμε πως η αριθμητική γίνεται modulo 3. Το F είναι σώμα με $3^2 = 9$ στοιχεία, άρα η πολλαπλαστική ομάδα F^* έχει 8 στοιχεία. Η τάξη ενός οποιουδήποτε στοιχείου θα είναι διαιρέτης του 8, δηλαδή ανήκει στο σύνολο $\{1, 2, 4, 8\}$. Προκειμένου το $\alpha \in F^*$ να είναι πρωταρχική ρίζα, πρέπει να ισχύει $\alpha^d \neq [1]$ για $d \in \{1, 2, 4\}$. Δοκιμάζουμε $\alpha = [X]$. Ισχύει $X^2 \equiv -1 \equiv 2 \pmod{X^2+1}$, άρα $X^4 \equiv 2^2 \equiv 1 \pmod{X^2+1}$:

i	1	2	4
$[X]^i$	$[X]$	$[2]$	$[1]$

Άρα $\mathrm{ord}[X] = 4$ οπότε το $[X]$ δεν είναι πρωταρχική ρίζα. Δοκιμάζουμε το $[2X]$, χρησιμοποιώντας τον παραπάνω πίνακα και έχοντας υπ'όψιν πως $[2]^2 = [1]$

i	1	2	4
$[2X]^i$	$[2X]$	$[2]$	$[1]$

Άρα ούτε το $[2X]$ είναι πρωταρχική ρίζα. Δοκιμάζουμε το $[X+1]$. Ισχύει

$$\begin{aligned} [X+1]^2 &= [X^2+2X+1] = [2+2X+1] = [2X] \neq [1] \\ [X+1]^2 &= [X+1]^2[X+1]^2 = [2X]^2 = [2] \neq [1] \end{aligned}$$

ή συνοπτικά

i	1	2	4
$[X+1]^i$	$[X+1]$	$[2X]$	$[2]$

χρησιμοποιώντας τον παραπάνω πίνακα. Άρα $\mathrm{ord}[X+1] = 8$, οπότε είναι πρωταρχική ρίζα. Όλες οι πρωταρχικές ρίζες θα είναι της μορφής $[X+1]^i$ όπου $1 \leqslant i \leqslant 8$ και $\mathrm{ΜΚΔ}(i, 8) = 1$:

$$\begin{aligned} [X+1]^3 &= [X+1]^2[X+1] = [2X][X+1] = [2X^2+2x] = [4+2X] = [2X+1] \\ [X+1]^5 &= [X+1]^4[X+1] = [2][X+1] = [2X+2] \\ [X+1]^7 &= [X+1]^4[X+1]^3 = [2][2X+1] = [4X+2] = [X+2] \end{aligned}$$

άρα όλες οι πρωταρχικές ρίζες είναι οι $[X+1]$, $[2X+1]$, $[2X+2]$, $[X+2]$. □

Σημείωση: Έχουμε δει πως οι κλάσεις των σταθερών πολυωνύμων δεν είναι πρωταρχικές ρίζες, στην συγκεκριμένη περίπτωση οι $[0]$, $[1]$, $[2]$. Στο σημείο που έχουμε αποκλείσει τις κλάσεις $[X]$ και $[2X]$, μπορούμε απλά να παρατηρήσουμε πως οι υπόλοιπες τέσσερεις κλάσεις, δηλαδή οι $[X+1]$, $[2X+1]$, $[2X+2]$, $[X+2]$, θα είναι αναγκαστικά όλες οι πρωταρχικές ρίζες, αφού αυτές είναι σε πλήθος $\varphi(8) = 4$. Αυτό το έξυπνο επιχείρημα δόθηκε από μερικούς φοιτητές.

4. *Δίνεται ότι το πολυώνυμο $X^5 + X^2 + 1$ είναι ανάγωγο στον $\mathbb{F}_2[X]$. Να αποδειχθεί ότι η κλάση $[X^2 + X + 1]$ είναι πρωταρχική ρίζα στο σώμα*

$$F = \mathbb{F}_2[X]/(X^5 + X^2 + 1).$$

(5 πόντοι)

Απόδειξη. Το σώμα F έχει $2^5 = 32$ στοιχεία, άρα η πολλαπλασιατική ομάδα F^* έχει 31, δηλαδή το F έχει $\varphi(31) = 30$ πρωταρχικές ρίζες (το 31 είναι πρώτος). Αφού οι κλάσεις $[0]$, $[1]$ προφανώς δεν είναι πρωταρχικές ρίζες, τότε όλα τα υπόλοιπα 30 στοιχεία του F, μέσα στα οποία και το $[X^2 + X + 1]$, είναι πρωταρχικές ρίζες. □

Σημείωση: Ισοδύναμα, θα μπορούσαμε να πούμε πως $\mathrm{ord}[X^2+X+1] \in \{1, 31\}$. Αφού $[X^2+X+1] \neq [1]$, τότε $\mathrm{ord}[X^2+X+1] \neq 1$, άρα $\mathrm{ord}[X^2+X+1] = 31$, αποδεικνύοντας το ζητούμενο.