Η Θεωρια Αριθμων στην Εκπαιδευση

Καθηγητὴς Ν.Γ. Τζανάκης

Θέμα ποὺ συζητήθηκε στὶς 12 καὶ 14-11-2014

Ἡ κυβικὴ ἐξίσωση τοῦ Fermat $x^3 + y^3 = z^3$
εἶναι ἀδύνατη σὲ μὴ μηδενικοὺς ἀκεραίους x, y, z.

Βασικὴ στρατηγική

Μελετοῦμε τὴν ἴδια ἐξίσωση, ἀλλὰ μὲ ἀγνώστους στὴν ἀκέραια περιοχὴ $D = \mathbb{Z}[\omega]$, ὅπου $\omega = \frac{1+i\sqrt{3}}{2}$. Θὰ ἀποδείξομε ὅτι δὲν ὑπάρχουν μὴ μηδενικὲς λύσεις $x, y, z \in D$, ὁπότε, κατὰ μείζονα λόγο, οὔτε στὸ $\mathbb{Z}$ ὑπάρχουν λύσεις.

Ἀριθμητικὰ δεδομένα τῆς D

- Τὸ ω εἶναι ρίζα τοῦ $X^2 - X + 1$. Ἡ δεύτερη ρίζα τοῦ πολυωνύμου εἶναι ἡ $-\omega^2$. Ἰσχύει $\omega^3 = -1$.
- $D^* = \{\pm 1, \pm\omega, \pm\omega^2\}$.
- Ἡ D εἶναι εὐκλείδεια περιοχὴ μὲ norm τὴν ἀπεικόνιση $\mathrm{N} : D \to \mathbb{N}_0$, ποὺ ὁρίζεται

$$\mathrm{N}(a + b\omega) = |a + b\omega|^2 = a^2 + ab + b^2 = (a + b\omega)(a - b\omega^2).$$

Εἰδικώτερα, στὴ D ἰσχύει ἡ μονοσήμαντη ἀνάλυση σὲ πρώτους

- Τὸ $\lambda = 1 + \omega$ εἶναι πρῶτο στοιχεῖο (πρῶτος) τῆς D καὶ $3 = -\omega^2\lambda^2$.

Κάποιες ἰδιότητες σχετικὲς μὲ τὸ λ

- Ἂν τὸ $\alpha \in D$ δὲν διαιρεῖται ἀπὸ τὸ λ, τότε $\alpha \equiv \pm 1 \pmod{\lambda}$, ἄρα καὶ $\alpha^3 = \alpha \pmod{\lambda}$.
- $\lambda^3 \equiv -3\lambda \pmod{\lambda^4}$. Συνέπεια αὐτοῦ εἶναι ὅτι, ἂν τὸ $\alpha \in D$ δὲν διαιρεῖται ἀπὸ τὸ λ, τότε $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$. Γι' αὐτὸν τὸν τελευταῖο ἰσχυρισμὸ ἀπαιτεῖται νὰ γράψομε $\alpha = \pm 1 + \beta\lambda$ καὶ νὰ κάνομε λίγες πράξεις.

Ἀναγωγὴ τῆς ἐξίσωσης

Θεωροῦμε τὴν ἐξίσωση $\xi^3 + \eta^3 + \zeta^3 = 0$, ὅπου $\xi, \eta, \zeta \in D$ καὶ $\xi\eta\zeta \neq 0$. Χωρὶς βλάβη τῆς γενικότητας μποροῦμε νὰ ὑποθέσομε ὅτι οἱ ξ, η, ζ εἶναι ἀνὰ δύο πρῶτοι μεταξύ

τους.[1] Ἂν ἦταν $\xi\eta\zeta \not\equiv 0 \pmod{\lambda}$, τότε

$$0 = \xi^3 + \eta^3 + \zeta^3 \equiv (\pm 1) + (\pm 1) + (\pm 1) \pmod{\lambda^4},$$

ὅπου τὰ τρία (± 1) εἶναι ἀνεξάρτητα μεταξύ τους. Εὔκολα βλέπομε ὅτι, ἀνάλογα μὲ τὸν συνδυασμὸ τῶν (± 1), τὸ δεξιώτερο μέλος εἴτε εἶναι $\pm 1, \pm 2$ (ἄρα, μὴ διαιρετὸ διὰ λ) εἴτε εἶναι ± 3, ἄρα διαιρετὸ μὲν διὰ λ^2, ὄχι ὅμως καὶ διὰ λ^4. Συνεπῶς, ἕνα ἀκριβῶς ἐκ τῶν ξ, η, ζ εἶναι διαιρετὸ διὰ λ καὶ ὑποθέτομε, δίχως βλάβη τῆς γενικότητος, ὅτι $\lambda | \zeta$. Ἂν λ^n εἶναι ἡ μέγιστη δύναμη τοῦ λ, ποὺ διαιρεῖ τὸ ζ, θέτομε $\zeta = \lambda^n \gamma$, ὅπου $n \geq 1$ καὶ τὸ λ δὲν διαιρεῖ κανένα ἐκ τῶν γ, ξ, η. Ἐπιπλέον, τὰ γ, ξ, η εἶναι ἀνὰ δύο πρῶτα μεταξύ τους καὶ καταλήξαμε στὴ σχέση $\xi^3 + \eta^3 + \lambda^{3n}\gamma^3 = 0$. Συνεπῶς:

Ἡ ἐξίσωση $x^3 + y^3 + \lambda^{3N} z^3 = 0$, μὲ ἀγνώστους τοὺς μὴ μηδενικούς, πρώτους μεταξύ τους $x, y, z \in D$ καὶ τὸν $N \in \mathbb{N}$, ἔχει λύση.

Ἴσως εἶναι περίεργο ἐκ πρώτης ὄψεως, ἀλλὰ εἶναι εὐκολώτερο ν' ἀποδείξομε ὅτι ἡ γενικώτερη ἐξίσωση

$$x^3 + y^3 + \mu\lambda^{3N} z^3 = 0, \quad x, y, z \in D \setminus \{0\},\ \lambda \nmid xyz, \quad \mu \in D^*, \quad N \in \mathbb{N}$$
$$x, y, z \text{ ἀνὰ δύο πρῶτοι μεταξύ τους}$$

εἶναι ἀδύνατη.[2] Ὑποθέτομε, λοιπόν, ὅτι ἡ παραπάνω ἐξίσωση ἔχει λύση καὶ θεωροῦμε μία λύση $(x, y, z, \mu, N) = (\xi, \eta, \zeta, \epsilon, n)$, τέτοια ὥστε τὸ $n \in \mathbb{N}$ νὰ εἶναι τὸ ἐλάχιστο δυνατό. Ἄρα,

$$\xi^3 + \eta^3 + \epsilon\lambda^{3n} \zeta^3 = 0, \quad \xi, \eta, \zeta \in D \setminus \{0\},\ \lambda \nmid \xi\eta\zeta, \quad \epsilon \in D^*, \quad n \in \mathbb{N} \tag{1}$$
$$\xi, \eta, \zeta \text{ ἀνὰ δύο πρῶτοι μεταξύ τους}$$

καὶ θὰ ὁδηγηθοῦμε σὲ ἄτοπο, βρίσκοντας νέα λύση $(\xi_1, \eta_1, \zeta_1, \epsilon', n')$ μὲ $1 \leq n' < n$.

Τὰ βήματα ποὺ ὁδηγοῦν στὸ ἄτοπο

- $n \geq 2$. Πράγματι, ἀπὸ τὴ σχέση

$$0 = \xi^3 + \eta^3 + \epsilon\lambda^{3n}\zeta^3 \equiv (\pm 1) + (\pm 1) + (\pm 1)\epsilon\lambda^{3n} \pmod{\lambda^4}.$$

Βλέπομε ὅτι, ἀναγκαστικά, τὰ δύο πρῶτα (± 1) πρέπει νὰ δώσουν 0, ἄρα $\lambda^{3n} \equiv 0 \pmod{\lambda^4}$. Ἡ ἰσοτιμία αὐτή, προφανῶς, εἶναι δυνατὴ μόνον ὅταν $n \geq 2$.

- Παραγοντοποιοῦμε τὴν (1):

$$-\epsilon\lambda^{3n}\zeta^3 = (\underbrace{\xi + \eta}_{\alpha_1})(\underbrace{\xi - \eta\omega}_{\alpha_2})(\underbrace{\xi + \eta\omega^2}_{\alpha_3}), \tag{2}$$

[1] Χρειάζεται, ὅμως, ἀπόδειξη!

[2] Οἱ ἄγνωστοι, δηλαδή, εἶναι οἱ x, y, z, μ, N.

ὅπου διαπιστώνομε εὔκολα ὅτι $\alpha_1 \equiv \alpha_2 \equiv \alpha_3 \pmod{\lambda}$. Ἐπιπλέον, τὸ γινόμενο $\alpha_1\alpha_2\alpha_3$ διαιρεῖται διὰ λ, ἄρα καὶ τὰ τρία α_i διαιροῦνται διὰ λ. Θέτομε, γιὰ $i = 1, 2, 3$,

$$\beta_i = \frac{\alpha_i}{\lambda} \quad \text{ὁπότε} \quad \beta_1\beta_2\beta_3 = -\epsilon\lambda^{3(n-1)}\zeta^3. \tag{3}$$

• Ἀποδεικνύομε ὅτι τὰ β_i εἶναι ἀνὰ δύο πρῶτα μεταξύ τους. Γιὰ παράδειγμα, ἂν τὰ β_1, β_2 δὲν ἦταν πρῶτα μεταξύ τους, θὰ ὑπῆρχε πρῶτος $\pi \in D$, ποὺ θὰ τὰ διαιροῦσε, ἄρα ὁ π θὰ διαιροῦσε καὶ τὸ $\beta_1 - \beta_2 = \ldots = \eta$ καὶ τὸ $\omega\beta_1 + \beta_2 = \ldots = \xi$, ἄτοπο.[3] Ἀπὸ τὴν ἐξίσωση (3) τώρα, καταλήγομε στὸ συμπέρασμα ὅτι ἀκριβῶς ἕνα ἐκ τῶν β_i διαιρεῖται διὰ λ. Δίχως βλάβη τῆς γενικότητος μποροῦμε νὰ ὑποθέσομε ὅτι τὸ β_1 εἶναι διαιρετὸ ἀπὸ τὸ λ,[4] ἐνῶ $\beta_2\beta_3 \not\equiv 0 \pmod{\lambda}$. Ἄρα, λόγῳ καὶ τῆς (3), μποροῦμε νὰ θέσομε

$$\beta_1 = \epsilon_1\lambda^{3n-3}\zeta_1^3, \quad \beta_2 = \epsilon_2\eta_1^3, \quad \beta_3 = \epsilon_3 = \epsilon_3\xi_1^3, \quad \epsilon_1\epsilon_2\epsilon_3 = -\epsilon, \quad \xi_1\eta_1\zeta_1 = \zeta, \tag{4}$$

$$\xi_1, \eta_1, \zeta_1 \text{ ἀνὰ δύο πρῶτα μεταξύ τους καὶ } \lambda \nmid \xi_1\eta_1\zeta_1.$$

• Παρατηροῦμε ὅτι $\omega^2\alpha_3 - \omega\alpha_2 + \alpha_1 = 0$[5], ἄρα $\omega^2\beta_3 - \omega\beta_2 + \beta_1 = 0$. Ἀντικαθιστώντας σ' αὐτὴ τὴ σχέση τὰ β_i ἀπὸ τὴν (4), καταλήγομε στὴν $\omega^2\epsilon_3\,\xi_1^3 - \omega\,\epsilon_2\,\eta_1^3 + \epsilon_1\lambda^{3n-3}\zeta_1^3 = 0$. Διαιρώντας μὲ τὴ μονάδα $\omega^2\epsilon_3$ παίρνομε τὴ σχέση

$$\xi_1^3 + \epsilon_4\,\eta_1^3 + \epsilon_5\lambda^{3n-3}\zeta_1^3 = 0, \tag{5}$$

ὅπου $\epsilon_4, \epsilon_4 \in D^*$. Ἡ (5), εἰδικώτερα, συνεπάγεται ὅτι $\xi_1^3 + \epsilon_4\,\eta_1^3 \equiv 0 \pmod{\lambda^3}$, διότι $n \geq 2$. Ἀφ' ἑτέρου, $\xi_1^3 \equiv \pm 1 \pmod{\lambda^4}$, ἄρα $\xi_1^3 \equiv \pm 1 \pmod{\lambda^3}$. Ἐντελῶς ἀνάλογα, $\eta_1^3 \equiv \pm 1 \pmod{\lambda^3}$. Ἄρα, ἀπ' τὴν (5), $(\pm 1) + (\pm 1)\epsilon_4 \equiv 0 \pmod{\lambda^3}$. Αὐτὴ ἡ ἰσοτιμία μπορεῖ νὰ ἀληθεύει μόνο ἂν $\epsilon = \pm 1$, ὁπότε, λόγῳ τῆς (5),

$$\xi_1^3 + (\pm\eta_1)^3 + \epsilon_5\lambda^{3n-3}\zeta_1^3 = 0.$$

Βρήκαμε, λοιπόν, νέα λύση τῆς ἐξίσωσης (1) μὲ $N = 3n - 3$. Ἐπειδὴ $1 \leq n - 1 < n$, καταλήξαμε σὲ ἀντίφαση μὲ τὴν ἐπιλογὴ τοῦ n.

[3] Ἄσκηση: Ἀποδεῖξτε ὅτι τὰ β_2, β_3 εἶναι πρῶτα μεταξύ τους, καθὼς καὶ τὰ β_1, β_3.

[4] Ἄσκηση: Γιατὶ δὲν βλάπτεται ἡ γενικότητα ἀπ' τὴν ὑπόθεση αὐτή;

[5] Πολὺ ἁπλό, λόγῳ τῆς $\omega^2 - \omega + 1 = 0$.