Η Θεωρια Αριθμων στην Εκπαιδευση

Καθηγητὴς Ν.Γ. Τζανάκης

Θέματα ποὺ συζητήθηκαν στὶς 15 καὶ 17-10-2014

Ἐπίλυση Διοφαντικῶν ἐξισώσεων μέσῳ τετραγωνικῶν σωμάτων.

- Λίγα ἱστορικὰ στοιχεῖα.

Θεώρημα 1. (C.L. Siegel-1929) *Ἔστω $f(x,y) \in \mathbb{Z}[x,y]$. Ἂν ἡ καμπύλη, ποὺ ὁρίζεται ἀπὸ τὴν ἐξίσωση $f = 0$ εἶναι γένους ≥ 1, τότε ἡ ἐξίσωση $f(x,y) = 0$ ἔχει πεπερασμένο, τὸ πολύ, πλῆθος λύσεων.*

Ἡ ἀπόδειξή του (πολὺ προχωρημένη) εἶναι μὴ κατασκευαστική (non-effective), δηλαδή, δὲν μᾶς δίνει φρᾶγμα γιὰ τὶς ἀπόλυτες τιμὲς τῶν x, y.

Θεώρημα 2. (A. Baker & J. Coates-1970) *Ἂν $a, b \in \mathbb{Z}$ καὶ $4a^3 + 27b^2 \neq 0$, τότε γιὰ τὶς ἀκέραιες λύσεις (x,y) τῆς ἐξίσωσης $y^2 = x^3 + ax + b$ ἰσχύει τὸ φρᾶγμα*

$$\max\{|x|,|y|\} \leq \exp(\exp(\exp((2H)^{10^{3^{10}}}))), \quad \text{ὅπου } H = \max\{|a|,|b|\}.$$

Ἡ (πολὺ προχωρημένη, ἐπίσης) ἀπόδειξη αὐτοῦ τοῦ θεωρήματος βασίζεται στὴ *Θεωρία Γραμμικῶν Μορφῶν Λογαρίθμων*. Τὸ θεώρημα αὐτὸ εἶναι "ἀποτελεσματικό" (effective) ἀφοῦ, τοὐλάχιστον θεωρητικά, παρέχει "ἀποτελεσματικό", ἢ "κατασκευαστικὸ" τρόπο ὑπολογισμοῦ τῶν ἀκεραίων λύσεων τῆς ἐξίσωσης. Ὅμως ☹

Ἄσκηση 1. Χρησιμοποιώντας τὸ θεώρημα Baker-Coates, ὑπολογῖστε ἕναν ἀκέραιο N, ἄνω φρᾶγμα τῶν ἀκεραίων λύσεων τῆς $x^2 + 2 = y^3$.

Ὁ θεώρημα Baker-Coates βελτιώθηκε πολύ:

Θεώρημα 3. (W. Schmidt-1992) *Ἂν $a, b \in \mathbb{Z}$ καὶ $4a^3 + 27b^2 \neq 0$, τότε γιὰ τὶς ἀκέραιες λύσεις (x,y) τῆς ἐξίσωσης $y^2 = x^3 + ax + b$ ἰσχύει τὸ φρᾶγμα*

$$\max\{|x|,|y|\} \leq \exp(c \cdot H^{12^{13}}),$$

ὅπου $H = \max\{|a|,|b|\}$ καὶ c προσδιορίσιμη θετικὴ σταθερά.

Ἐν γένει, ἡ σταθερὰ c εἶναι πάρα πολὺ μεγάλη. Ἀλλὰ ἀκόμη κι ἂν τὴν πάρομε ἴση μὲ 1, ἰδού!

Ἄσκηση 2. Χρησιμοποιώντας τὸ θεώρημα Schmidt μὲ $c = 1$, ὑπολογῖστε ἕναν ἀκέραιο N, ἄνω φρᾶγμα τῶν ἀκεραίων λύσεων τῆς $x^2 + 2 = y^3$.

Σημείωση. Τὰ θεωρήματα 2 καὶ 3 ἔχουν διατυπωθεῖ γιὰ πολὺ γενικότερης μορφῆς Διοφαντικὲς ἐξισώσεις!

- Ἐπίλυση τῆς Διοφαντικῆς ἐξίσωσης (ἀκέραιες λύσεις)

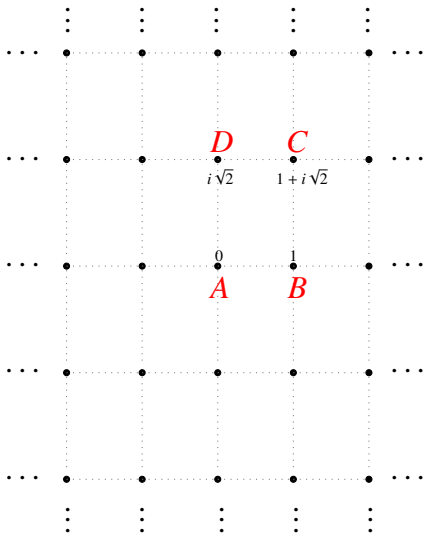
$$x^2 + 2 = y^3. \tag{1}$$

Τὰ βήματα:

1. Δουλεύομε στὸ τετραγωνικὸ σῶμα $K = \mathbb{Q}(i\sqrt{2})$. Σύμφωνα μὲ τὰ γενικὰ θεωρήματα, ποὺ ἔχομε ἀποδείξει,

$$O_K = \{x + yi\sqrt{2} : x, y \in \mathbb{Z}\}, \quad O_K^* = \{\pm 1\}.$$

2. Ἀποδείξαμε ὅτι στὴν ἀκέραια περιοχὴ O_K ἔχομε εὐκλείδεια διαίρεση, ἐπειδὴ μποροῦμε νὰ ὁρίσομε *στάθμη* (νόρμα). Στὴν ἀπόδειξη μᾶς βοήθησε τὸ παρακάτω *πλέγμα* (lattice) καὶ ἡ προφανὴς παρατήρηση ὅτι κάθε σημεῖο z τοῦ μιγαδικοῦ ἐπιπέδου περιέχεται στὸ ἐσωτερικὸ ἢ τὴν περίμετρο ἑνὸς παραλληλογράμμου, ἄρα ὑπάρχει ἕνα σημεῖο τοῦ πλέγματος, ποὺ ἡ ἀπόστασή του ἀπὸ τὸ z εἶναι, τὸ πολύ, $\sqrt{3}/2$.



Ἀπεικόνιση τῆς ἀκέραιας περιοχῆς O_K στὸ μιγαδικὸ ἐπίπεδο

3. Ἀποδείξαμε ὅτι τὸ $i\sqrt{2}$ εἶναι πρῶτος τῆς O_K, ἄρα ἡ ἀνάλυση τοῦ 2 σὲ πρώτους τῆς O_K εἶναι $2 = -(i\sqrt{2})^2$.

4. Ἀποδείξαμε ὅτι στὴν (1) ὁ x εἶναι περιττὸς καί, ἂν ἀναλύσομε τὸ ἀριστερὸ μέλος ὡς $(x + i\sqrt{2})(x - i\sqrt{2})$, οἱ δύο παράγοντες εἶναι πρῶτοι μεταξύ τους.

5. Χρησιμοποιώντας τὴν Ἄσκηση 3 (βλ. παρακάτω), συμπεράναμε ὅτι

$$x + i\sqrt{2} = (a + bi\sqrt{2})^3.$$

Ἀναπτύσσοντας τὸ δεξιὸ μέλος καὶ συγκρίνοντας τὰ δύο μέλη, καταλήξαμε στὶς σχέσεις

$$1 = b(3a^2 - 2b^2), \quad x = a(a^2 - 6b^2),$$

ἀπὸ τὶς ὁποῖες προκύπτει πολὺ εὔκολα ὅτι $(b, a) = (\pm 1, \pm 1)$. Ἄρα, $x = \pm 5$ καί, συνεπῶς, $y = 3$.

Οἱ μόνες ἀκέραιες λύσεις τῆς ἐξίσωσης $x^2 + 2 = y^3$ *εἶναι* $(x, y) = (\pm 5, 3)$.

Ἀμέσως παρακάτω ὑπενθυμίζομε τὸν γενικὸ ὁρισμὸ τῆς μονοσήμαντης ἀνάλυσης, τὸν ὁποῖο εἶναι ἀπαραίτητο νὰ καταννοήσετε προκειμένου νὰ λύσετε τὶς Ἀσκήσεις 3 καὶ 4 (μᾶλλον ἀσκήσεις ρουτίνας, κατὰ τ' ἄλλα). Εἶναι βολικὸ νὰ καθιερώσομε τὴν ἑξῆς ὁρολογία:

Ὁρολογία. Σὲ μιὰ ἀκέραια περιοχὴ D, δύο στοιχεῖα a, b χαρακτηρίζονται *συνεταιρικά* ἂν ὑπάρχει $\epsilon \in D^*$ (δηλαδή, τὸ ϵ εἶναι μονάδα τῆς D ἤ, ἀλλοιῶς, ἀντιστρέψιμο στοιχεῖο τῆς D, ἔτσι ὥστε νὰ ἰσχύει $b = \epsilon a$.

Προφανῶς ἡ *συνεταιρικότητα* εἶναι σχέση ἰσοδυναμίας στὴ D.

Ὁρισμὸς Μία ἀκέραια περιοχὴ D χαρακτηρίζεται *περιοχὴ ἀνάλυσης* (σὲ πρώτους) ἂν κάθε μὴ μηδενικὸ στοιχεῖο της, ποὺ δὲν εἶναι μονάδα, μπορεῖ νὰ γραφεῖ ὡς γινόμενο πεπερασμένου πλήθους πρώτων τῆς D. Ἡ περιοχὴ ἀνάλυσης D λέγεται *περιοχὴ μονοσήμαντης ἀνάλυσης*, ἂν ἡ προαναφερθεῖσα ἀνάλυση μπορεῖ νὰ γίνει, "οὐσιαστικὰ" μὲ ἕνα μόνο τρόπο. Τὸ ἐπίρρημα "οὐσιαστικὰ" λέγεται ἐδῶ ὑπὸ τὴν ἑξῆς ἔννοια: Ἂν τὸ μὴ μηδενικὸ στοιχεῖο a δὲν εἶναι μονάδα καὶ $a = p_1 \cdots p_n$, $a = q_1 \cdots q_m$ εἶναι δύο ἀναλύσεις τοῦ a σὲ πρώτους τῆς D, τότε, ὑποχρεωτικά, $n = m$ καὶ ὑπάρχει μιὰ μετάθεση $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, τέτοια ὥστε τὸ q_1 νὰ εἶναι συνεταιρικὸ μὲ τὸ p_{i_1}, τὸ q_2 νὰ εἶναι συνεταιρικὸ μὲ τὸ p_{i_2}, ..., τὸ q_n νὰ εἶναι συνεταιρικὸ μὲ τὸ p_{i_n}.

Ἄσκηση 3. Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης, $a, b, c \in D$ καὶ $n \in \mathbb{N}$, τέτοια ὥστε τὰ a, b εἶναι πρῶτα μεταξύ τους καὶ $ab = c^n$. Ἀποδεῖξτε ὅτι ὑπάρχουν $c_1, c_2 \in D$ πρῶτα μεταξύ τους καὶ $\epsilon_1, \epsilon_2 \in D^*$, τέτοια ὥστε

$$a = \epsilon_1 c_1^n, \quad b = \epsilon_2 c_2^n, \quad c = c_1 c_2, \quad \epsilon_1 \epsilon_2 = 1.$$

Ἄσκηση 4. Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης, $a, b, c, d \in D$ καὶ $n \in \mathbb{N}$, τέτοια ὥστε τὰ a, b εἶναι πρῶτα μεταξύ τους καὶ $ab = dc^n$. Ἀποδεῖξτε ὅτι ὑπάρχουν $c_1, c_2, d_1, d_2 \in D$ καὶ $\epsilon_1, \epsilon_2 \in D^*$, τέτοια ὥστε, τὰ d_1c_1 καὶ d_2c_2 εἶναι πρῶτα μεταξύ τους καὶ

$$a = \epsilon_1 d_1 c_1^n, \quad b = \epsilon_2 d_2 c_2^n, \quad d = d_1 d_2, \quad c = c_1 c_2, \quad \epsilon_1 \epsilon_2 = 1.$$

- Τὸ ‘‘παράδοξο’’ τῆς Διοφαντικῆς ἐξίσωσης

$$x^2 + 5 = 2y^3. \tag{2}$$

Ἀφοῦ τὸ ἀριστερὸ μέλος τῆς (2) παραγοντοποιεῖται $(x+i\sqrt{5})(x-i\sqrt{5})$, εἶναι φανερὸ ὅτι πρέπει νὰ ἐργαστοῦμε στὸ τετραγωνικὸ σῶμα $K = \mathbb{Q}(i\sqrt{5})$ καί, εἰδικώτερα, στὴν ἀκέραια περιοχὴ O_K.

Μιμηθήκαμε τὸν τρόπο ἐπίλυσης τῆς (1), ἐκτὸς ‘‘μόνο’’ ποὺ ‘‘ξεχάσαμε’’ νὰ ἐξετάσομε ἂν ἰσχύει ἡ μονοσήμαντη ἀνάλυση στὴν ἀκέραια περιοχὴ O_K. Βάσει τῶν θεωρημάτων, ποὺ ἔχουν διδαχθεῖ,

$$O_K = \{x + yi\sqrt{5} : x, y \in \mathbb{Z}\}, \quad O_K^* = \{\pm 1\}.$$

Ἀποδείξαμε ὅτι 2 καὶ $i\sqrt{5}$ εἶναι πρῶτοι. Ἀποδείξαμε μετὰ ὅτι ὁ x στὴ (2) δὲν διαιρεῖται ἀπὸ τὸ 5 (διαιρετότητα στὸ $\mathbb{Z}$) καὶ βάσει αὐτῶν ὁδηγηθήκαμε στὸ συμπέρασμα ὅτι οἱ $x + i\sqrt{5}, x - i\sqrt{5}$ εἶναι πρῶτοι μεταξύ τους (ὡς στοιχεῖα τῆς O_K).
Ἕπεται, ἀπὸ τὴν Ἄσκηση 4, ὅτι

$$x + i\sqrt{5} = 2(a + bi\sqrt{5})^3, \quad a, b \in \mathbb{Z},$$

εἴτε $x - i\sqrt{5} = 2(a + bi\sqrt{5})^3$, ἀλλὰ αὐτὴ ἡ δεύτερη περίπτωση εἶναι ἐντελῶς ὅμοια μὲ τὴν πρώτη. Ἀναπτύσσοντας τὸ δεξιὸ μέλος καὶ ἐξισώνοντας τοὺς συντελεστὲς τοῦ $i\sqrt{5}$ στὰ δύο μέλη καταλήγομε στὴν ἀδύνατη ἰσότητα $1 = 2(3a^2b - 5b^3)$.

Συμπέρασμα: Ἡ ἐξίσωση (2) δὲν ἔχει ἀκέραιες λύσεις. Ὅμως, $7^2 + 5 = 2 \cdot 3^3$! Ποῦ ἔγινε τὸ λάθος;

Ἀπάντηση: Στὸ ὅτι θεωρήσαμε δεδομένη τὴ μονοσήμαντη ἀνάλυση σὲ πρώτους, ἡ ὁποία δὲν ἰσχύει, σύμφωνα μὲ τὴν παρακάτω ἄσκηση.

Ἄσκηση 5. Στὴν ἀκέραια περιοχὴ O_K, ὅπου $K = \mathbb{Q}(i\sqrt{5})$, οἱ $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ εἶναι πρῶτοι, ἰσχύει $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ καὶ οἱ πρῶτοι τοῦ ἀριστεροῦ μέλους δὲν εἶναι συνεταιρικοὶ μὲ τοὺς πρώτους τοῦ δεξιοῦ μέλους. Ἄρα, στὴν O_K δὲν ἰσχύει ἡ μονοσήμαντη ἀνάλυση.