Η Θεωρια Αριθμων στην Εκπαιδευση

Καθηγητὴς Ν.Γ. Τζανάκης

Θέματα ποὺ συζητήθηκαν στὶς 3-10-2014

• Στοὺς ἀκεραίους, πῶς σχετίζεται ἡ μονοσήμαντη ἀνάλυση σὲ πρώτους μὲ τὴν εὐκλείδεια διαίρεση;

Στρατηγική

1. Χάρη στὴν εὐκλείδεια διαίρεση ἀποδεικνύομε ὅτι, δοθέντων τῶν $a, b \in \mathbb{Z}$ (θεωροῦμε ὅτι δὲν εἶναι καὶ οἱ δύο μηδέν), ὑπάρχει θετικὸς $d \in \mathbb{Z}$, τέτοιος ὥστε $\{ax + by : x, y \in \mathbb{Z}\} = d\mathbb{Z}$. Ὕστερα ἀποδεικνύομε εὔκολα ὅτι ὁ d εἶναι κοινὸς διαιρέτης τῶν a, b καί, ἐπιπλέον, ὁ d διαιρεῖται ἀπὸ κάθε κοινὸ διαιρέτη d' τῶν a, b. Συνεπῶς, $d = \text{μκδ}(a, b)$ καὶ ὁ d γράφεται ὡς γραμμικὸς συνδυασμὸς τῶν a, b, μὲ ἀκέραιους συντελεστές.

2. Τυπικὸς ὁρισμὸς τοῦ πρώτου: Ὁ $p > 1$ εἶναι πρῶτος ἂν ἀληθεύει ἡ συνεπαγωγή

$$p = ab \ \ \& \ a, b \in \mathbb{Z} \quad \Rightarrow a = \pm 1 \ \vee \ b = \pm 1$$

3. Τὸ γεγονὸς ὅτι ὁ μκδ δύο ἀριθμῶν γράφεται ὡς γραμμικὸς συνδυασμὸς τῶν ἀριθμῶν αὐτῶν, σὲ συνδυασμὸ μὲ τὸ (2) μᾶς ἐπιτρέπει ν' ἀποδείξομε πολὺ εὔκολα τὴ συνεπαγωγὴ

$$p \text{ πρῶτος} \ \& \ p|ab \quad \Rightarrow \quad p|a \ \vee \ p|b$$

Αὐτὴ εἶναι ἡ κρίσιμη ἰδιότητα τῶν πρώτων, χάρη στὴν ὁποία ἀποδεικνύεται τὸ *μονοσήμαντο* τῆς ἀνάλυσης σὲ πρώτους.

• Πῶς μπορεῖ νὰ γενικευθεῖ ἡ παραπάνω στρατηγικὴ σὲ μιὰ ἀκέραια περιοχὴ D;

1. Ἡ ἔννοια τῆς διαιρετότητας προέρχεται ἀπὸ ἄμεση γενίκευση τῆς διαιρετότητας στὸ $\mathbb{Z}$. Ἔτσι, γιὰ $a, b \in D$ μὲ $b \neq 0$, ὁρίζομε

$$b|a \ \Leftrightarrow \ \exists\, c \in D : a = bc$$

2. Δείξαμε γιατί, στὸν ὁρισμὸ τοῦ πρώτου ἡ συνθήκη, ποὺ στὸ $\mathbb{Z}$ διατυπώθηκε ὡς $p > 1$, τώρα πρέπει ν' ἀντικατασταθεῖ ἀπὸ τὴν $p \in D \setminus D^*$, ὅπου D^* εἶναι τὸ σύνολο τῶν *ἀντιστρεψίμων στοιχείων (μονάδων)* τῆς D. (Ὑπενθύμιση: D^* εἶναι πολλαπλασιαστικὴ ὁμάδα, μὲ τὸν πολλαπλασιασμὸ τῆς D.) Ἐπίσης, δείξαμε γιατὶ στὴ θέση τῆς συνεπαγωγῆς, ποὺ ὁρίζει τοὺς πρώτους p τοῦ $\mathbb{Z}$ (βλ. προηγούμενο (2)), τώρα πρέπει νὰ ἔχομε: Ὁ $p \in D \setminus D^*$ εἶναι πρῶτος ἂν ἀληθεύει ἡ συνεπαγωγή

$$p = ab \ \ \& \ a, b \in D \ \ \Rightarrow a \in D^* \ \vee \ b \in D^*$$

3. Ὁ ΜΚΔ ὁρίζεται ὅπως καὶ στοὺς ἀκεραίους: Ὁ $d \in D$ χαρακτηρίζεται μέγιστος κοινὸς διαιρέτης τῶν $a, b \in D$ (δὲν εἶναι καὶ οἱ δύο μηδέν) ἂν εἶναι κοινὸς διαιρέτης τους καί, ἐπίσης, διαιρεῖται ἀπὸ κάθε κοινὸ διαιρέτη τῶν a, b. Ἡ διαφορὰ ἔγκειται στὸ ὅτι οἱ ab εἶναι δυνατὸν νὰ ἔχουν πολλοὺς ΜΚΔ. Ἀκριβέστερα, ἂν ὁ d εἶναι ΜΚΔ τῶν a, b, τότε, γιὰ κάθε $\epsilon \in D^*$, καὶ ὁ ϵd εἶναι ΜΚΔ τῶν a, b. Καὶ ἀντιστρόφως, ἂν d_1, d_2 εἶναι καὶ οἱ δύο ΜΚΔ τῶν a, b, τότε ὑπάρχει $\epsilon \in D^*$, τέτοιο ὥστε $d_2 = \epsilon d_1$.

4. Αὐτὸ ποὺ δὲν μπορεῖ νὰ ὁρισθεῖ σὲ κάθε ἀκέραια περιοχὴ εἶναι ἡ εὐκλείδεια διαίρεση. Μποροῦμε, ὅμως, νὰ ἐξετάσομε τί μποροῦμε νὰ συμπεράνομε ἂν ὑποθέσομε τὴν ὕπαρξη μιᾶς συνάρτησης *στάθμης* ἢ *νόρμας* $N : D \to \mathbb{N}_0$, ποὺ ἔχει τὶς ἑξῆς ἰδιότητες:

   (α′) $N(a) = 0 \Leftrightarrow a = 0$ καὶ (β′) $b|a \Rightarrow N(b) \le N(a)$

   Ἂν μπορεῖ νὰ ὁριστεῖ μιὰ τέτοια συνάρτηση N ἐπὶ τῆς D, τότε χαρακτηρίζομε τὴ D *εὐκλείδεια περιοχή*.

5. Ὅταν ἡ D εἶναι εὐκλείδεια περιοχή, μποροῦμε νὰ μιμηθοῦμε τὴ «στρατηγική», ποὺ περιγράψαμε γιὰ τὴν περίπτωση τῶν ἀκεραίων: Ἂν $a, b \in D$ δὲν εἶναι καὶ οἱ δύο μηδέν (0_D), τότε ὑπάρχει $d \in D$, τέτοιο ὥστε $\{ax + by : x, y \in D\} = dD$. Αὐτὸ μᾶς ἐπιτρέπει νὰ συμπεράνομε ὅτι ὁ d εἶναι ΜΚΔ τῶν a, b καὶ ὁ d γράφεται ὡς γραμμικὸς συνδυασμὸς τῶν a, b, μὲ συντελεστὲς στὴ D. Ἀλλά τότε μιὰ σχέση στὴ D τῆς μορφῆς $p|ab$ μὲ τὸν p πρῶτο, εὔκολα συνεπάγεται, ὅπως δείξαμε, ὅτι $p|a$ εἴτε $p|b$.

Ἀναφορὲς

[1] Ν.Γ. Τζανάκης, *Θεμελιώδης Θεωρία Ἀριθμῶν* Σημειώσεις, 22-5-2012.
http://server.math.uoc.gr/~tzanakis/Courses/NumberTheory/textbook_main.pdf