Η Θεωρια Αριθμων στην Εκπαιδευση

Καθηγητὴς Ν.Γ. Τζανάκης

Θέματα ποὺ συζητήθηκαν στὶς 1-10-2014

1. Τί σημαίνει *συζυγὴς* μιᾶς παράστασης; Πῶς μποροῦμε, μὲ Στοιχειώδη Μαθηματικά, νὰ δικαιολογήσομε, γιὰ παράδειγμα, τὸ ἑξῆς;

   Ἔστω $f(X) \in \mathbb{Q}[X]$ καὶ $\xi = (a + b\sqrt{m})/c$ μὲ τοὺς $a, b, c, m \in \mathbb{Z}$, $c \neq 0$ καὶ m ὄχι τέλειο τετράγωνο. Ἂν ἰσχύει ἡ σχέση $f(\xi) = 0$, τότε ἰσχύει καὶ ἡ συζυγής της $f(\xi') = 0$, ὅπου $\xi' = (a - b\sqrt{m})/c$.

2. Συζητήσαμε διεξοδικὰ τὴν ἁπλῆ ἄσκηση: *Ἔστω ὅτι γιὰ τοὺς ἀκεραίους x, y ἰσχύει $x^2 = y^3$. Ἂν ὁ p εἶναι πρῶτος καὶ $p^2|x$, δεῖξτε ὅτι $p^2|y$.*
   Μὲ ἀφορμὴ τὴ συζήτηση καταλήξαμε στὴ χρησιμότητα τῆς συνάρτησης $\nu_p(n)$, ὅπως αὐτὴ ὁρίζεται στὴ σελίδα 16 τῶν σημειώσεών μου. Κάθε ἀκέραιος ἀριθμὸς $a \neq 0$ γράφεται ὡς ἑξῆς:
$$a = \prod_{p\in\mathbb{P}}^{*} p^{\nu_p(a)},$$
   ὅπου $\mathbb{P}$ εἶναι τὸ σύνολο τῶν πρώτων καὶ ὁ ἀστερίσκος στὸ $\prod$ δηλώνει ὅτι γιὰ πεπερασμένο, τὸ πολύ, πλῆθος $p \in \mathbb{P}$ εἶναι $\nu_p(n) \neq 0$. Εἶναι ἁπλὸ νὰ δοῦμε ὅτι ἰσχύουν τὰ ἑξῆς:

   - $a|b \Leftrightarrow \nu_p(a) \leq \nu_p(b) \ \ \forall p \in \mathbb{P}$
   - $\nu_p(ab) = \nu_p(a) + \nu_p(b)$
   - $\nu_p(a^n) = n\nu_p(a)$

3. Συζητήσαμε τὴ λύση τῆς Διοφαντικῆς ἐξίσωσης $x^2 - y^2 = 24$ σὲ θετικοὺς ἀκεραίους x, y. Ὕστερα, δυσκολεύοντας λίγο τὰ πράγματα, ἀσχοληθήκαμε μὲ τὴν $x^2 - y^2 = z^n$, σὲ θετικοὺς ἀκεραίους x, y, z, μὲ τοὺς x, y πρώτους μεταξύ τους (ὁ n θεωρεῖται δεδομένος ἀκέραιος ≥ 2). Βασικὸ ἐργαλεῖο εἶναι ἡ ἑξῆς ἁπλῆ, ἀλλὰ ἐξαιρετικὰ σημαντική, πρόταση:

Πρόταση Ἂν $a, b \in \mathbb{N}$ εἶναι πρῶτοι μεταξύ τους καὶ $ab = c^n$, ὅπου $c \in \mathbb{N}$ καὶ n εἶναι δεδομένος ἀκέραιος, τότε ὑπάρχουν $c_1, c_2 \in \mathbb{N}$, πρῶτοι μεταξύ τους, ἔτσι ὥστε νὰ ἰσχύουν οἱ σχέσεις:

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

Γιὰ τὴν ἐπίλυση τῆς ἐξίσωσης $x^2 - y^2 = z^n$, ποὺ ἀναφέρθηκε παραπάνω, διακρίναμε τὶς περιπτώσεις: (α′) Ὁ ἕνας ἐκ τῶν x, y νὰ εἶναι ἄρτιος καὶ ὁ ἄλλος περιττός, καὶ (β′) Οἱ x, y νὰ εἶναι καὶ οἱ δύο περιττοί.
Βάσει αὐτῶν μπορεῖτε νὰ λύσετε πλήρως (οἱ λύσεις ἐκφράζονται συναρτήσει δύο παραμέτρων) τὴν ἐξίσωση· βλ. ἄσκηση 4.

Ἀσκήσεις

1. Ἔστω πολυώνυμο $g(X) \in \mathbb{Q}[X]$ ἀνάγωγο καὶ $\xi \in \mathbb{C}$ ρίζα τοῦ $g(X)$. Ἂν τὸ ξ εἶναι ρίζα καὶ κάποιου ἄλλου πολυωνύμου $f(X) \in \mathbb{Q}[X]$, τότε τὸ $g(X)$ διαιρεῖ τὸ $f(X)$ (στὸν δακτύλιο $\mathbb{Q}[X]$).
   Μὲ τὶς ἴδιες ὑποθέσεις, συμπεράνατε τὸ ἑξῆς: Ἂν $\xi' \in \mathbb{C}$ εἶναι μιὰ ἄλλη ρίζα τοῦ $g(X)$, τότε καὶ $f(\xi') = 0$.

2. Ἔστω ὅτι $a, b, m, n \in \mathbb{N}$, οἱ m, n εἶναι πρῶτοι μεταξύ τους καὶ $a^m = b^n = c$. Ἀποδεῖξτε ὅτι ὁ c εἶναι mn-οστὴ δύναμη.

3. Ἔστω ὅτι οἱ ἀκέραιοι a, b εἶναι πρῶτοι μεταξύ τους. Ἀποδεῖξτε ὅτι, ἂν ὁ ἕνας εἶναι ἄρτιος καὶ ὁ ἄλλος περιττός, τότε $\text{ΜΚΔ}(a + b, a - b) = 1$, ἐνῶ ἂν καὶ οἱ δύο εἶναι περιττοί, τότε $\text{ΜΚΔ}(a + b, a - b) = 2$.
   Ὑπόδειξη. Στὴν περίπτωση ποὺ οἱ a, b εἶναι περιττοί, παρατηρῆστε ὅτι $b \equiv \pm a \pmod 4$. Ἂν ἰσχύει τὸ $+$, τότε ὁ $(a - b)/2$ εἶναι ἄρτιος καὶ ὁ $(a + b)/2$ εἶναι περιττός. Ἂν ἰσχύει τὸ $-$, τότε ὁ $(a + b)/2$ εἶναι ἄρτιος καὶ ὁ $(a - b)/2$ εἶναι περιττός.

4. Ἔστω n δεδομένος θετικὸς ἀκέραιος. Νὰ ἐκφράσετε συναρτήσει δύο ἀκεραίων παραμέτρων τὶς λύσεις (x, y, z) τῆς Διοφαντικῆς ἐξίσωσης $x^2 - y^2 = z^n$, στὴν ὁποία $x, y, z \in \mathbb{N}$ καὶ οἱ x, y εἶναι πρῶτοι μεταξύ τους.
   Ὑπόδειξη. Παραγοντοποιῆστε τὸ ἀριστερὸ μέλος καὶ χρησιμοποιεῖστε τὴν ἄσκηση 3 καὶ τὴν Πρόταση, ποὺ ἀναφέρω παραπάνω.

Ἀναφορὲς

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