Η Θεωρια Αριθμων στην Εκπαιδευση

Καθηγητὴς Ν.Γ. Τζανάκης

Ἄθροισμα δύο τετραγώνων

Θεώρημα 1. *Ἔστω ἀκέραιος $n > 1$ καὶ $l^2 \equiv -1 \pmod{n}$. Τότε, ὑπάρχει ἕνα, ἀκριβῶς ζεῦγος (x, y) ἀκεραίων ποὺ ἱκανοποιεῖ ὅλες τὶς παρακάτω συνθῆκες:*

$$x > 0,\ y > 0,\ (x, y) = 1, \quad y \equiv lx \pmod{n}, \quad x^2 + y^2 = n.$$

Θεώρημα 2. *Ἔστω $n \in \mathbb{N}$ καὶ $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, ὅπου $k_0 \geq 0$, $r \geq 0$, ἀλλὰ τὰ k_0 καὶ r δὲν εἶναι συγχρόνως μηδὲν καί, στὴν περίπτωση ποὺ $r \geq 1$, οἱ $p_1, \ldots, p_r$ εἶναι διαφορετικοὶ περιττοὶ πρῶτοι καὶ οἱ ἐκθέτες $k_1, \ldots, k_r$ εἶναι ὅλοι θετικοί. Τότε, τὸ πλῆθος $V(n)$ τῶν διαφορετικῶν λύσεων τῆς ἰσοτιμίας $x^2 \equiv -1 \pmod{n}$ δίνεται ἀπὸ τὸν τύπο*

$$V(n) = \begin{cases} 0 & \text{ἂν } k_0 \geq 2 \text{ εἴτε } p_i \equiv 3 \pmod{4} \text{ γιὰ κάποιο } i \in \{1, \ldots, r\} \\ 2^r & \text{διαφορετικά} \end{cases}.$$

Συμβολισμός: Γιὰ κάθε $n \in \mathbb{N}$ συμβολίζομε μὲ $U(n)$ τὸ πλῆθος τῶν διατεταγμένων ζευγῶν $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, ποὺ ἱκανοποιοῦν τὴ σχέση $x^2 + y^2 = n$.

Θεώρημα 3.

$$U(n) = 4 \sum_{d^2 | n} V\left(\frac{n}{d^2}\right).$$

Χαρακτῆρες mod k. Ἡ συνάρτηση $\chi : \mathbb{Z} \to \mathbb{C}$ λέμε ὅτι εἶναι χαρακτήρας mod k ἂν ἱκανοποιεῖ ὅλες τὶς παρακάτω συνθῆκες:

1. $\chi(a) = 0$ γιὰ κάθε a μὲ $(a, k) > 1$.
2. $\chi(1) \neq 0$.
3. $\chi(ab) = \chi(a)\chi(b)$.
4. Ἂν $a_1 \equiv a_2 \pmod{k}$, τότε $\chi(a_1) = \chi(a_2)$.

Ἄμεσες συνέπειες τοῦ παραπάνω ὁρισμοῦ εἶναι ὅτι $\chi(1) = 1$ καί, γιὰ κάθε a πρῶτο πρὸς k, ὁ ἀριθμὸς $\chi(a)$ εἶναι $\phi(k)$-ρίζα τῆς μονάδας.

Εἶναι εὔκολο νὰ δοῦμε ὅτι ἡ συνάρτηση χ, ποὺ ὁρίζεται

$$\chi(a) = \begin{cases} 0 & \text{ἂν ὁ } a \text{ εἶναι ἄρτιος} \\ (-1)^{(a-1)/2} & \text{ἂν ὁ } a \text{ εἶναι περιττός} \end{cases}, \tag{1}$$

εἶναι χαρακτήρας mod 4.

Θεώρημα 4.

$$U(n) = 4 \sum_{d|n} \chi(d).$$

Ἡ σχέση αὐτὴ "διαβάζεται" καὶ ὡς ἑξῆς (πάντα, ὅταν γράφομε $d|n$ ἐννοοῦμε ὅτι ὁ d εἶναι θετικὸς *διαιρέτης τοῦ n):*

$$\tfrac{1}{4}U(n) = \sharp\{d|n \ \ \textit{καὶ} \ \ d \equiv 1 \pmod 4\} - \sharp\{d|n \ \ \textit{καὶ} \ \ d \equiv 3 \pmod 4\}$$