Αλγεβρα I

Καθηγητὴς Ν.Γ. Τζανάκης

Χειμερινὸ ἑξάμηνο 2015-2016

Βασικὴ περιγραφὴ τῶν θεμάτων ποὺ συζητήθηκαν τὴν 4$^{\eta}$ ἑβδομάδα

(Δὲν πρόκειται γιὰ λεπτομερῆ περιγραφή.)

• **Θεώρημα 1** ("Μικρὸ Θεώρημα τοῦ Fermat")**.** *Ἔστω πρῶτος p καὶ a ἀκέραιος μὴ διαιρετὸς διὰ p (ἰσοδύναμα, $(a,p)=1$). Τότε, στὸ $\mathbb{Z}_p$ ἰσχύει $[a]^{p-1}=[1]$. Ἡ τελευταία ἰσότητα κλάσεων ἰσοδυναμεῖ μὲ τὴν ἰσοτιμία $a^{p-1}\equiv 1 \pmod{p}$.*

• **Τὸ σύνολο $\mathbb{Z}_m^*$ τῶν ἀντιστρέψιμων κλάσεων τοῦ $\mathbb{Z}_m$.**

• **Πρόταση 2.** *(1) Ἂν $[a],[b]\in\mathbb{Z}_m^*$, τότε $[a][b]\in\mathbb{Z}_m^*$.*
(2) Ἂν $[a]\in\mathbb{Z}_m^*$, τότε $[a]^{-1}\in\mathbb{Z}_m$.

• **Συμβολισμός**: $|\mathbb{Z}_m^*|=\phi(m)$ ("συνάρτηση ϕ τοῦ Euler")
Ἀποδείξαμε, σὰν ἄσκηση, ὅτι, ἂν ὁ p εἶναι πρῶτος, τότε $\phi(p)=p-1$ καί, γενικότερα, $\phi(p^k)=p^k-p^{k-1}$ γιὰ κάθε $k\geq 1$.

• **Θεώρημα 3** ("Κινέζικο Θεώρημα")**.** *Ἔστω ὅτι $m_1,m_2>1$ καὶ $(m_1,m_2)=1$. Τότε, γιὰ ὁποιοδήποτε ζεῦγος ἀκεραίων a_1,a_2, ὑπάρχει ἀκέραιος b, τέτοιος ὥστε*

$$b\equiv a_1 \pmod{m_1} \quad \text{καὶ} \quad b\equiv a_2 \pmod{m_2}.$$

Ἂν γιὰ κάποιο ἄλλο b' ἰσχύει $b'\equiv a_1 \pmod{m_1}$ καὶ $b'\equiv a_2 \pmod{m_2}$, τότε

$$b'\equiv b \pmod{m_1m_2}.$$

• **Πρόταση 4.** *Ἔστω $(m_1,m_2)=1$ (m_1,m_2 ἀκέραιοι >1). Θεωροῦμε τὰ σύνολα $\mathbb{Z}_{m_1},\mathbb{Z}_{m_2}$ καὶ $\mathbb{Z}_{m_1m_2}$. Τὶς κλάσεις στὰ σύνολα αὐτὰ συμβολίζομε μὲ $[\ ]_{m_1}$, $[\ ]_{m_2}$, $[\ ]_{m_1m_2}$, ἀντιστοίχως. Θεωροῦμε, ἐπίσης, καὶ τὰ σύνολα τῶν ἀντιστρέψιμων κλάσεων $\mathbb{Z}_{m_1}^*\subset\mathbb{Z}_{m_1}$, $\mathbb{Z}_{m_2}^*\subset\mathbb{Z}_{m_2}$, $\mathbb{Z}_{m_1m_2}^*\subset\mathbb{Z}_{m_1m_2}$. Σὲ κάθε $([a_1]_{m_1},[a_2]_{m_2})\in\mathbb{Z}_{m_1}^*\times\mathbb{Z}_{m_2}^*$ ἀντιστοιχοῦμε τὴν κλάση $[b]_{m_1m_2}$, ὅπου $b\equiv a_i \pmod{m_i}$ γιὰ $i=1,2$. Ἡ ἀντιστοιχία αὐτὴ ὁρίζει μία ἀπεικόνιση $f:\mathbb{Z}_{m_1}^*\times\mathbb{Z}_{m_2}^*\to\mathbb{Z}_{m_1m_2}$, ἡ ὁποία εἶναι ἀμφιμονοσήμαντη. Συνεπῶς, $|\mathbb{Z}_{m_1}^*\times\mathbb{Z}_{m_2}^*|=|\mathbb{Z}_{m_1m_2}|$, ἄρα $|\mathbb{Z}_{m_1}^*|\cdot|\mathbb{Z}_{m_2}^*|=|\mathbb{Z}_{m_1m_2}|$.*

• **Πόρισμα 1** (Τύπος τοῦ $\phi(m)$)**.** *Ἔστω* $m > 1$ *καὶ* $m = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ *ἡ κανονικὴ ἀνάλυση τοῦ* m *σὲ πρώτους. Τότε*

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) = m\prod_{p|m}\left(1 - \frac{1}{p}\right).$$

Ἀναφορὲς

[1] Δ. Βάρσος, Δ. Δεριζιώτης, Γ. Εμμανουήλ, Μ. Μαλιάκας, Ο. Ταλέλλη, *Μια Εισαγωγή στην Άλγεβρα*, Γ΄ έκδοση, Εκδόσεις ΣΟΦΙΑ, Αθήνα 2012.