Αλγεβρικη Θεωρια Αριθμων

Φθινοπωρινὸ ἐξάμηνο 2006

Καθηγητὴς Ν. Γ. Τζανάκης

Ζ΄ Φυλλάδιο Ἀσκήσεων

Ασκησεις Επαναληψεως

1. Ἔστω K ἀριθμητικὸ σῶμα βαθμοῦ n. Ἀποδεῖξτε ὅτι, γιὰ κάθε φυσικὸ ἀριθμὸ a, τὸ πλῆθος τῶν ἀκεραίων ἰδεωδῶν τοῦ K στάθμης a εἶναι, τὸ πολύ, ἴσο μὲ τὸ πλῆθος τῶν n-άδων $(x_1, \ldots, x_n) \in \mathbb{Z}^n_{>0}$, οἱ ὁποῖες ἱκανοποιοῦν τὴ σχέση $x_1 \cdots x_n = a$.
Ὑπόδειξη. Ἂν $a = 1$, ὁ ἰσχυρισμὸς εἶναι προφανής. Ἔστω ὅτι $a > 1$ καὶ $p_1, \ldots, p_r$ εἶναι ὅλοι οἱ διαφορετικοὶ πρῶτοι διαιρέτες τοῦ a. Δεῖξτε ὅτι κάθε ἰδεῶδες (p_j) γράφεται ὡς γινόμενο $\mathfrak{p}_{j1} \cdots \mathfrak{p}_{jn}$, ὅπου κάθε $\mathfrak{p}_{ji}$ εἶναι, ἢ πρῶτο, ἢ ἴσο μὲ τὸ A (A ὁ δακτύλιος τῶν ἀκεραίων τοῦ K), δίχως νὰ εἶναι ὅλα τὰ $\mathfrak{p}_{j1}, \ldots, \mathfrak{p}_{jn}$ ἴσα μὲ A. Κάθε ἰδεῶδες μὲ στάθμη a εἶναι γινόμενο $\mathfrak{a}_1 \cdots \mathfrak{a}_n$, ὅπου $\mathfrak{a}_i = \mathfrak{p}_{1i}^{\alpha_{1i}} \cdots \mathfrak{p}_{ni}^{\alpha_{ni}}$, μὲ τοὺς α_{ji} μὴ ἀρνητικοὺς ἀκεραίους καί, ἂν $\mathfrak{p}_{ji} = A$, $\alpha_{ji} = 0$. Ἔστω $\mathrm{N}(\mathfrak{a}_i) = x_i \in \mathbb{N}$ κλπ.

2. Ἔστω K ἀριθμητικὸ σῶμα καὶ A ὁ δακτύλιος τῶν ἀκεραίων του. Γιὰ κάθε μὴ μηδενικὸ ἰδεῶδες $\mathfrak{a}$ τοῦ A συμβολίζομε μὲ $\phi(\mathfrak{a})$ τὸ πλῆθος τῶν διαφορετικῶν κλάσεων $x + \mathfrak{a}$ καθὼς τὸ x διατρέχει τὸ A καὶ τὸ ἰδεῶδες (x) εἶναι πρῶτο πρὸς τὸ $\mathfrak{a}$. Ὁ βασικὸς στόχος αὐτῆς τῆς ἀσκήσεως εἶναι νὰ ἀποδείξει ἕνα τύπο γιὰ τὴ συνάρτηση ϕ, ἀνάλογο μὲ τὸν γνωστὸ ἀπὸ τὴ στοιχειώδη Θεωρία Ἀριθμῶν τύπο τῆς *συνάρτησης ϕ τοῦ Euler* καὶ μία πρόταση ἀνάλογη μὲ τὸ θεώρημα (στὸ $\mathbb{Z}$) τοῦ Euler $a^{\phi(m)} \equiv 1 \pmod{m}$ ὅταν $(a, m) = 1$.

   (α΄) Ἔστω μὴ μηδενικὸ ἰδεῶδες $\mathfrak{a}$ τοῦ A. Ἀποδεῖξτε ὅτι τὸ $x + \mathfrak{a}$ εἶναι ἀντιστρέψιμο στοιχεῖο τοῦ δακτυλίου $A/\mathfrak{a}$ ἂν, καὶ μόνο ἄν, τὸ κύριο ἰδεῶδες (x) εἶναι πρῶτο πρὸς τὸ $\mathfrak{a}$.
   Ὑπόδειξη. Ἔχομε ’δεῖ διάφορες ἰσοδύναμες προτάσεις γιὰ τὸ πότε δύο ἰδεώδη $\mathfrak{a}, \mathfrak{b}$ εἶναι πρῶτα μεταξύ τους καὶ μία ἀπὸ αὐτὲς εἶναι, $\mathfrak{a} + \mathfrak{b} = A$.

   (β΄) Ἔστω ὅτι τὰ ἰδεώδη $\mathfrak{a}, \mathfrak{b}$ εἶναι πρῶτα μεταξύ τους. Ἀποδεῖξτε ὅτι ὁ κανονικὸς ὁμομορφισμὸς δακτυλίων $A \to A/\mathfrak{a} \times A/\mathfrak{b}$ ἐπάγει ἕναν ἰσομορφισμὸ τῶν δακτυλίων $A/\mathfrak{ab}$ καὶ $A/\mathfrak{a} \times A/\mathfrak{b}$. [1]

   (γ΄) Ἔστω ὅτι τὰ ἰδεώδη $\mathfrak{a}, \mathfrak{b}$ εἶναι πρῶτα μεταξύ τους. Ἀποδεῖξτε ὅτι $\phi(\mathfrak{ab}) = \phi(\mathfrak{a})\phi(\mathfrak{b})$.
   Ὑπόδειξη. Μία προφανὴς πρόταση τῆς στοιχειώδους Ἄλγεβρας εἶναι ὅτι, ἂν R, S εἶναι ἀντιμεταθετικοὶ δακτύλιοι μὲ μοναδιαῖο, τότε τὸ $(r, s) \in R \times S$ εἶναι ἀντιστρέψιμο στοιχεῖο τοῦ δακτυλίου $R \times S$ ἄν, καὶ μόνο ἄν, τὸ r εἶναι ἀντιστρέψιμο στοιχεῖο τοῦ R καὶ τὸ s εἶναι ἀντιστρέψιμο στοιχεῖο τοῦ S. Χρησιμοποιεῖστε, ἐπίσης, τὰ (α΄) καὶ (β΄).

[1] Στὴν πραγματικότητα, ἡ πρόταση αὐτὴ εἶναι γενικὴ καὶ ἰσχύει σὲ κάθε ἀντιμεταθετικὸ δακτύλιο μὲ μοναδιαῖο, ἡ δὲ συνθήκη νὰ εἶναι τὰ $\mathfrak{a}, \mathfrak{b}$ πρῶτα μεταξύ τους διατυπώνεται ὡς $\mathfrak{a} + \mathfrak{b} = A$.

(δ΄) Ἔστω $\mathfrak{p}$ πρῶτο ἰδεῶδες. Ἀποδεῖξτε ὅτι, γιὰ κάθε ἀκέραιο $k \geq 1$, ἰσχύει $|\mathfrak{p}/\mathfrak{p}^k| = \mathrm{N}(\mathfrak{p})^{k-1}$.

Ὑπόδειξη. Θεωρῆστε τὴν ἀλυσσίδα τῶν προσθετικῶν ὑποομάδων $\mathfrak{p}^k < \mathfrak{p} < A$. Ἕνα ἀπὸ τὰ *θεωρήματα ἰσομορφισμοῦ* τῶν Ὁμάδων λέει ὅτι, ἂν $K < H < G$ εἶναι ἀλυσσίδα ὑποομάδων μὲ $K \lhd G$ [2] καὶ $H \lhd G$, τότε $K \lhd H$, $H/K \lhd G/K$ καὶ $(G/K)/(H/K) \cong G/H$.

(ε΄) Ἔστω $\mathfrak{p}$ πρῶτο ἰδεῶδες καὶ $k \geq 1$ ἀκέραιος. Ἀποδεῖξτε ὅτι τὸ πλῆθος τῶν διαφορετικῶν κλάσεων $x + \mathfrak{p}^k$, ὅταν $x \in A$ καὶ $\mathfrak{p}|x$, εἶναι ἴσο μὲ $\mathrm{N}(\mathfrak{p})^{k-1}$. Ἐξ αὐτοῦ συμπεράνατε ὅτι $\phi(\mathfrak{p}^k) = \mathrm{N}(\mathfrak{p})^k - \mathrm{N}(\mathfrak{p})^{k-1}$.
Βασισθεῖτε στὸ (δ΄).

(ϛ΄) Χρησιμοποιεῖστε κάποια ἀπὸ τὰ προηγούμενα συμπεράσματα γιὰ νὰ καταλήξετε στὸν τύπο

$$\phi(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right) .$$

(ζ΄) Ἔστω ἰδεῶδες $\mathfrak{m}$ καὶ $\alpha \in A$ πρῶτο πρὸς τὸ $\mathfrak{m}$. Ἀποδεῖξτε ὅτι (γενίκευση τοῦ θεωρήματος τοῦ Euler τῆς στοιχειώδους Θεωρίας Ἀριθμῶν)

$$\alpha^{\phi(\mathfrak{m})} \equiv 1 \pmod{\mathfrak{m}} .$$

Ὑπόδειξη. Παρατηρῆστε ὅτι τὸ σύνολο τῶν κλάσεων $x + \mathfrak{m}$, καθὼς τὸ x διατρέχει τὸ A καὶ εἶναι πρῶτο πρὸς τὸ $\mathfrak{m}$, ἀποτελεῖ πολλαπλασιαστικὴ ὁμάδα τάξεως $\phi(\mathfrak{m})$.

(η΄) Μὲ ἐφαρμογὴ τοῦ (ζ) ἀποδεῖξτε ὅτι, ἂν ὁ ρητὸς πρῶτος p ἀναλύεται πλήρως στὸ K (δηλαδή, εἶναι γινόμενο n διαφορετικῶν πρώτων ἰδεωδῶν τοῦ K), τότε, γιὰ κάθε $\alpha \in A$ πρῶτο πρὸς τὸν p ἰσχύει

$$\alpha^{p^n - 1} \equiv 1 \pmod{p} \quad \text{(ἰσοτιμία στὸ } A\text{)}.$$

3. Ἀποδεῖξτε ὅτι ὅλες οἱ ἀκέραιες λύσεις (x, y) τῆς ἐξίσωσης $17x^2 + 32xy + 14y^2 = 9$ δίνονται ἀπὸ τοὺς τύπους

$$17x + 16y + 3\sqrt{2}y = \pm(15 + 6\sqrt{2})(3 + 2\sqrt{2})^n , \quad n \in \mathbb{Z} .$$

Ὑπόδειξη. Μὴ ξεχνᾶτε τὴ σχολικοῦ ἐπιπέδου συνεπαγωγή, $ax^2 + 2bxy + cy^2 = m \Rightarrow (ax + by)^2 - Dy^2 = am$, ὅπου $D = b^2 - ac$.

4. Ἡ ἄσκηση αὐτὴ χρειάζεται τὴ θεωρία παραγοντοποίησης σὲ τετραγωνικὸ σῶμα. Ἡ ἀπόδειξη τῶν ἰσχυρισμῶν της μὲ στοιχειώδη μέσα εἶναι δύσκολη.

(α΄) Ἀποδεῖξτε ὅτι ὁ πρῶτος $p > 5$ γράφεται ὑπὸ τὴ μορφὴ $x^2 + 5y^2$ ($x, y \in \mathbb{Z}$) ἂν, καὶ μόνο ἂν, $p \equiv 1, 9 \pmod{20}$.

(β΄) Ἀποδεῖξτε ὅτι ὁ πρῶτος $p > 5$ γράφεται ὑπὸ τὴ μορφὴ $2x^2 + 2xy + 3y^2$ ($x, y \in \mathbb{Z}$) ἂν, καὶ μόνο ἂν, $p \equiv 3, 7 \pmod{20}$.

[2] $\lhd$ σημαίνει κανονικὴ ὑποομάδα.