

Ασκήσεις Πεπερασμένων Σωμάτων και κρυπτογραφίας  
2 Φυλλάδιο

Παράδοση 30 Απριλίου 2012

**Άσκηση 1.** Να υπολογιστεί το πλήθος των αναγώγων πολυωνύμων βαθμού 24 πάνω από ένα σώμα με  $q$  το πλήθος στοιχείων.

**Λύση:** Το πλήθος των αναγώγων πολυωνύμων βαθμού 24 πάνω από το  $\mathbb{F}_q$  είναι ίσο με

$$\begin{aligned} a_q(24) &= \frac{1}{24} \sum_{d|24} \mu(d) q^{n/d} \\ &= \frac{1}{24} (\mu(1)q^{24} + \mu(2)q^{12} + \mu(3)q^8 + \mu(4)q^6 + \mu(6)q^4 + \mu(8)q^3 + \mu(12)q^2 + \mu(24)q) \\ &= \frac{1}{24} (q^{24} - q^{12} - q^8 + q^4). \end{aligned}$$

**Άσκηση 2.** Για κάθε διαιρέτη  $k$  του  $2^4 - 1 = 15$  να υπολογίστουν οι πρωταρχικές  $k$  ρίζες του 1 σε κατάλληλες επεκτάσεις του σώματος με 2 στοιχεία. Υπόδειξη: Το  $x^4 + x + 1$  είναι ένα πρωταρχικό πολυώνυμο.

**Λύση:** Αφού  $k \mid 2^4 - 1$  έχουμε  $x^k - 1 \mid x^{2^4-1} - 1$ , οπότε αρκεί να βρεθούν οι  $k$ -πρωταρχικές ρίζες πάνω στο  $\mathbb{F}_{2^4}$ .

Θεωρούμε το  $p(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ . Αυτό είναι ανάγωγο γιατί το 0 και το 1 δεν είναι ρίζες του. Άρα αν δεν ήταν ανάγωγο τότε θα γράφονταν ως γινόμενο δύο δευτοβαθμίων πολυωνύμων. Δηλαδή:

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (b+d+ca)x^2 + (ad+cb)x + bd.$$

Από την σύγκριση των σταθερών όρων έχουμε ότι  $b = d = 1$ , ενώ από την σύγκριση του κυβικού όρου έχουμε ότι  $a = c = 1$  ή  $a = c = 0$ . Η τελευταία περίπτωση πρέπει να αποκλειστεί γιατί τότε το  $x^2 + 1 = (x+1)^2$  θα ήταν παράγοντας του  $x^4 + x + 1$  άρα το  $x = 1$  θα ήταν ρίζα. Άρα  $a = c = 1$  και καταλήγουμε σε άτοπο συγκρίνοντας τους συντελεστές του  $x^2$  ή  $x$ .

Συνεπώς

$$\mathbb{F}_{2^4} = \mathbb{F}_2[x]/x^4 + x + 1.$$

Παρατηρούμε ότι αν  $x$  ρίζα του  $x^4 + x + 1$  τότε οι δυνάμεις του  $x$  παράγουν το  $\mathbb{F}_{2^4}^*$ . Πράγματι  $|\mathbb{F}_{2^4}^*| = 2^4 - 1 = 15$ . Άρα οι πιθανές τάξεις της κυκλικής ομάδας που παράγει το  $x$  είναι 1, 3, 5 ή 15. Η τάξη του  $x$  δεν είναι ένα ούτε 3. Θα πρέπει να αποκλείσουμε  $x^5 - 1 \neq 0 \pmod{x^4 + x + 1}$ . Αυτό όμως είναι εύκολο αφού  $x^4 = x + 1$  συνεπώς  $x^5 = x^2 + x$  και  $x^5 - 1 = x^2 + x + 1$  το οποίο δεν είναι 0 αφού είναι βαθμού μικρότερου του 4.

Για κάθε  $k \mid 15$  οι πρωταρχικές  $k$ -ρίζες είναι  $x^{15i/k}$  όπου  $(i, k) = 1$  και  $i < k$ . Έτσι για  $k = 15$  έχουμε τα  $x^i$  με  $(i, 15) = 1$   $i < 15$  δηλαδή  $i = 1, 2, 4, 7, 8, 11, 12, 13, 14$ .

Για  $k = 5$  έχουμε τα  $x^{3i}$  με  $(i, 5) = 1$  και  $i < 5$  δηλαδή  $i = 1, 2, 3, 4$ .

Για  $k = 3$  έχουμε τα  $x^{5i}$  με  $(i, 3) = 1$  και  $i < 3$  δηλαδή  $i = 1, 2$ .

Για  $k = 15$  έχουμε το  $x^{15} = 1$ .

**Άσκηση 3.** Να υπολογιστούν τα κυκλοτομικά πολυώνυμα τάξης μέχρι 12 πάνω

από ένα σώμα που έχει χαρακτηριστική  $p > 12$ .

**Λύση:** Θα χρησιμοποιήσουμε τον τύπο  $\prod_{d|n} \Phi_d(X) = x^n - 1$ , όπου  $\Phi_d(x)$  είναι το κυκλοτομικό πολυώνυμο τάξης  $d$ .

Έτσι:

$$n = 1 \text{ έχουμε } \Phi_1(x) = x - 1.$$

$$n = 2 \text{ έχουμε } \Phi_2(x) = (x^2 - 1)/(x - 1) = x + 1.$$

$$n = 3 \text{ έχουμε } \Phi_3(x) = (x^3 - 1)/(x - 1) = x^2 + x + 1$$

$$n = 4 \text{ έχουμε } \Phi_4(x) = \frac{x^4 - 1}{\Phi_2 \Phi_1} = x^2 + 1$$

$$n = 5 \text{ έχουμε } \Phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$$

$$n = 6 \text{ έχουμε } \Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6 - 1}{(x^3 - 1)(x + 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1.$$

$$n = 7 \text{ έχουμε } \Phi_7(x) = (x^7 - 1)/(x - 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$n = 8 \text{ έχουμε } \Phi_8(x) = \frac{x^8 - 1}{\prod_{d=1,2,3,4} \Phi_d(x)} = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1$$

$$n = 9 \text{ έχουμε } \Phi_9(x) = \frac{x^9 - 1}{\prod_{d=1,3} \Phi_d(x)} = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1$$

$$n = 10 \text{ έχουμε } \Phi_{10}(x) = \frac{x^{10} - 1}{\prod_{d=1,2,5} \Phi_d(x)} = \frac{x^{10} - 1}{(x^5 - 1)(x + 1)} = \frac{x^5 + 1}{x + 1} = x^4 - x^3 + x^2 - x + 1$$

$$n = 11 \text{ έχουμε } \Phi_{11}(x) = \sum_{i=0}^{10} x^i.$$

$$n = 12 \text{ έχουμε } \Phi_{12}(x) = \frac{x^{12} - 1}{\prod_{d=1,2,3,4,6} \Phi_d(x)} = \frac{x^{12} - 1}{(x^6 - 1)\Phi_4(x)} = \frac{x^6 + 1}{x^2 + 1} = x^4 - x^2 + 1.$$

**Άσκηση 4.** Να αποδειχτεί ότι τα κυκλοτομικά πολυώνυμα ενός σώματος με  $p^h$  στοιχεία έχουν συντελεστές που ανήκουν στο σώμα με  $p$  το πλήθος στοιχεία.

**Λύση:** Παρατηρούμε ότι  $L/K$  επέκταση σωμάτων,  $f \in L[x]$   $fg \in K[x]$  και  $g \in K[x]$  τότε και  $f \in K[x]$ . Πράγματι  $f = \frac{fg}{g} \in K(x)$ , όπου  $K(x)$  είναι το σώμα πηλίκων της απ. περιοχής  $K[x]$ . Όμως το  $f$  είναι πολυώνυμο συνεπώς  $f \in K[x]$ .

Η απόδειξη γίνεται με επαγωγή. Το  $\Phi_1(x) = x - 1 \in \mathbb{F}_p$ . Υποθέτουμε ότι  $\Phi_d(x) \in \mathbb{F}_p[x]$  για κάθε  $d \leq n - 1$  οπότε

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} \Phi_d(x)} \in \mathbb{F}_p[x].$$

**Άσκηση 5.** Να αποδειχτεί ότι το  $n$  κυκλοτομικό πολυώνυμο δίνεται από τον τύπο

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)},$$

όπου  $\mu$  είναι η πολλαπλασιαστική συνάρτηση του Möbius

$$\mu(m) = \begin{cases} 1 & \text{αν } m = 1 \\ (-1)^k & \text{αν το } m \text{ διασπάται σε γινόμενο } k \text{ διαφορετικών πρώτων} \\ 0 & \text{αν το } m \text{ διαιρείται με τετράγωνο} \end{cases}$$

**Λύση:** Υπολογίζουμε:

$$\prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n} \left( \prod_{t|\frac{n}{d}} \Phi_t(x) \right)^{\mu(d)} = \prod_{t|n} \prod_{d|\frac{n}{t}} \Phi_t(x)^{\mu(d)} =$$

$$\prod_{t|n} \Phi_t(x)^{\sum_{d|\frac{n}{t}} \mu(d)} = \Phi_n(x),$$

γιατί

$$\sum_{k|n} \mu(k) = \begin{cases} 0 & \text{αν } n > 1 \\ 1 & \text{αν } n = 1 \end{cases}$$