Πεπερασμένα Σώματα και Κωδικοποίηση

ΕΡΓΑΣΙΑ Ε

Ονομ/νο: Νούλας Δημήτριος
ΑΜ: 1112201800377
email: dimitriosnoulas@gmail.com

(1) Να βρεθούν όλοι οι κυκλικοί κώδικες μήκους 11 επί του σώματος $\mathbb{Z}_3$. Για κάθε έναν από αυτούς να βρείτε το πολυώνυμο ελέγχου και έναν αδύναμο γεννήτορα. Ποιοι απ' αυτούς είναι ελάχιστοι, ποιοι μέγιστοι· Να κάνετε ένα διάγραμμα όπου να διατάξετε όλους αυτούς τους κώδικες ως προς τη σχέση 'του περιέχεσθαι'. (Θεωρήστε γνωστό ότι $x^{11} - 1 = (x - 1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1)$.)

(2) (i) Έστω $\mathcal{C}$ ένας κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι ο $\mathcal{C}$ είναι αυτο-ορθογώνιος (δηλαδή $\mathcal{C} \subseteq \mathcal{C}^{\perp}$). Δείξτε ότι το $x - 1$ διαιρεί το $\gamma(x)$.

(ii) Δείξτε ότι ένας αυτο-ορθογώνιος κυκλικός κώδικας είναι κώδικας μηδενικού αθροίσματος.

(3) Δείξτε ότι το πολυώνυμο $x^{2^n} - x \in \mathbb{Z}_2[x]$ αναλύεται σε γινόμενο όλων των αναγώγων πολυωνύμων με συντελεστές από το $\mathbb{Z}_2$ με βαθμό που διαιρεί το n.

(1) Έστω $\mathcal{R}_{11} = \mathbb{Z}_3[x]/ < x^{11} - 1 >$

$$x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 = 1)(x^5 - x^3 + x^2 - x - 1)$$

Οι κυκλικοί κώδικες μήκους 11 επί του σώματος $\mathbb{Z}_3$ είναι τα κύρια ιδεώδη του δακτυλίου $\mathcal{R}_{11}$, ωστόσο ένα κύριο ιδεώδες μπορεί να παράγεται από περισσότερα του ενός πολυώνυμα. Από θεώρημα, για έναν κυκλικό κώδικα $\mathcal{C}$ υπάρχει μοναδικό πολυώνυμο $\gamma(x) \in \mathcal{R}_{11}$ τέτοιο ώστε το $\gamma(x)$ είναι ελαχίστου βαθμού, $\mathcal{C} =< \gamma(x) >$ και $\gamma(x) \mid x^{11} - 1$. Το $\gamma(x)$ είναι το λεγόμενο πολυώνυμο γεννήτορας.

Από δεύτερο θεώρημα, ένα μονικό $g(x) \in \mathcal{R}_{11}$ είναι πολυώνυμο γεννήτορας ενός κυκλικού κώδικα $\mathcal{C} \subseteq \mathcal{R}_{11}$ αν και μόνο αν $g(x) \mid x^{11} - 1$.

Συνεπώς όλοι οι ζητούμενοι κυκλικοί κώδικες είναι τα κύρια ιδεώδη που προκύπτουν από τους διαιρέτες του $x^{11} - 1$ και επειδή το $x^{11} - 1$ αναλύεται σε τρεις παράγοντες έχουμε 2^3 διαιρέτες. Δηλαδή:

$$\mathcal{C}_0 =< x^{11} - 1 >= \{0\}$$
$$\mathcal{C}_1 =< (x-1)(x^5 + x^4 - x^3 + x^2 - 1) >=< x^6 + x^4 - x^3 - x + 1 >:=< \gamma_1(x) >$$
$$\mathcal{C}_2 =< (x-1)(x^5 - x^3 + x^2 - x - 1) >=< x^6 - x^5 - x^4 - x^3 + x^2 + 1 >:=< \gamma_2(x) >$$
$$\mathcal{C}_3 =< x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 >:=< \gamma_3(x) >$$
$$\mathcal{C}_4 =< x - 1 >:=< \gamma_4(x) >$$
$$\mathcal{C}_5 =< x^5 + x^4 - x^3 + x^2 - 1 >:=< \gamma_5(x) >$$
$$\mathcal{C}_6 =< x^5 - x^3 + x^2 - x - 1 >:=< \gamma_6(x) >$$
$$\mathcal{C}_7 =< 1 >= \mathcal{R}_{11}$$

Επιπλέον, έχουμε για κάθε πολυώνυμο γεννήτορα $\gamma(x)$ ένα μοναδικό πολυώνυμο ελέγχου $\delta(x)$ τέτοιο ώστε $\gamma(x) \cdot \delta(x) = x^{11} - 1$. Από την σχέση $\gamma(x)\delta(x) = x^n - 1$ έπεται ότι μκδ$(\gamma(x), \delta(x)) = 1$ εφόσον το $x^n - 1$ έχει μόνο απλές ρίζες, τις n-οστές ρίζες της μονάδας. Επομένως, κάθε ανάγωγος παράγοντας του θα είναι διαιρέτης είτε του $\gamma(x)$ είτε του $\delta(x)$. Άρα το $\delta(x)$ του κάθε κώδικα αποτελείται από το γινόμενο των παραγόντων του $x^{11} - 1$ που δεν διαιρούν το αντίστοιχο $\gamma(x)$.

Κυκλικός κώδικας	Πολυώνυμο ελέγχου
$\mathcal{C}_0$	1
$\mathcal{C}_1$	$\gamma_6(x)$
$\mathcal{C}_2$	$\gamma_5(x)$
$\mathcal{C}_3$	$\gamma_4(x)$
$\mathcal{C}_4$	$\gamma_3(x)$
$\mathcal{C}_5$	$\gamma_2(x)$
$\mathcal{C}_6$	$\gamma_1(x)$
$\mathcal{C}_7$	$x^{11} - 1$

Για να βρούμε έναν αδύναμο γεννήτορα του κάθε κυκλικού κώδικα πρέπει να εκφράσουμε το 1 ως γραμμικό συνδυασμό των $\gamma(x), \delta(x)$. Αυτό είναι εφικτό εφόσον μκδ$(\gamma(x), \delta(x)) = 1$ έχουμε ότι υπάρχουν $a(x), b(x) \in \mathcal{R}_{11}$ τέτοια ώστε $a(x)\gamma(x) + b(x)\delta(x) = 1$. Τότε ο μοναδικός αδύναμος γεννήτορας του κάθε κώδικα θα είναι το $e(x) = a(x)\gamma(x)$. Είναι πράγματι μοναδικός γιατί είναι το ουδέτερο στοιχείο του κυκλικού κώδικα $\mathcal{C}$ ως δακτυλίου, αφού για ένα στοιχείο $c(x)$ του κυκλικού κώδικα $\mathcal{C}$ έχουμε:

$$a(x)\gamma(x) + b(x)\delta(x) = 1 \implies c(x)a(x)\gamma(x) + c(x)\delta(x)b(x) = c(x) \quad mod(x^{11} - 1)$$

Δηλαδή $e(x)c(x) = c(x)$, αφού το $c(x)$ είναι στοιχείο του κώδικα και το $\delta(x)$ είναι το πολυώνυμο ελέγχου.

Συνεπώς χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο εύρεσης μεγίστου κοινού διαιρέτη για τους κώδικες $\mathcal{C}_i, i = 1, \ldots, 6$ και πηγαίνοντας προς τα πίσω έχουμε τους εξής γραμμικούς συνδυασμούς του 1:

$$\Big(x^4 + x^3 + x^2 + 2x\Big)\gamma_1(x) + \Big(2x^5 + 2x^4 + x^2 + 2\Big)\Big(x^5 + 2x^3 + x^2 + 2x + 2\Big) = 1$$

$$\Big(x^4 + x^3 + 1\Big)\gamma_2(x) + \Big(2x^5 + x^4 + x^2\Big)\Big(x^5 + x^4 + 2x^3 + x^2 + 2\Big) = 1$$

$$2\gamma_3(x) + \Big(x^9 + 2x^8 + x^6 + 2x^5 + x^3 + 2x^2 + 1\Big)\Big(x + 2\Big) = 1$$

$$\Big(x^9+2x^8+x^6+2x^5+x^3+2x^2+1\Big)\gamma_4(x)+2\Big(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1\Big) = 1$$

$$\Big(2x^5 + x^4 + x^2\Big)\gamma_5(x) + \Big(x^4 + x^3 + 1\Big)\Big(x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1\Big) = 1$$

$$\Big(2x^5 + 2x^4 + x^2 + 2\Big)\gamma_6(x) + \Big(x^4 + x^3 + x^2 + 2x\Big)\Big(x^6 + x^4 + 2x^3 + 2x + 1\Big) = 1$$

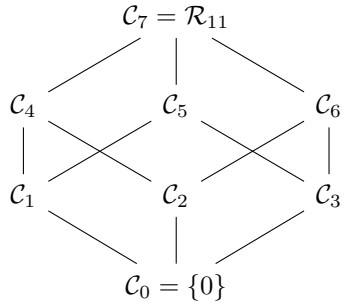
(Για την αποφυγή λαθών στις πράξεις οι γραμμικοί συνδυασμοί βρέθηκαν με την χρήση ΄κώδικα΄ του μαθηματικού πακέτου Sage της γλώσσας προγραμματισμού python. Με αυτό προσομοιώνονται η διαδικασία εύρεσης μεγίστου κοινού διαιρέτη και οι πράξεις πηγαίνοντας προς τα πίσω. Ο ΄κώδικας΄ παρατίθεται στο τέλος της εργασίας.)

Κυκλικός κώδικας	Αδύναμος γεννήτορας
$\mathcal{C}_0$	0
$\mathcal{C}_1$	$x^{10} + x^9 + 2x^8 + 2x^7 + x^4 + 2x^2 + 2x$
$\mathcal{C}_2$	$x^{10} + x^8 + x^7 + x^6 + x^2 + 1$
$\mathcal{C}_3$	$2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2$
$\mathcal{C}_4$	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 2$
$\mathcal{C}_5$	$2x^{10} + 2x^8 + 2x^7 + 2x^6 + 2x^2$
$\mathcal{C}_6$	$2x^{10} + 2x^9 + x^8 + x^7 + 2x^4 + x^2 + x + 1$
$\mathcal{C}_7$	1

Αν $x^{11} - 1 = \prod_{i=1}^{3} m_i(x) = \gamma_4(x)\gamma_5(x)\gamma_6(x)$ όπου τα $m_i(x)$ είναι μονικά ανάγωγα, έχουμε ότι οι κυκλικοί κώδικες της μορφής $< m_i(x) >$ είναι μέγιστοι και αντίστοιχα οι κυκλικοί κώδικες της μορφής $< \frac{x^{11}-1}{m_i(x)} >$ είναι ελάχιστοι. Συνεπώς οι μέγιστοι κυκλικοί κώδικες (εκτός από τον ίδιο τον δακτύλιο $\mathcal{R}_{11}$) είναι οι $\mathcal{C}_4, \mathcal{C}_5, \mathcal{C}_6$ και αντίστοιχα οι ελάχιστοι

(εκτός από τον τετριμμένο) είναι οι $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$.

Επιπλέον αν ένας κυκλικός κώδικας έχει γεννήτορα πολυώνυμο $\gamma(x)$ που δεν είναι ανάγωγο τότε από τον ορισμό του ιδεωδούς αυτός περιέχεται στους κυκλικούς κώδικες που έχουν γεννήτορα πολυώνυμο τους ανάγωγους παράγοντες του $\gamma(x)$. Συνεπώς έχουμε το ακόλουθο διάγραμμα ως προς την σχέση του ΄περιέχεσθαι΄:



(2) (i) Έστω κυκλικός κώδικας $\mathcal{C} \subseteq \mathcal{R}_n$ με γεννήτορα πολυώνυμο $\gamma(x)$. Έχουμε $\mathcal{C} =< \gamma(x) >$ και γνωρίζουμε ότι υπάρχει μοναδικό πολυώνυμο ελέγχου $\delta(x) \in \mathcal{R}_n$, δηλαδή:

$$x^n - 1 = \gamma(x)\delta(x)$$

με $\mathcal{R}_n = \mathbb{F}[x]/ < x^n - 1 >$ για κάποιο πεπερασμένο σώμα $\mathbb{F}$.

Από το θεώρημα 3.2.16 γνωρίζουμε ότι ο κώδικας $C^{\perp}$ είναι επίσης κυκλικός και ένα από τα πολυώνυμα που τον παράγουν είναι το αμοιβαίο πολυώνυμο του $\delta(x)$, δηλαδή το $\delta^*(x) = x^k\delta(x^{-1})$ όπου $k = deg\,(\delta(x))$. (Δεν είναι αναγκαστικά το πολυώνυμο γεννήτορας καθώς δεν είναι μονικό, αν πολλαπλασιάσουμε με τον αντίστροφο συντελεστή του σταθερού όρου του $\delta(x)$ τότε παίρνουμε το πολυώνυμο γεννήτορα.)

Θεωρούμε τον ομομορφισμό εκτίμησης:

$$\phi_1 : \mathcal{R}_n \longrightarrow \mathbb{F}$$

$$g(x) \longmapsto g(1)$$

Εφαρμόζοντας τον ϕ_1 στην παραπάνω πολυωνυμική σχέση παίρνουμε ότι:

$$\gamma(1)\delta(1) = 0_{\mathbb{F}}$$

Εφόσον το $\mathbb{F}$ είναι σώμα και άρα ακέραια περιοχή έχουμε ότι $\gamma(1) = 0$ ή $\delta(1) = 0$.

Αν ισχύει ότι $\gamma(1) = 0$ αυτό σημαίνει ότι το 1 είναι ρίζα του $\gamma(x)$ στο $\mathcal{R}_n$, δηλαδή:

$$x - 1 \mid \gamma(x) \quad \text{στο } \mathcal{R}_n$$

Διαφορετικά, αν $\delta(1) = 0$ θεωρούμε το $\delta(x)$ να έχει μορφή $\delta(x) = x^k + a_{k-1}x^{k-1} + \ldots a_1x + a_0 \in \mathcal{R}_n$. Τότε:

$$\delta(1) = \delta^*(1) = 1 + a_{k-1} + \ldots a_1 + a_0 = 0_{\mathbb{F}}$$

δηλαδή το 1 είναι επιπλέον ρίζα και του $\delta^*(x)$ στο $\mathcal{R}_n$. Επομένως:

$$x - 1 \mid \delta^*(x) \quad \text{στο } \mathcal{R}_n$$

(Γενικότερα ισχύει ότι a ρίζα του $g(x) \iff a^{-1}$ ρίζα του $g^*(x)$.)

Επιπλέον έχουμε ότι ο κώδικας $\mathcal{C}$ είναι αυτο-ορθογώνιος, δηλαδή:

$$< \gamma(x) > \subseteq < \delta^*(x) >$$

Εφόσον το $\mathcal{C}$ περιέχεται στο $\mathcal{C}^{\perp}$, θα περιέχεται και το $\gamma(x)$ στο $\mathcal{C}^{\perp}$. Δηλαδή, υπάρχει πολυώνυμο $g(x) \in \mathcal{R}_n$ τέτοιο ώστε $\delta^*(x)g(x) = \gamma(x) \pmod{x^n - 1}$. Συνεπώς, έχουμε ότι $\delta^*(x) \mid \gamma(x)$ και $x - 1 \mid \delta^*(x)$ στο $\mathcal{R}_n$, τα οποία συνεπάγουν ότι $x - 1 \mid \gamma(x)$.

Σε κάθε περίπτωση δηλαδή παίρνουμε το αποτέλεσμα $x - 1 \mid \gamma(x)$ στο $\mathcal{R}_n$.

(ii) Από το προηγούμενο ερώτημα, αν ένας κυκλικός κώδικας $\mathcal{C}$ με γεννήτορα πολυώνυμο $\gamma(x)$ είναι αυτο-ορθογώνιος, τότε $x-1 \mid \gamma(x)$ στο $\mathcal{R}_n$. Επιπλέον, έχουμε ότι υπάρχει $g(x) \in \mathcal{R}_n$ τέτοιο ώστε $\gamma(x) = (x-1)g(x) \in < (x-1) >$. Συνεπώς:

$$\mathcal{C} = < \gamma(x) > \subseteq < x-1 >$$

Αρκεί να δειχτεί ότι ο κυκλικός κώδικας $< x-1 >$ είναι κώδικας μηδενικού αθροίσματος. Πράγματι, έστω $p(x) \in < x-1 >$. Υπάρχει $g(x) = a_0 + a_1 x + \ldots a_{n-1}x^{n-1} \in \mathcal{R}_n$ τέτοιο ώστε:

$$p(x) = (x-1)g(x) \mod (x^n - 1)$$

Δηλαδή:

$$\begin{aligned} p(x) = (x-1)(a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}) &= a_0 x + a_1 x^2 + \ldots + a_{n-1}x^n \\ &\quad -a_0 - a_1 x - \ldots - a_{n-1}x^{n-1} \\ = -a_0 + (a_0 - a_1)x + (a_1 - a_2)x^2 + \ldots + (a_{n-2} - a_{n-1})x^{n-1} &+ a_{n-1}x^n \end{aligned}$$

Προσθαφαιρούμε το a_{n-1} στο τέλος της παραπάνω παράστασης και έτσι έχουμε

$$a_{n-1}x^n - a_{n-1} = 0 \mod (x^n - 1)$$

Άρα $p(x) = (a_{n-1} - a_0) + (a_0 - a_1)x + \ldots + (a_{n-2} - a_{n-1})x^{n-1} \mod (x^n - 1)$. Συνεπώς το τυχόν στοιχείο $p(x)$ αντιστοιχεί στην κωδικολέξη:

$$(a_{n-1} - a_0)(a_0 - a_1)\ldots(a_{n-2} - a_{n-1})$$

η οποία είναι μηδενικού αθροίσματος και άρα έπεται το ζητούμενο.

(3) Θα αποδειχτεί το γενικότερο αποτέλεσμα ότι για κάθε πρώτο p το πολυώνυμο $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ αναλύεται σε γινόμενο όλων των αναγώγων μονικών πολυωνύμων με συντελεστές από το $\mathbb{Z}_p$ με βαθμό που διαιρεί το n.

Καθώς το $\mathbb{Z}_p$ είναι σώμα, η ανάλυση του $f(x)$ σε ανάγωγους μονικούς παράγοντες γίνεται κατά τρόπο ουσιαστικά μοναδικό. (Το ουσιαστικά με την έννοια ότι βρισκόμαστε σε περιοχή μοναδικής παραγοντοποίησης.)

Επιπλέον, γνωρίζουμε ότι για κάθε πολυώνυμο $g(x)$ βαθμού ≥ 1 σε έναν δακτύλιο $\mathbb{F}[x]$ υπάρχει επέκταση του σώματος $\mathbb{F}$ που περιέχει ρίζα του $g(x)$. Έστω $p(x)$ ανάγωγος παράγοντας του $g(x)$. Τότε μια τέτοια επέκταση είναι η:

$$\mathbb{F}[x]/ < p(x) >$$

Επεκτείνοντας επαγωγικά το σώμα μέχρις ότου να είναι όλοι οι ανάγωγοι παράγοντες του $g(x)$ πρωτοβάθμιοι έχουμε την ύπαρξη σώματος ριζών του $g(x)$ υπεράνω του $\mathbb{F}$. (Μάλιστα και με βαθμό επέκτασης $\leq deg\,(g(x))!$).

Έστω λοιπόν σώμα ριζών K του $f(x)$. Τότε για τις ρίζες του $f(x)$ που υπάρχουν στο K ισχύει το εξής:

Ισχυρισμός: Οι ρίζες του $f(x)$ είναι απλές.

Πράγματι, η τυπική παράγωγός του είναι $f'(x) = p^n x^{p^n-1} - 1 = -1$. Συνεπώς έχουμε μκδ$(f(x), f'(x)) = 1$ το οποίο ολοκληρώνει τον ισχυρισμό αφού το κριτήριο της παραγώγου μας λέει ότι αν μια ρίζα a είναι διπλή τότε $x - a \mid f(x)$ και $x - a \mid f'(x)$.

Με βάση αυτόν τον ισχυρισμό έχουμε ότι οι μονικοί ανάγωγοι παράγοντες του $f(x)$ είναι διακεκριμένοι. Αρκεί να δείξουμε τον παρακάτω ισχυρισμό:

Ισχυρισμός: Ένα ανάγωγο $g(x) \in \mathbb{Z}_p[x]$ βαθμού m διαιρεί το $f(x)$ αν και μόνο αν $m \mid n$.

Αν ισχύει ο ισχυρισμός θα έχουμε ότι η ανάλυση του $f(x)$ σε γινόμενο αναγώγων μονικών θα περιλαμβάνει όλα τα ανάγωγα μονικά πολυώνυμα με βαθμό διαιρέτη του n.

Για την απόδειξη του δεύτερου ισχυρισμού θα χρειαστούμε μερικές προτάσεις:

- Για ένα σώμα $\mathbb{F}$ χαρακτηριστικής $p > 0$ ισχύει $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ για κάθε $a, b \in \mathbb{F}$.

  Πράγματι, έχουμε $ab = ba$ από την μεταθετικότητα του σώματος. Θα γίνει η απόδειξη με επαγωγή. Για $n = 1$:

  $$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} = a^p + b^p$$

  Καθώς για $0 < k < p$ ισχύει ότι:

  $$\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1} \implies p \mid k\binom{p}{k} \implies p \mid \binom{p}{k}$$

  Υποθέτωντας ότι ισχύει για n, χρησιμοποιώντας την βάση της επαγωγής έχουμε:

  $$(a+b)^{p^{n+1}} = \left((a+b)^{p^n}\right)^p = \left(a^{p^n} + b^{p^n}\right)^p = \left(a^{p^n}\right)^p + \left(b^{p^n}\right)^p = a^{p^{n+1}} + b^{p^{n+1}}$$

- $|K| = p^n$.

  Έστω $E = \{c \in K : f(c) = 0\}$. Το E είναι υπόσωμα του K. Πράγματι $0, 1 \in E$. Επιπλέον αν $c, d \in E$ τότε:

  $c + d \in E$ αφού είμαστε σε χαρακτηριστική p και $(c+d)^{p^n} = c^{p^n} + d^{p^n} = c + d$

  $$cd \in E \quad \text{αφού } (cd)^{p^n} = c^{p^n} d^{p^n} = cd$$

  Επιπλέον το K ως σώμα ριζών του $f(x)$ είναι το ελάχιστο σώμα στο οποίο το $f(x)$ αναλύεται πλήρως. Συνεπώς καθώς το E είναι και αυτό σώμα παίρνουμε ότι $K = E$. Έχουμε ότι οι ρίζες του $f(x)$ είναι απλές και υπάρχουν το πολύ $deg f(x)$ ρίζες του $f(x)$ σε κάθε επέκταση σώματος, συνεπώς $|E| = |K| = p^n$.

- Αν L πεπερασμένο σώμα με τάξη p^n (η προηγούμενη πρόταση μάλιστα μας εξασφαλίζει ύπαρξη) και E υπόσωμα του L, τότε το E έχει τάξη p^m με $m \mid n$.

  Αν $|E| = q$ τότε καθώς το L είναι E-διανυσματικός χώρος και πεπερασμένα παραγόμενος (ως πεπερασμένος) υπάρχει πεπερασμένη βάση $a_1, \dots a_k$ του L. Κάθε στοιχείο του K γράφεται κατά μοναδικό τρόπο ως $:b_1 a_1 + \dots b_k a_k$ με $b_i \in E$. Συνεπώς $|L| = |E|^k = q^k = p^n$. Από μοναδικότητα στην παραγοντοποίηση ακεραίων έχουμε ότι $q = p^m$ όπου $mk = n$.

Απόδειξη. Αν $g(x) \mid f(x)$ τότε υπάρχει κοινή ρίζα a των $g(x), f(x)$ και επειδή το K είναι σώμα ριζών του $f(x)$ έχουμε ότι $a \in K$. Επειδή $\mathbb{Z}_p \subseteq K$ παίρνουμε ότι το $\mathbb{Z}_p(a)$ είναι υπόσωμα του K. Επιπλέον $[\mathbb{Z}_p(a) : \mathbb{Z}_p] = m$ καθώς το a είναι ρίζα του αναγώγου $g(x)$ βαθμού m. (Αν το $g(x)$ δεν είναι μονικό ισχύει το ίδιο αποτέλεσμα για το $g_0^{-1} g(x)$).

Έχουμε ότι το $\mathbb{Z}_p(a)$ είναι $\mathbb{Z}_p$-διανυσματικός χώρος με διάσταση m, δηλαδή έχει τάξη p^m. Καθώς είναι και υπόσωμα του K από την παραπάνω πρόταση παίρνουμε ότι $m \mid n$.

Αντίστροφα, έστω ότι $m \mid n$. Αν $n = ms$ έχουμε ότι:

$$p^n - 1 = (p^m - 1)(p^{m(s-1)} + p^{m(s-2)} + \dots p^m + 1)$$

δηλαδή $p^m - 1 \mid p^n - 1$. Όμοια, αν $a = bc \in \mathbb{Z}$:

$$x^a - 1 = (x^b - 1)(x^{b(c-1)} + x^{b(c-2)} + \dots x^b + 1)$$

δηλαδή $x^b - 1 \mid x^a - 1$, από όπου παίρνουμε:

$$f(x) = x^{p^n} - x = x(x^{p^n - 1} - 1) \implies x(x^{p^m - 1} - 1) = x^{p^m} - x \mid f(x)$$

Έστω a ρίζα του $g(x)$ σε κάποια επέκταση του $\mathbb{Z}_p$. τότε το $\mathbb{Z}_p(a)$ είναι σώμα με τάξη p^m. Από την απόδειξη παραπάνω πρότασης έχουμε ότι το $\mathbb{Z}_p(a)$ είναι σώμα ριζών του $x^{p^m} - x$ και μάλιστα κάθε στοιχείο του είναι και ρίζα. Άρα η τυχόν ρίζα a του αναγώγου $g(x)$ είναι και ρίζα του $x^{p^m} - x$ από όπου παίρνουμε ότι:

$$g(x) \mid x^{p^m} - x \mid x^{p^n} - x$$

□

Ο 'κώδικας' του πακέτου SageMath που χρησιμοποιήθηκε στο πρώτο ερώτημα:

```
P.<x> = PolynomialRing(IntegerModRing(3)) #Z_3 [x]
#list: (generator polynomial, check polynomial)
l=[[x^6 + x^4 -x^3 -x +1, x^6 -x^5 -x^4 -x^3 + x^2 +1 , x^10 + x^9 + x^8 + x^7
     + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, x-1 , x^5 + x^4 - x^3 +x^2 - 1, x
    ^5 - x^3 + x^2 -x - 1],[x^5 -x^3 + x^2 -x -1,x^5 + x^4 - x^3 +x^2 - 1 , x
    -1 , x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, x^6 -x
    ^5 -x^4 -x^3 + x^2 +1 , x^6 + x^4 -x^3 -x +1 ]]
for k in range(0,len(l[0])): #for every pair (generator, check)
  a=l[0][k]
  b=l[1][k]

  tmp = a.quo_rem(b)  #(1)
  r=[a,b,tmp[1]]
  q=[0,0,tmp[0]]
  i=2


  while r[i] != 0:  #(2)
    i=i+1
    tmp = r[i-2].quo_rem(r[i-1])
    q.append(tmp[0])
    r.append(tmp[1])


  lc = r[i-1].coefficients()[-1]    #(3)


  A = 1
  B = -q[i-1]
  for j in reversed(range(2,i-1)):  #(4)
    tmp = B
    B = A-q[j]*B
    A = tmp
  # (A/lc) * a + (B/lc)*b = r[i-1]/lc   linear combination of a,b = 1 (gcd)

  # print(A/lc)
  # print("$\\bigg("+str(latex(A/lc))+"\\bigg)\\bigg("+str(latex(a))+"\\bigg)
    + \\bigg("+str(latex(B/lc))+"\\bigg)\\bigg("+str(latex(b))+"\\bigg) = "+
    str(latex(r[i-1]/lc))+"$")
  print (A/lc)*a    #(5)
```

Σχόλια:

(1) Η συνάρτηση quo_ rem επιστρέφει ένα διατεταγμένο ζεύγος της μορφής (πηλίκο,υπόλοιπο) καθώς κάνει την διαίρεση των a, b με βάση τον πολυωνυμικό δακτύλιο που ανήκουν.

(2) Όσο το υπόλοιπο βγαίνει διάφορο του μηδενός συνέχισε τις διαιρέσεις κρατώντας τα προηγούμενα πηλίκα και υπόλοιπα σε αντίστοιχες λίστες.

(3) Η συνάρτηση coefficients κρατάει σε μια καινούργια λίστα τους συντελεστές του πολυωνύμου που είναι σαν μεταβλητή το $r[i-1]$ υπόλοιπο και γνωρίζουμε ότι το τελευταίο μη μηδενικό υπόλοιπο είναι ο μέγιστος κοινός διαιρέτης.

Η γλώσσα προγραμματισμού Python χρησιμοποιεί το -1 ως δείκτη του τελευταίου στοιχείου μιας λίστας. Αυτό βολεύει όταν δεν ξέρουμε από πριν το μέγεθος μιας λίστας που δημιουργείται στην πορεία του προγράμματος. Έτσι με το $[-1]$ στο τέλος ορίζεται το lc να είναι ο μεγιστοβάθμιος συντελεστής (leading coefficient). Θα διαιρέσουμε με το lc στην συνέχεια ώστε να είναι το αποτέλεσμα μονικό.

(4) Εδώ γίνονται οι πράξεις του Ευκλείδειου αλγορίθμου αντίστροφα ώστε να βρεθούν τα A, B τέτοια ώστε $Aa + Bb = \mu\kappa\delta$.

(5) Η γραμμή 32 μας τυπώνει τον συντελεστή του γεννήτορα πολυωνύμου στον γραμμικό συνδυασμό και η γραμμή 33 μας τυπώνει τον ίδιο τον γραμμικό συνδυασμό του γεννήτορα πολυωνύμου με το πολυώνυμο ελέγχου (και μάλιστα έτοιμο σε LaTeX). Για χάρη

ενός παραδείγματος εκτέλεσης του προγράμματος, αδρανοποιούμε αυτές τις δύο εντολές αφήνοντάς τες ως σχόλια και εκτελούμε μόνο την γραμμή 34 που μας δίνει τους αδύναμους γεννήτορες.(Φυσικά το πρόγραμμα τρέχει για τους ενδιάμεσους κώδικες $\mathcal{C}_1$ έως $\mathcal{C}_6$.)

Παράδειγμα εκτέλεσης του προγράμματος που μας τυπώνει τους αδύναμους γεννήτορες: