ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΜΑΘΗΜΑΤΙΚΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΤΟΥΣ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΤΟΙΧΕΙΑ ΠΕΠΕΡΑΣΜΕΝΩΝ ΣΩΜΑΤΩΝ ΜΕ ΔΕΔΟΜΕΝΗ ΤΑΞΗ ΚΑΙ ΔΕΔΟΜΕΝΑ ΙΧΝΗ

ΗΛΙΑΝΑ ΜΑΡΓΑΡΙΤΗ ΤΟΥ ΕΜΜΑΝΟΥΗΛ
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

ΚΡΗΤΗ 2011

UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS

GRADUATE PROGRAM
MATHEMATICS AND APPLICATIONS

MASTER THESIS

FINITE FIELD ELEMENTS WITH SPECIFIED ORDER AND TRACES

ILIANA MARGARITI
THESIS ADVISOR: THEODOULOS GAREFALAKIS

CRETE 2011

Η μεταπτυχιακή αυτή εργασία πραγματοποήθηκε στα πλαίσια του Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών “ Μαθηματικά και Εφαρμογές τους ” στην κατεύθυνση “ Μαθηματικά Θεμέλια Πληροφορικής και Εφαρμογές ” και παρουσιάστηκε τον Οκτώβριο του 2011. Την επιτροπή κρίσης αποτέλεσαν οι:

Αντωνιάδης Ιωάννης, Καθηγητής
Γαρεφαλάκης Θεόδουλος, Επίκουρος Καθηγητής
Τζανάκης Νικόλας, Καθηγητής

Την επίβλεψη της εργασίας έχει αναλάβει ο κ. Γαρεφαλάκης Θεόδουλος τον οποίο ευχαριστώ για την πολύτιμη βοήθεια του. Επίσης θα ήθελα να ευχαριστίσω το Ίδρυμα Κρατικών Υποτροφιών για την καταβολή υποτροφίας για την εκπόνιση των μεταπτυχιακών σπουδών μου.

Στον Μιχάλη

και

Στον Μάνο

Περίληψη

Έστω $\mathbb{F}_q$ πεπερασμένο σώμα τάξης q, όπου q είναι δύναμη ενός πρώτου αριθμού p. Υποθέτουμε ότι $f_1(x), ..., f_r(x)$ (με $r \geq 1$) είναι δεδομένα πολυώνυμα του $\mathbb{F}_{q^n}[x]$ όπου n θετικός ακέραιος και $t_1, ..., t_r$ είναι δεδομένα στοιχεία του $\mathbb{F}_q$. Στην εργασία αυτή θα αποδείξουμε ότι για δεδομένο θετικό ακέραιο l και για ικανοποιητικά μεγάλους ακεραίους n με $l|q^n-1$, υπάρχει ένα στοιχείο γ της επέκτασης $\mathbb{F}_{q^n}$ τάξης $(q^n-1)/l$ τέτοιο ώστε το $\mathbb{F}_q-$ίχνος του $f_i(\gamma)$ να είναι το συγκεκριμμένο στοιχείο t_i για κάθε $i = 1, ..., r$. Για να μπορέσουμε όμως να το αποδείξουμε κάνουμε την εξής υπόθεση: Έστω $h(x) = \sum_{i=1}^{r} c_i f_i(x)$ όπου $c_i \in \mathbb{F}_q$, $i = 1, ..., r$ και $\deg h(x) = s$. **Υποθέτουμε ότι είτε:** (i) $(s, q) = 1$ **για όλα τα διαφορετικά πολυώνυμα** $h(x)$ **που παράγονται καθώς τα** c_i**,** $i = 1, ..., r$ **διατρέχουν τα στοιχεία του** $\mathbb{F}_q$**, είτε γενικότερα:** (ii) **το πολυώνυμο** $z^q - z - h(x)$ **είναι ανάγωγο σε μία αλγεβρική θήκη του** $\mathbb{F}_{q^n}$ **για όλα τα διαφορετικά πολυώνυμα** $h(x)$**.**

Ο Cohen αποδεικνύει το Θεώρημα αυτό για ρητές συναρτήσεις $f_1, ..., f_r$ υποθέτοντας ότι είναι ισχυρά γραμμικά ανεξάρτητες (strongly linear independent) πάνω από το $\mathbb{F}_q$. Η εργασία στηρίζεται στο άρθρο [1] του Cohen. Το Θεώρημα μας βρίσκει εφαρμογή σε BCH κώδικες.

Abstract

Let $\mathbb{F}_q$ be the finite field of order q, a power of a prime p. Suppose that $f_1(x), ..., f_r(x)$ (with $r \geq 1$) are prescribed polynomials in $\mathbb{F}_{q^n}[x]$, n is a positive integer and $t_1, ..., t_r$ are prescribed members of $\mathbb{F}_q$. In this thesis, we will prove that, given a positive integer l, then, for sufficiently large integers n such that $l|q^n - 1$, there exists an element γ of the extension $\mathbb{F}_{q^n}$ of order $(q^n - 1)/l$ such that the $\mathbb{F}_q-$trace of $f_i(\gamma)$ is the specified element t_i for each $i = 1, ..., r$. To show this we suppose that: Let $h(x) = \sum_{i=1}^{r} c_i f_i(x)$, $c_i \in \mathbb{F}_q$, $i = 1, ..., r$ and $\deg h(x) = s$. **Suppose that either** (i) $(s, q) = 1$ **for all different polynomials** $h(x)$ **which generate when** c_i**,** $i = 1, ..., r$ **are the members of** $\mathbb{F}_q$**, or more generally:** (ii) **the polynomial** $z^q - z - h(x)$ **is irreducible in an algebraic closure of** $\mathbb{F}_{q^n}$ **for all different polynomials** $h(x)$**.**

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Έστω $\mathbb{F}_q$ πεπερασμένο σώμα τάξης q, όπου q είναι δύναμη ενός πρώτου αριθμού p. Υποθέτουμε ότι $f_1(x), ..., f_r(x)$ (με $r \geq 1$) είναι δεδομένα πολυώνυμα του $\mathbb{F}_{q^n}[x]$ όπου n θετικός ακέραιος και $t_1, ..., t_r$ είναι δεδομένα στοιχεία του $\mathbb{F}_q$. Σκοπός μας είναι να αποδείξουμε ότι για δεδομένο θετικό ακέραιο l και για ικανοποιητικά μεγάλους ακεραίους n με $l|q^n - 1$, υπάρχει ένα στοιχείο γ της επέκτασης $\mathbb{F}_{q^n}$ τάξης $(q^n - 1)/l$ τέτοιο ώστε το $\mathbb{F}_q-$ίχνος του $f_i(\gamma)$ να είναι το συγκεκριμμένο στοιχείο t_i για κάθε $i = 1, ..., r$. Για να μπορέσουμε όμως να το αποδείξουμε κάνουμε την εξής υπόθεση: Έστω $h(x) = \sum_{i=1}^{r} c_i f_i(x)$ όπου $c_i \in \mathbb{F}_q$, $i = 1, ..., r$ και $\deg h(x) = s$. **Υποθέτουμε ότι είτε:** (i) $(s, q) = 1$ **για όλα τα διαφορετικά πολυώνυμα** $h(x)$ **που παράγονται καθώς τα** c_i, $i = 1, ..., r$ **διατρέχουν τα στοιχεία του** $\mathbb{F}_q$, **είτε γενικότερα:** (ii) **το πολυώνυμο** $z^q - z - h(x)$ **είναι ανάγωγο σε μία αλγεβρική θήκη του** $\mathbb{F}_{q^n}$ **για όλα τα διαφορετικά πολυώνυμα** $h(x)$**.** Στη συνέχεια θα συμβολίζουμε με Tr_n την απεικόνιση ίχνος από το $\mathbb{F}_{q^n}$ στο $\mathbb{F}_q$. Το θεώρημα λοιπόν που θα αποδείξουμε είναι το εξής:

Θεώρημα 1. *Έστω* $f_1(x), ..., f_r(x) \in \mathbb{F}_{q^n}[x]$ *και* $h(x) = \sum_{i=1}^{r} c_i f_i(x)$ *όπου* $c_i \in \mathbb{F}_q$, $i = 1, ..., r$ *και* $\deg h(x) = s$. *Υποθέτουμε ότι είτε:*

(i) $(s, q) = 1$ *για όλα τα διαφορετικά πολυώνυμα* $h(x)$ *που παράγονται καθώς τα* c_i, $i = 1, ..., r$ *διατρέχουν τα στοιχεία του* $\mathbb{F}_q$, *είτε γενικότερα:*

(*ii*) *το πολυώνυμο* $z^q - z - h(x)$ *είναι ανάγωγο σε μία αλγεβρική θήκη του* $\mathbb{F}_{q^n}$ *για όλα τα διαφορετικά πολυώνυμα* $h(x)$.

Θέτουμε

$$S = \max_{i=1,...,r} \deg f_i(x)$$

Έστω επίσης $t_1, ..., t_r \in \mathbb{F}_q$ *και* l *ένας οποιοσδήποτε διαιρέτης του* $q^n - 1$. *Αν*

$$n > 4\left[r + log_q 4.9 l^{3/4} S\right],$$

τότε υπάρχει ένα στοιχείο $\gamma \in \mathbb{F}_{q^n}$ *τάξης* $(q^n - 1)/l$ *τέτοιο ώστε:*

$$Tr_n\left(f_i(\gamma)\right) = t_i, \quad i = 1, ..., r. \tag{1.0.1}$$

Ο Ozbudak αποδεικνύει το Θεώρημα 1 στο [5] για ρητές συναρτήσεις $f_1, ..., f_r$ υποθέτοντας ότι είναι ισχυρά γραμμικά ανεξάρτητες (strongly linear independent) πάνω από το $\mathbb{F}_q$. Το ίδιο αποδεικνύει και ο Cohen στο άρθρο [1] χρησιμοποιώντας όμως στην απόδειξη του χαρακτήρες. Η εργασία στηρίζεται στο άρθρο [1] του Cohen. Το Θεώρημα 1 βρίσκει εφαρμογή σε BCH κώδικες.

Στο επόμενο κεφάλαιο θα ορίσουμε τους χαρακτήρες και θα διατυπώσουμε τις κυριότερες ιδιότητες τους και κάποια θεωρήματα που θα χρειαστούμε στη συνέχεια. Επίσης θα δούμε συγκεκριμένα τους προσθετικούς και τους πολλαπλασιαστικούς χαρακτήρες του $\mathbb{F}_q$. Στη συνέχεια, στην Παράγραφο 3.1 αποδεικνύουμε τρεις σημαντικές Προτάσεις: Στην Πρόταση 1 γράφουμε τη χαρακτηριστική συνάρτηση στοιχείων του $\mathbb{F}_q$ τάξης r με τη βοήθεια χαρακτήρων, στο Λήμμα 1 υπολογίζουμε ένα άθροισμα το οποίο το χρησιμοποιούμε για να υπολογίσουμε το άθροισμα της Πρότασης 2. Στην Παράγραφο 3.2 ορίζουμε ως $N_{l,r}$ το πλήθος των στοιχείων $\gamma \in \mathbb{F}_{q^n}$ τάξης $(q^n - 1)/l$ τα οποία ικανοποιούν τη σχέση 1.0.1 και υπολογίζουμε ένα κάτω φράγμα γι' αυτό. Τέλος, στην Παράγραφο 3.3 δίνουμε δύο παραδείγματα στα οποία εφαρμόζεται το Θεώρημα 1.

Κεφάλαιο 2

Χαρακτήρες

2.1 Ορισμοί και Ιδιότητες

Ορισμός 1. *Έστω $(G_n, \cdot)$ μια πεπερασμένη αβελιανή ομάδα, τάξης n και με μοναδιαίο στοιχείο $\mathbf{1}_{G_n}$. Ένας* ***χαρακτήρας χ της*** *G_n είναι ένας ομομορφισμός από την G_n στην πολλαπλασιαστική ομάδα U των μιγαδικών αριθμών. Δηλαδή,*

$$\chi : G_n \to U \quad \mu\epsilon \quad \chi(g_1 \cdot g_2) = \chi(g_1)\chi(g_2) \ \gamma\iota\alpha \quad \kappa\alpha\theta\varepsilon \quad g_1, g_2 \in G_n$$

όπου $U = \{z \in \mathbb{C} : |z| = 1\}$.

Παρατηρήσεις

1. Ισχύει $\chi(\mathbf{1}_{G_n}) = 1$.
   Πράγματι, $\chi(\mathbf{1}_{G_n}) = \chi(\mathbf{1}_{G_n} \cdot \mathbf{1}_{G_n}) = \chi(\mathbf{1}_{G_n}) \cdot \chi(\mathbf{1}_{G_n})$ και $\chi(\mathbf{1}_{G_n}) \neq 0$

2. Έχουμε :

   $$(\chi(g))^n = \chi(g^n) = \chi(\mathbf{1}_{G_n}) = 1 \quad \gamma\iota\alpha \quad \kappa\alpha\theta\varepsilon \quad g \in G_n$$

   Άρα οι τιμές ενός χαρακτήρα χ της G_n είναι οι $n-$ρίζες της μονάδας.

3. Επίσης ισχύει:

   $$\chi(g) \cdot \chi(g^{-1}) = \chi(g \cdot g^{-1}) = \chi(\mathbf{1}_{G_n}) = 1$$

Επομένως,

$$\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)} \ \ \gamma\iota\alpha \ \ \kappa\alpha\theta\varepsilon \ \ g \in G_n$$

όπου με παύλα συμβολίζουμε τον συζυγή μιγαδικό.

Ορισμός 2. *Ανάμεσα στους χαρακτήρες της G_n έχουμε τον* ***τετριμμένο χαρακτήρα*** χ_0 *που ορίζεται ως:*

$$\chi_0(g) = 1 \ \ \gamma\iota\alpha \ \ \kappa\alpha\theta\varepsilon \ \ g \in G_n$$

Όλοι οι άλλοι χαρακτήρες της G_n ονομάζονται ***μη τετριμμένοι****.*

Ορισμός 3. *Για κάθε χαρακτήρα χ της G_n ορίζεται ο* ***συζυγής χαρακτήρας*** $\overline{\chi}$ *ως εξής:*

$$\overline{\chi}(g) = \overline{\chi(g)} \ \ \gamma\iota\alpha \ \ \kappa\alpha\theta\varepsilon \ \ g \in G_n$$

Ορισμός 4. *Δεδομένου πεπερασμένο το πλήθος χαρακτήρων $\chi_1, \ldots, \chi_m$ της G_n, ορίζουμε τον* ***χαρακτήρα γινόμενο*** $\chi_1 \cdots \chi_m$ *ως εξής:*

$$\chi_1 \cdots \chi_m(g) = \chi_1(g) \cdot \ldots \cdot \chi_m(g) \ \ \gamma\iota\alpha \ \ \kappa\alpha\theta\varepsilon \ \ g \in G_n$$

Αν $\chi_1 = \ldots = \chi_m = \chi$, τότε συμβολίζουμε με χ^m τον χαρακτήρα $\chi_1 \cdots \chi_m$.

Έστω $\widehat{G}_n$ το σύνολο με στοιχεία τους χαρακτήρες της G_n. Είναι προφανές ότι το $\widehat{G}_n$ είναι μία αβελιανή ομάδα με πράξη τον πολλαπλασιασμό χαρακτήρων, ουδέτερο στοιχείο τον τετριμένο χαρακτήρα χ_0 και αντίστροφο στοιχείο ενός στοιχείου $\chi \in \widehat{G}_n$ τον συζυγή του $\overline{\chi}$. Επίσης, η $\widehat{G}_n$ είναι πεπερασμένη ομάδα, αφού οι τιμές που μπορούν να πάρουν οι χαρακτήρες της G_n είναι μόνο οι $n-$ρίζες της μονάδας.

Θα δούμε τώρα ως ένα παράδειγμα την ειδική περίπτωση όπου η πεπερασμένη ομάδα είναι κυκλική, το οποίο θα μας φανεί χρήσιμο στην συνέχεια.

Παράδειγμα 1. *Έστω G_n μία πεπερασμένη κυκλική ομάδα τάξης n, g ένας γεννήτορας της και $\zeta_{n,k} = e^{\frac{2\pi ik}{n}}, \ \ k = 0, \ldots, n-1$ οι $n-$ρίζες της μονάδας. Για έναν σταθερό ακέραιο j, $0 \leq j \leq n-1$, η απεικόνιση*

$$\chi_j(g^k) = e^{\frac{2\pi ijk}{n}} = \zeta_{n,k}^j, \ \ k = 0, \ldots, n-1$$

ορίζει έναν χαρακτήρα της G_n.

Από την άλλη, αν χ *είναι ένας χαρακτήρας της* G_n, *τότε το* $\chi(g)$ *θα πρέπει να είναι μία* $n-$*ρίζα της μονάδας, έστω* $\chi(g) = e^{\frac{2\pi ij}{n}}$ *για κάποιο* $j, 0 \leq j \leq n-1$. *Έπεται τότε ότι* $\chi \equiv \chi_j$.

Έτσι η $\widehat{G}_n$ *αποτελείται ακριβώς από τους χαρακτήρες* $\chi_0, \ldots, \chi_{n-1}$. *Επίσης ισχύει:*

$$\chi_1(g^k) = e^{\frac{2\pi ik}{n}} = \zeta_{n,k}, \quad k = 0, ..., n-1$$

Παρατηρούμε ότι για έναν σταθερό ακέραιο j, $\quad 0 \leq j \leq n-1$ *ισχύει:*

$$\chi_j(g^k) = (\chi_1(g^k))^j, \quad k = 0, ..., n-1$$

Δηλαδή, $\chi_j \equiv \chi_1^j, \quad j = 0, ..., n-1$. *Άρα* $\widehat{G}_n =< \chi_1 >$, *και επομένως η* $\widehat{G}_n$ *είναι επίσης κυκλική ομάδα τάξης* n.

Θεώρημα 2. *Έστω* H *μία υποομάδα της πεπερασμένης αβελιανής ομάδας* G_n *και έστω* ψ *ένας χαρακτήρας της* H. *Τότε ο* ψ *μπορεί να επεκταθεί σε έναν χαρακτήρα της* G_n. *Δηλαδή υπάρχει ένας χαρακτήρας* χ *της* G_n *τέτοιος ώστε* $\chi(h) = \psi(h) \;\; \gamma\iota\alpha \;\; \kappa\alpha\theta\varepsilon \;\; h \in H$.

Απόδειξη Έστω H μία γνήσια υποομάδα της G_n. Επιλέγουμε $\alpha \in G_n$ με $\alpha \notin H$ και έστω m ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $\alpha^m \in H$. Υπάρχει τέτοιος ακέραιος m διότι $\alpha^{|G|} = 1 \in H$. Επομένως από την Αρχή της Πληρότητας υπάρχει ελάχιστος φυσικός m με $\alpha^m \in H$. Συμβολίζουμε με H_1 την υποομάδα της G_n που παράγεται από την H και το α : $H_1 =< H \cup \{\alpha\} >$. Τότε κάθε στοιχείο $g \in H_1$ μπορεί να γραφεί με μοναδικό τρόπο στη μορφή $g = \alpha^j h$ με $0 \leq j < m$ και $h \in H$. Πράγματι, έστω $g \in H_1 =< H \cup \{\alpha\} >$. Τότε $g = \alpha^k h'$ με $h' \in H$ και $k \in \mathbb{N}$. Από τον αλγόριθμο της Ευκλείδειας Διαίρεσης έχουμε ότι υπάρχουν μοναδικοί ακέραιοι l, j τέτοιοι ώστε $k = m \cdot l + j$ όπου $0 \leq j < m$. Επομένως, $g = \alpha^j (\alpha^m)^l h' = \alpha^j h$, όπου $h = (\alpha^m)^l h' \in H$ και $0 \leq j < m$. Για την μοναδικότητα τώρα έχουμε : Έστω $g = \alpha^{j_1} h_1 = \alpha^{j_2} h_2$. Τότε $\alpha^{j_1 - j_2} = h_2 h_1^{-1} \in H$. Άτοπο διότι $j_1 - j_2 < m$ και m ο ελάχιστος θετικός ακέραιος.

Ορίζουμε μία απεικόνιση ψ_1 στην H_1 ως εξής:

$$\psi_1(g) = \omega^j \psi(h)$$

όπου ω είναι ένας σταθερός μιγαδικός αριθμός τέτοιος ώστε $\omega^m = \psi(\alpha^m)$. Η ψ_1 είναι ένας χαρακτήρας της H_1. Πράγματι, έστω $g_1 = \alpha^{j_1} h_1$ με $0 \leq j_1 < m$ και $h_1 \in H$ ένα άλλο στοιχείο της H_1.

- Αν $j + j_1 < m$, τότε $\psi_1(gg_1) = \omega^{j+j_1}\psi(hh_1) = \omega^j\psi(h)\omega^{j_1}\psi(h_1) = \psi_1(g)\psi_1(g_1)$

- Αν $j + j_1 \geq m$, τότε $gg_1 = \alpha^{j+j_1-m}(\alpha^m hh_1)$ με $0 \leq j + j_1 - m < m$ και έτσι:

$$\begin{aligned} \psi_1(gg_1) &= \omega^{j+j_1-m}\psi(\alpha^m hh_1) = \omega^{j+j_1-m}\psi(\alpha^m)\psi(h)\psi(h_1) \\ &= \omega^j\psi(h)\omega^{j_1}\psi(h_1) = \psi_1(g)\psi_1(g_1) \end{aligned}$$

Επίσης είναι προφανές ότι $\psi_1(h) = \psi(h) \ \ \gamma\iota\alpha \ \ \kappa\alpha\theta\varepsilon \ \ h \in H$

Αν $H_1 \equiv G_n$, τότε έχουμε τελειώσει. Διαφορετικά μπορούμε να συνεχίσουμε όμοια την παραπάνω διαδικασία μέχρι να αποκτήσουμε μία επέκταση ψ της G_n, μετά από πεπερασμένο πλήθος βημάτων.

□

Πόρισμα 1. *Για κάθε δύο διαφορετικά στοιχεία $g_1, g_2 \in G_n$, υπάρχει ένας χαρακτήρας χ της G_n τέτοιος ώστε $\chi(g_1) \neq \chi(g_2)$.*

Απόδειξη Αρκεί να δείξουμε ότι για $h = g_1 g_2^{-1} \neq \mathbf{1}_{G_n}$ υπάρχει ένας χαρακτήρας χ της G_n με $\chi(h) \neq 1$. Πράγματι τότε $\chi(g_1 g_2^{-1}) \neq 1 \Leftrightarrow \chi(g_1)\chi(g_2)^{-1} \neq 1 \Leftrightarrow \chi(g_1) \neq \chi(g_2)$. Αυτό προκύπτει άμεσα από το Παράδειγμα 1 και το Θεώρημα 2 θέτοντας ως Η την κυκλική υποομάδα της G_n που παράγεται από το h.

□

Θεώρημα 3. *Έστω G_n μία πεπερασμένη αβελιανή ομάδα.*

(i) Αν χ είναι ένας μη τετριμένος χαρακτήρας της G_n, τότε

$$\sum_{g \in G_n} \chi(g) = 0 \tag{2.1.1}$$

(*ii*) *Αν* $g \in G_n$ *με* $g \neq \mathbf{1}_{G_n}$, *τότε*

$$\sum_{\chi \in \widehat{G}_n} \chi(g) = 0 \tag{2.1.2}$$

Απόδειξη

(*i*) Αφού χ είναι ένας μη τετριμμένος χαρακτήρας, υπάρχει στοιχείο $h \in G_n$ τέτοιο ώστε $\chi(h) \neq 1$. Επομένως:

$$\chi(h) \cdot \sum_{g \in G_n} \chi(g) = \sum_{g \in G_n} \chi(hg) = \sum_{g \in G_n} \chi(g)$$

όπου η τελευταία ισότητα ισχύει διότι όταν το g διατρέχει τα στοιχεία του G_n, το ίδιο συμβαίνει και για το hg. Έτσι έχουμε:

$$[\chi(h) - 1] \cdot \sum_{g \in G_n} \chi(g) = 0 \Rightarrow \sum_{g \in G_n} \chi(g) = 0$$

(*ii*) Ορίζουμε στο $\widehat{G}_n$ την απεικόνιση $\widehat{g}$ ως εξής:

$$\widehat{g}(\chi) = \chi(g)$$

για $\chi \in \widehat{G}_n$. Η $\widehat{g}$ είναι ένας χαρακτήρας της πεπερασμένης αβελιανής ομάδας $\widehat{G}_n$. Ο χαρακτήρας αυτός είναι μη τετριμμένος αφού από το Πόρισμα 1 υπάρχει χαρακτήρας $\chi \in \widehat{G}_n$ με $\chi(g) \neq \chi(1_{G_n}) = 1$. Έτσι αν εφαρμόσουμε την σχέση 2.1.1 στην ομάδα $\widehat{G}_n$ θα πάρουμε:

$$\sum_{\chi \in \widehat{G}_n} \chi(g) = \sum_{\chi \in \widehat{G}_n} \widehat{g}(\chi) = 0$$

□

Θεώρημα 4. *Το πλήθος των χαρακτήρων μιας πεπερασμένης αβελιανής ομάδας* G_n *είναι ίσο με την τάξη της* n.

Απόδειξη

Έστω $G_n = \{g_0 = 1_{G_n}, g_1, ..., g_{n-1}\}$ με $|G_n| = n$ και $\widehat{G}_n = \{\chi_0, \chi_1, ..., \chi_{m-1}\}$

με $|\widehat{G}_n| = m$. Έχουμε:

$$\begin{aligned}\sum_{g\in G_n}\sum_{\chi\in\widehat{G}_n}\chi(g) &= \sum_{g\in G_n}[\chi_0(g)+\chi_1(g)+...+\chi_{m-1}(g)]\\ &= [\chi_0(1_{G_n})+\chi_1(1_{G_n})+...+\chi_{m-1}(1_{G_n})]+...+[\chi_0(g_{n-1})+...+\chi_{m-1}(g_{n-1})]\\ &= \underbrace{1+1+...+1}_{m}+0+...+0 = m = |\widehat{G}_n|\end{aligned}$$

Επίσης:

$$\begin{aligned}\sum_{\chi\in\widehat{G}_n}\sum_{g\in G_n}\chi(g) &= \sum_{g\in\widehat{G}_n}[\chi(1_{G_n})+\chi(g_1)+...+\chi(g_{n-1})]\\ &= [\chi_0(1_{G_n})+\chi_0(g_1)+...+\chi_0(g_{n-1})]+...+[\chi_{m-1}(1_{G_n})+...+\chi_{m-1}(g_{n-1})]\\ &= \underbrace{1+1+...+1}_{n}+0+...+0 = n = |G_n|\end{aligned}$$

Έτσι έχουμε:

$$|\widehat{G}_n| = \sum_{g\in G_n}\sum_{\chi\in\widehat{G}_n}\chi(g) = \sum_{\chi\in\widehat{G}_n}\sum_{g\in G_n}\chi(g) = |G_n|$$

□

Οι ισχυρισμοί των Θεωρημάτων 3 και 4 μπορούν να συνδυαστούν στις **σχέσεις ορθογωνιότητας των χαρακτήρων**. Έστω χ και ψ χαρακτήρες της ομάδας G_n. Τότε:

$$\frac{1}{|G_n|}\cdot\sum_{g\in G_n}\chi(g)\overline{\psi(g)} = \begin{cases}1 & \text{αν } \chi{=}\psi\\ 0 & \text{αν } \chi{\neq}\,\psi\end{cases} \tag{2.1.3}$$

Επίσης, αν g και h είναι στοιχεία της ομάδας G_n, τότε:

$$\frac{1}{|G_n|}\cdot\sum_{\chi\in\widehat{G}_n}\chi(g)\overline{\chi(h)} = \begin{cases}1 & \text{αν } g=h\\ 0 & \text{αν } g\neq h\end{cases} \tag{2.1.4}$$

Πράγματι για την σχέση 2.1.3 έχουμε:

$$\frac{1}{|G_n|}\cdot\sum_{g\in G_n}\chi(g)\overline{\psi(g)} = \frac{1}{|G_n|}\cdot\sum_{g\in G_n}\chi(g)\overline{\psi}(g) = \frac{1}{|G_n|}\cdot\sum_{g\in G_n}(\chi\overline{\psi})(g)$$

- Αν $\chi \neq \psi$ τότε $\chi\psi^{-1} \neq \chi_0$ δηλαδή $\chi\overline{\psi} \neq \chi_0$, άρα από την σχέση 2.1.1 έπεται ότι $\sum_{g\in G_n}(\chi\overline{\psi})(g) = 0$.

- Αν $\chi = \psi$ δηλαδή $\chi\overline{\psi} = \chi_0$, έπεται ότι $\sum_{g\in G_n}(\chi\overline{\psi})(g) = \sum_{g\in G_n}\chi_0(g) = \sum_{g\in G_n} 1 = |G_n|$

Ενώ η σχέση 2.1.4 προκύπτει ως εξής:

$$\frac{1}{|G_n|}\cdot\sum_{\chi\in\widehat{G}_n}\chi(g)\overline{\chi(h)} = \frac{1}{|G_n|}\cdot\sum_{\chi\in\widehat{G}_n}\chi(g)\chi(h^{-1}) = \frac{1}{|G_n|}\cdot\sum_{\chi\in\widehat{G}_n}\chi(gh^{-1})$$

- Αν $gh^{-1} \neq 1_{G_n}$ δηλαδή $g \neq h$, τότε από την σχέση 2.1.2 έπεται ότι $\sum_{\chi\in\widehat{G}_n}\chi(gh^{-1}) = 0$

- Αν $gh^{-1} = 1_{G_n}$ δηλαδή $g = h$, έπεται ότι $\sum_{\chi\in\widehat{G}_n}\chi(gh^{-1}) = \sum_{\chi\in\widehat{G}_n}\chi(1_{G_n}) = \sum_{\chi\in\widehat{G}_n} 1 = |\widehat{G}_n| = |G_n|$

2.2 Οι χαρακτήρες του $\mathbb{F}_q$

Έστω $\mathbb{F}_q$ πεπερασμένο σώμα με $char\mathbb{F}_q = p$, όπου p πρώτος και q μία δύναμη του p. Στο $\mathbb{F}_q$ έχουμε δύο πεπερασμένες αβελιανές ομάδες, την προσθετική και την πολλαπλασιαστική. Γι' αυτό θα πρέπει να κάνουμε μία διάκριση μεταξύ των χαρακτήρων που αναφέρονται σε αυτές τις δύο ομάδες. Και στις δύο περιπτώσεις θα δώσουμε σαφείς μορφές για τους χαρακτήρες.

Προσθετικοί χαρακτήρες του $\mathbb{F}_q$

Ας θεωρήσουμε αρχικά την προσθετική ομάδα του $\mathbb{F}_q$. Το πρώτο σώμα που περιέχεται στο $\mathbb{F}_q$ είναι το $\mathbb{F}_p$. Έστω $Tr : \mathbb{F}_q \to \mathbb{F}_p$ η απεικόνιση ίχνος (trace) από το $\mathbb{F}_q$ στο $\mathbb{F}_p$. Τότε η απεικόνιση ψ_1 που ορίζεται ως εξής:

$$\psi_1(c) = e^{2\pi i Tr(c)/p}, \quad c \in \mathbb{F}_q$$

είναι ένας χαρακτήρας της προσθετικής ομάδας του $\mathbb{F}_q$. Πράγματι, για $c_1, c_2 \in \mathbb{F}_q$ έχουμε $Tr(c_1 + c_2) = Tr(c_1) + Tr(c_2)$. Άρα,

$$\psi_1(c_1 + c_2) = e^{2\pi i Tr(c_1+c_2)/p} = e^{2\pi i Tr(c_1)/p}\cdot e^{2\pi i Tr(c_2)/p} = \psi_1(c_1)\cdot\psi_1(c_2)$$

Από εδώ και στο εξής αντί της έκφρασης "**χαρακτήρας της προσθετικής αμάδας του** $\mathbb{F}_q$", θα χρησιμοποιούμε την έκφραση "**προσθετικός χαρακτήρας του** $\mathbb{F}_q$". Ο χαρακτήρας ψ_1 ονομάζεται "**κανονικός προσθετικός χαρακτήρας του** $\mathbb{F}_q$".

Όλοι οι προσθετικοί χαρακτήρες του $\mathbb{F}_q$ μπορούν να εκφραστούν συναρτήσει του ψ_1:

Θεώρημα 5. *Έστω $b \in \mathbb{F}_q$. Η απεικόνιση ψ_b με*

$$\psi_b(c) = \psi_1(bc) \quad \gamma\iota\alpha \quad \kappa\alpha\theta\varepsilon \quad c \in \mathbb{F}_q$$

είναι ένας προσθετικός χαρακτήρας του $\mathbb{F}_q$ και κάθε προσθετικός χαρακτήρας του $\mathbb{F}_q$ παράγεται με αυτόν τον τρόπο.

Απόδειξη

Έστω $c_1, c_2 \in \mathbb{F}_q$. Τότε:

$$\psi_b(c_1+c_2) = \psi_1(b(c_1+c_2)) = \psi_1(bc_1+bc_2) = \psi_1(bc_1)\cdot\psi_1(bc_2) = \psi_b(c_1)\cdot\psi_b(c_2)$$

Άρα ψ_b προσθετικός χαρακτήρας του $\mathbb{F}_q$.

Αφού η Tr είναι ένας μη τετριμμένος γραμμικός μετασχηματισμός από το $\mathbb{F}_q$ (ως $\mathbb{F}_p$-Διανυσματικού Χώρου) στο $\mathbb{F}_p$ (ως $\mathbb{F}_p$-Διανυσματικού Χώρου)(διότι η επέκταση $\mathbb{F}_q|\mathbb{F}_p$ είναι διαχωρίσιμη), η ψ_1 είναι ένας μη τετριμμένος χαρακτήρας. Έτσι αν $a, b \in \mathbb{F}_q$ με $a \neq b$, τότε:

$$\begin{aligned} \frac{\psi_a(c)}{\psi_b(c)} &= \frac{\psi_1(ac)}{\psi_1(bc)} = \psi_1(ac)\cdot(\psi_1(bc))^{-1} = \psi_1(ac)\cdot\psi_1((bc)^{-1}) \\ &= \psi_1(ac)\cdot\psi_1(-bc) = \psi_1((a-b)c) \neq 1 \end{aligned}$$

για κατάλληλο $c \in \mathbb{F}_q$. Άρα οι απεικονίσεις ψ_a και ψ_b με $a, b \in \mathbb{F}_q$ και $a \neq b$, είναι διακεκριμένοι χαρακτήρες του $\mathbb{F}_q$. Έτσι, αν το b διατρέχει τα στοιχεία της προσθετικής ομάδας του $\mathbb{F}_q$, παίρνουμε q διακεκριμένους προσθετικούς χαρακτήρες ψ_b. Από την άλλη μεριά, το $\mathbb{F}_q$ έχει ακριβώς q χαρακτήρες, όσους και η τάξη του. Έτσι η λίστα των προσθετικών χαρακτήρων έχει ολοκληρωθεί.

□

Θέτοντας $b = 0$ στο Θεώρημα 5, παίρνουμε τον τετριμένο προσθετικό χαρακτήρα ψ_0 για τον οποίο ισχύει $\psi_0(c) = 1$ για κάθε $c \in \mathbb{F}_q$.

Σημείωση

Έστω $\mathbb{E}$ μία πεπερασμένη επέκταση του $\mathbb{F}_q$,και έστω ψ_1 και μ_1 οι κανονικοί προσθετικοί χαρακτήρες του $\mathbb{F}_q$, και του $\mathbb{E}$ αντίστοιχα, δηλαδή

$$\psi_1(c) = e^{2\pi i Tr_{\mathbb{F}_q}(c)/p} \quad \kappa\alpha\iota \quad \mu_1(b) = e^{2\pi i Tr_{\mathbb{E}}(b)/p}$$

όπου $c \in \mathbb{F}_q$, $b \in \mathbb{E}$, και $Tr_{\mathbb{F}_q} : \mathbb{F}_q \to \mathbb{F}_p$, $Tr_{\mathbb{E}} : \mathbb{E} \to \mathbb{F}_p$ οι απεικονίσεις ίχνη. Γνωρίζουμε ότι ισχύει:

$$Tr_{\mathbb{E}}(b) = Tr_{\mathbb{F}_q}(Tr_{\mathbb{E}/\mathbb{F}_q}(b)) \quad \gamma\iota\alpha \quad o\lambda\alpha \quad \tau\alpha \quad b \in \mathbb{E}$$

όπου $Tr_{\mathbb{E}/\mathbb{F}_q}$ η απεικόνιση ίχνος από το $\mathbb{E}$ στο $\mathbb{F}_q$. Άρα τα ψ_1 και μ_1 συνδέονται με την σχέση:

$$\mu_1(b) = e^{2\pi i Tr_{\mathbb{F}_q}(Tr_{\mathbb{E}/\mathbb{F}_q}(b))/p} = \psi_1(Tr_{\mathbb{E}/\mathbb{F}_q}(b)) \quad \gamma\iota\alpha \quad \kappa\alpha\theta\varepsilon \quad b \in \mathbb{E}$$

Δηλαδή,

$$\mu_1 = \psi_1 \circ Tr_{\mathbb{E}/\mathbb{F}_q} \tag{2.2.1}$$

Πολλαπλασιαστικοί χαρακτήρες του $\mathbb{F}_q$

Οι χαρακτήρες της πολλαπλασιαστικής ομάδας $\mathbb{F}_q^*$ του σώματος $\mathbb{F}_q$ ονομάζονται **πολλαπλασιαστικοί χαρακτήρες του** $\mathbb{F}_q$. Αφού η $\mathbb{F}_q^*$ είναι κυκλική τάξης $q-1$, οι χαρακτήρες της μπορούν εύκολα να οριστούν.

Θεώρημα 6. *Έστω g ένα σταθερό πρωταρχικό στοιχείο του $\mathbb{F}_q$. Για κάθε $j = 0, 1, ..., q-2$, η απεικόνιση χ_j με:*

$$\chi_j(g^k) = e^{2\pi i jk/(q-1)} \quad \gamma\iota\alpha \quad k = 0, 1, ..., q-2$$

ορίζει έναν πολλαπλασιαστικό χαρακτήρα του $\mathbb{F}_q$ και κάθε πολλαπλασιαστικός χαρακτήρας του $\mathbb{F}_q$ παράγεται με αυτόν τον τρόπο.

Απόδειξη

Έπεται από το Παράδειγμα 1.

□

Πόρισμα 2. *Η ομάδα των πολλαπλασιαστικών χαρακτήρων του $\mathbb{F}_q$ είναι κυκλική τάξης $q-1$ με μοναδιαίο στοιχείο το χ_0.*

Απόδειξη

Κάθε χαρακτήρας χ_j στο Θεώρημα 6, με j σχετικά πρώτο με το $q-1$, είναι ένας γεννήτορας της ομάδας.

□

Οι σχέσεις ορθογωνιότητας 2.1.3 και 2.1.4 στους προσθετικούς και στους πολλαπλασιαστικούς χαρακτήρες του $\mathbb{F}_q$, παράγουν θεμελιώδεις ταυτότητες. Θεωρούμε αρχικά την περίπτωση των προσθετικών χαρακτήρων. Για τους προσθετικούς χαρακτήρες ψ_a και ψ_b έχουμε:

$$\sum_{c\in\mathbb{F}_q}\psi_a(c)\overline{\psi_b(c)}=\begin{cases} q & \text{αν } a=b \\ 0 & \text{αν } a\neq b \end{cases}$$

Συγκεκριμένα,

$$\sum_{c\in\mathbb{F}_q}\psi_a(c)=0 \quad \gamma\iota\alpha \quad a\neq 0 \tag{2.2.2}$$

Επίσης, αν $c,d\in\mathbb{F}_q$, έχουμε:

$$\sum_{b\in\mathbb{F}_q}\psi_b(c)\overline{\psi_b(d)}=\begin{cases} q & \text{αν } c=d \\ 0 & \text{αν } c\neq d \end{cases}$$

Για πολλαπλασιαστικούς χαρακτήρες χ και τ του $\mathbb{F}_q$ έχουμε:

$$\sum_{c\in\mathbb{F}_q^*}\chi(c)\overline{\tau(c)}=\begin{cases} q-1 & \text{αν } \chi=\tau \\ 0 & \text{αν } \chi\neq\tau \end{cases}$$

Συγκεκριμένα,

$$\sum_{c\in\mathbb{F}_q^*}\chi(c)=0 \quad \gamma\iota\alpha \quad \chi\neq\chi_0 \tag{2.2.3}$$

Επίσης, αν $c,d\in\mathbb{F}_q^*$, έχουμε:

$$\sum_{\chi}\chi(c)\overline{\chi(d)}=\begin{cases} q-1 & \text{αν } c=d \\ 0 & \text{αν } c\neq d \end{cases}$$

Κεφάλαιο 3

Στοιχεία με δεδομένη τάξη και δεδομένα ίχνη

3.1 Στοιχεία με δεδομένη τάξη σε μία κυκλική ομάδα

Έστω G_n μία (πολλαπλασιαστική) κυκλική ομάδα τάξης n. Γνωρίζουμε ότι υπάρχουν $\phi(n)$ το πλήθος στοιχεία της G_n τα οποία παράγουν την ομάδα. Για κάθε διαιρέτη r του n, συμβολίζουμε με $\Lambda_{n,r}$ την χαρακτηριστική συνάρτηση στοιχείων τάξης r στο G_n. Δηλαδή, για κάθε $x \in G_n$ είναι:

$$\Lambda_{n,r}(x) = \begin{cases} 1 & \text{αν } ord(x) = r \\ 0 & \text{διαφορετικά} \end{cases}$$

Η $\Lambda_{n,r}$ μπορεί επίσης να εκφραστεί συναρτήσει των χαρακτήρων χ της πολλαπλασιαστικής ομάδας χαρακτήρων $\widehat{G}_n(\cong G_n)$. Στην επόμενη Πρόταση συμβολίζουμε με μ την συνάρτηση *Möbius* και με ϕ τη συνάρτηση Euler.

Πρόταση 1. *Έστω r διαιρέτης του n και έστω $k = \frac{n}{r}$. Ισχύει:*

$$\Lambda_{n,r}(x) = \frac{\phi(r)}{n} \sum_{d|r} \frac{\mu(d)}{\phi(d)} \sum_{\substack{e|k \\ (d,k/e)=1}} \sum_{ord\chi=de} \chi(x), \tag{3.1.1}$$

όπου με $\sum_{ord\chi=m}$ *συμβολίζουμε το άθροισμα πάνω σε όλους τους χαρακτήρες με τάξη ακριβώς* m *στο* $\widehat{G}_n$.

Απόδειξη

Θέτουμε

$$A(x)=\sum_{ord\chi=de}\chi(x),\quad B(x)=\sum_{\substack{e|k\\(d,k/e)=1}}A(x),\quad \kappa\alpha\iota\quad C(x)=\sum_{d|r}\frac{\mu(d)}{\phi(d)}B(x).$$

Παρατηρούμε ότι οι όροι του αθροίσματος $C(x)$ που είναι μη μηδενικοί, καθώς το d διατρέχει τους διαιρέτες του r, είναι εκείνοι για τους οποίους το d είναι ελεύθερου τετραγώνου (square-free).

Έστω $G_n =< g >$, όπου g ένας γεννήτορας της G_n και έστω $x \in G_n$ με $ord(x)=\frac{n}{l}$, όπου l διαιρέτης του n. Τότε $x=g^{lu}$ με $(u,n/l)=1$. Πράγματι, έστω $x=g^v$. Τότε $ord(x)=\frac{n}{(n,v)}$. Άρα:

$$l=(n,v)\ \Leftrightarrow\ \begin{cases} v=l\cdot u\\ n=l\cdot\frac{n}{l}\\ (u,\frac{n}{l})=1\end{cases}$$

Επίσης, στο Παράδειγμα 1 είδαμε ότι $\widehat{G}_n =< \chi_1 >$. Οι χαρακτήρες τάξης s είναι ακριβώς τα στοιχεία του συνόλου $\{\chi_1^{m\cdot\frac{n}{s}} : 1\le m\le s\ \ \kappa\alpha\iota\ \ (m,s)=1\}$. Πράγματι, αν $\chi_j \in \widehat{G}_n$ για κάποιο $j=1,...,n-1$, ισχύει $ord(\chi_j)=\frac{n}{(n,j)}$. Θέλουμε τους χαρακτήρες τάξης s, δηλαδή αναζητούμε τα j, $\ j=1,...,n-1$, τέτοια ώστε

$$s=\frac{n}{(n,j)}\ \Leftrightarrow\ (n,j)=\frac{n}{s}\ \Leftrightarrow\ \begin{cases} j=m\cdot\frac{n}{s}\\ n=s\cdot\frac{n}{s}\\ (m,s)=1\end{cases}$$

Είναι:

$$1\le j\le n-1\ \Leftrightarrow\ 1\le m\cdot\frac{n}{s}\le n-1\ \Leftrightarrow\ \frac{s}{n}\le m\le\frac{n-1}{n}\cdot s<s\ \Leftrightarrow\ 1\le m\le s-1$$

Στη συνέχεια θα συμβολίσουμε με ζ_t μία πρωταρχική $t-$ρίζα της μονάδας. Επίσης παρατηρώντας το $B(x)$ και το $C(x)$ συμπεραίνουμε ότι το d διατρέχει

τους διαιρέτες του r και το e διατρέχει τους διαιρέτες του k. Όμως τα k, r είναι διαιρέτες του n. Άρα $de|n$. Έτσι έχουμε:

$$\begin{aligned} A(x) &= \sum_{ord\chi=de} \chi(x) = \sum_{\substack{m=1 \\ (m,de)=1}}^{de} (\chi_1(x))^{m\cdot\frac{n}{de}} = \sum_{\substack{m=1 \\ (m,de)=1}}^{de} (\chi_1(g^{lu}))^{m\cdot\frac{n}{de}} \\ &= \sum_{\substack{m=1 \\ (m,de)=1}}^{de} (\chi_1(g))^{m\cdot\frac{nlu}{de}} = \sum_{\substack{m=1 \\ (m,de)=1}}^{de} \zeta_n^{m\cdot\frac{nlu}{de}} = \sum_{\substack{m=1 \\ (m,de)=1}}^{de} (\zeta_n^{\frac{n}{de}})^{mlu} \end{aligned}$$

Γνωρίζουμε ότι, αν ζ_t είναι μία πρωταρχική $t-$ρίζα της μονάδας και $b|t$, τότε η $\zeta_t^{\frac{t}{b}}$ είναι μία πρωταρχική $b-$ρίζα της μονάδας, δηλαδή $\zeta_t^{\frac{t}{b}} = \zeta_b$. Άρα $\zeta_n^{\frac{n}{de}} = \zeta_{de}$. Επομένως,

$$A(x) = \sum_{\substack{m=1 \\ (m,de)=1}}^{de} (\zeta_{de})^{mlu} = \sum_{m=1}^{de} \left\lfloor \frac{1}{(m,de)} \right\rfloor \zeta_{de}^{mlu} = \sum_{m=1}^{de} \sum_{j|(m,de)} \mu(j)\zeta_{de}^{mlu} = \sum_{m=1}^{de} \sum_{\substack{j|m \\ j|de}} \mu(j)\zeta_{de}^{mlu}$$

Το τελευταίο διπλό άθροισμα σημαίνει ότι για έναν συγκεκριμένο διαιρέτη j του de, η άθροιση πρέπει να γίνει για όλους τους ακεραίους m με $1 \le m \le de$ που είναι πολλαπλάσια του j. Έτσι, αν θέσουμε $m = q \cdot j$, τότε θα είναι $1 \le m \le de \quad \Leftrightarrow \quad 1 \le q \le de/j$. Επομένως το $A(x)$ μπορεί να γραφεί ως εξής:

$$A(x) = \sum_{j|de} \sum_{q=1}^{de/j} \mu(j)\zeta_{de}^{luqj} = \sum_{j|de} \mu(j) \sum_{q=1}^{de/j} \zeta_{de}^{luqj}$$

Θέτοντας $j = de/v$ παίρνουμε:

$$A(x) = \sum_{(de/v)|de} \mu(\frac{de}{v}) \sum_{q=1}^{v} \zeta_{de}^{luq\frac{de}{v}} = \sum_{j|de} \mu(\frac{de}{j}) \sum_{q=1}^{j} (\zeta_{de}^{lu\frac{de}{j}})^q$$

Ισχύει $j/lu \Leftrightarrow j/l$. Πράγματι, έστω j/lu. Το j διατρέχει τους διαιρέτες του de, άρα j/n. Έχουμε ότι $(u, n/l) = 1$, άρα υπάρχουν μοναδικοί ακέραιοι x, y τέτοιοι ώστε $ux + \frac{n}{l}y = 1 \Leftrightarrow ulx + ny = l$. Έχουμε $j/(ulx + ny)$, άρα j/l.

Είναι:

$$\sum_{q=1}^{j} (\zeta_{de}^{lu\frac{de}{j}})^q = \begin{cases} j & \text{αν } j|l \\ 0 & \text{διαφορετικά} \end{cases}$$

Πράγματι,

- Αν $j|l$, τότε το $\frac{l}{j}u \cdot de$ είναι πολλαπλάσιο του de και άρα $\zeta_{de}^{\frac{l}{j}ude} = 1$. Επομένως,

$$\sum_{q=1}^{j}(\zeta_{de}^{lu\frac{de}{j}})^q = \sum_{q=1}^{j} 1^q = j$$

- Αν $j \nmid l$, τότε το $lu \cdot \frac{de}{j}$ δεν είναι πολλαπλάσιο του de και άρα $\zeta_{de}^{lu\frac{de}{j}} \neq 1$. Τότε το άθροισμα αυτό αποτελεί γεωμετρική πρόοδο και έτσι έχουμε,

$$\sum_{q=1}^{j}(\zeta_{de}^{lu\frac{de}{j}})^q = \frac{1-(\zeta_{de}^{lu\frac{de}{j}})^j}{1-\zeta_{de}^{lu\frac{de}{j}}} = \frac{1-\zeta_{de}^{lude}}{1-\zeta_{de}^{lu\frac{de}{j}}} = \frac{1-1}{1-\zeta_{de}^{lu\frac{de}{j}}} = 0$$

Άρα

$$A(x) = \sum_{\substack{j|de \\ j|l}} \mu(\frac{de}{j})j \quad \kappa\alpha\iota \quad B(x) = \sum_{\substack{e|k \\ (d,k/e)=1}} \sum_{\substack{j|de \\ j|l}} \mu(\frac{de}{j})j$$

Τώρα γράφουμε το k ως $k = k_1k_2$, όπου ο παράγοντας k_1 αποτελείται από τους πρώτους του k (στην αντίστοιχη δύναμη που εμφανίζονται στο k), και περιέχονται συγχρόνως και στο d , ενώ $(d, k_2) = 1$. Προφανώς ισχύει και $(k_1, k_2) = 1$. Όμοια γράφουμε και τα l, e, j ως $l = l_1l_2, e = e_1e_2, j = j_1j_2$. Επίσης λαμβάνουμε υπόψην μας ότι το d είναι ελεύθερο τετραγώνου. Έχουμε λοιπόν:

$$B(x) = \sum_{\substack{e_1e_2|k_1k_2 \\ (d,k_1k_2/e_1e_2)=1}} \sum_{\substack{j_1j_2|de_1e_2 \\ j_1j_2|l_1l_2}} \mu\left(\frac{de_1e_2}{j_1j_2}\right) j_1j_2$$

Αφού η συνάρτηση *Möbius* είναι πολλαπλασιαστική και ισχύει $\left(\frac{de_1}{j_1}, \frac{e_2}{j_2}\right) = 1$ έχουμε:

$$B(x) = \sum_{\substack{e_1|k_1 \\ (d,k_1/e_1)=1}} \sum_{e_2|k_2} \sum_{\substack{j_1|de_1 \\ j_1|l_1}} \sum_{\substack{j_2|e_2 \\ j_2|l_2}} \mu\left(\frac{de_1}{j_1}\right)\mu\left(\frac{e_2}{j_2}\right) j_1j_2$$

Στο πρώτο άθροισμα έχουμε τη συνθήκη $\left(d, \frac{k_1}{e_1}\right) = 1$. Αυτό μπορεί να συμβεί μόνο αν $e_1 = k_1$. Έτσι:

$$B(x) = \sum_{e_2|k_2} \sum_{\substack{j_1|dk_1 \\ j_1|l_1}} \mu\left(\frac{dk_1}{j_1}\right) j_1 \sum_{\substack{j_2|e_2 \\ j_2|l_2}} \mu\left(\frac{e_2}{j_2}\right) j_2 = \sum_{\substack{j_1|dk_1 \\ j_1|l_1}} \mu\left(\frac{dk_1}{j_1}\right) j_1 \sum_{e_2|k_2} \sum_{\substack{j_2|e_2 \\ j_2|l_2}} \mu\left(\frac{e_2}{j_2}\right) j_2$$

Αν $k_1 \nmid j_1$, τότε $\mu\left(\frac{dk_1}{j_1}\right) = 0$. Επομένως αν $k_1 \nmid l_1$, τότε $k_1 \nmid j_1$ για κάθε τιμή του j_1 και το άθροισμα είναι ίσο με το μηδέν. Για $k_1|l_1$ οι μη μηδενικοί όροι του αθροίσματος έρχονται για $k_1|j_1$, οπότε:

$$\begin{aligned}\sum_{\substack{j_1|dk_1\\ j_1|l_1}} \mu\left(\frac{dk_1}{j_1}\right) j_1 &= \sum_{\substack{j_1|dk_1\\ j_1|l_1\\ k_1|j_1}} \mu\left(\frac{dk_1}{j_1}\right) j_1 = \sum_{\substack{j_1'k_1|dk_1\\ j_1'k_1|l_1}} \mu\left(\frac{dk_1}{j_1'k_1}\right) j_1'k_1 \\ &= k_1 \sum_{\substack{j_1'|d\\ j_1'|\frac{l_1}{k_1}}} \mu\left(\frac{d}{j_1'}\right) j_1' = k_1 \sum_{j_1'|\left(d,\frac{l_1}{k_1}\right)} \mu\left(\frac{d}{j_1'}\right) j_1'\end{aligned}$$

όπου έχουμε θέσει $j_1 = j_1'k_1$.

Επίσης, το διπλό άθροισμα $\sum_{e_2|k_2} \sum_{\substack{j_2|e_2\\ j_2|l_2}} \mu\left(\frac{e_2}{j_2}\right) j_2$ σημαίνει ότι για έναν συγκεκριμένο διαιρέτη j_2 του l_2, η άθροιση πρέπει να γίνει για όλους τους ακέραιους διαιρέτες e_2 του k_2 που είναι πολλαπλάσια του j_2. Έτσι αν θέσουμε $e_2 = e_2'j_2$ θα πάρουμε:

$$\begin{aligned}\sum_{\substack{j_2|l_2\\ j_2|k_2}} \sum_{\substack{e_2|k_2\\ e_2=e_2'j_2}} \mu(e_2')j_2 &= \sum_{\substack{j_2|l_2\\ j_2|k_2}} j_2 \sum_{e_2'|\frac{k_2}{j_2}} \mu(e_2') = \sum_{\substack{j_2|l_2\\ j_2|k_2}} j_2 \left\lfloor \frac{1}{\frac{k_2}{j_2}} \right\rfloor = \sum_{j_2|(k_2,l_2)} j_2 \left\lfloor \frac{j_2}{k_2} \right\rfloor \\ &= \begin{cases} \sum_{j_2|l_2} j_2 \cdot 1 & \text{αν } j_2 = k_2 \\ \sum_{j_2|l_2} j_2 \cdot 0 & \text{διαφορετικά} \end{cases}\end{aligned}$$

Επομένως αν το $k_2|l_2$ τότε το άθροισμα είναι ίσο με k_2, ενώ αν το $k_2 \nmid l_2$ τότε το άθροισμα θα είναι ίσο με μηδέν. Άρα το $B(x)$ γίνεται:

$$B(x) = \begin{cases} k \sum_{j_1'|\left(d,\frac{l_1}{k_1}\right)} \mu\left(\frac{d}{j_1'}\right) j_1' & \text{αν } k|l \\ 0 & \text{διαφορετικά} \end{cases}$$

Έστω λοιπόν $k|l$ και $l = k\rho$. Έχουμε επίσης $n = kr$. Ισχύει: $\left(d, \frac{l_1}{k_1}\right) = \left(d, \frac{l}{k}\right) = (d, \rho) = \rho^*$. Αν θέσουμε $d = d^*\rho^*$, τότε $(d^*, \rho^*) = 1$ αφού το d είναι ελεύθερο τετραγώνου. Έτσι έχουμε:

$$\begin{aligned}B(x) &= k \sum_{j_1'|\rho^*} \mu\left(\frac{d^*\rho^*}{j_1'}\right) j_1' = k\mu\left(d^*\right) \sum_{j_1'|\rho^*} \mu\left(\frac{\rho^*}{j_1'}\right) j_1' \\ &= k\mu\left(d^*\right)\phi\left(\rho^*\right) = k\frac{\mu\left(d\right)}{\mu\left(\rho^*\right)}\phi\left(\rho^*\right)\end{aligned}$$

Επομένως η $C(x)$ γράφεται:

$$C(x) = k \sum_{d|r} \frac{\mu^2(d)}{\phi(d)} \cdot \frac{\phi(\rho^*)}{\mu(\rho^*)}$$

Έχουμε $n = k \cdot r$, $l = k \cdot \rho$ και $l|n$. Άρα $k \cdot \rho | k \cdot r$, δηλαδή $\rho | r$. Θέτουμε $r = r' \cdot \rho$ και $d = d_1 d_2$ με $(d_1, \rho) = 1$ και $(d_1, d_2) = 1$. Γνωρίζουμε ότι το d είναι διαιρέτης του r. Άρα $d_1 d_2 | r'\rho$ και επειδή $(d_1, \rho) = 1$ και το d είναι ελεύθερο τετραγώνου έπεται ότι το $d_1 | r'$ και το $d_2 | \rho$. Έτσι, $\rho^* = (d, \rho) = (d_1 d_2, \rho) = (d_2, \rho) = d_2$. Επομένως:

$$\begin{aligned} C(x) &= k \sum_{d_1 d_2 | r'\rho} \frac{\mu^2(d_1 d_2)}{\phi(d_1 d_2)} \cdot \frac{\phi(d_2)}{\mu(d_2)} = k \sum_{\substack{d_1 | r' \\ d_2 | \rho \\ (d_1, \rho) = 1}} \frac{\mu^2(d_1)\mu^2(d_2)}{\phi(d_1)\phi(d_2)} \cdot \frac{\phi(d_2)}{\mu(d_2)} \\ &= k \sum_{\substack{d_1 | r' \\ (d_1, \rho) = 1}} \frac{\mu^2(d_1)}{\phi(d_1)} \sum_{d_2 | \rho} \mu(d_2) = k \sum_{\substack{d_1 | r' \\ (d_1, \rho) = 1}} \frac{\mu^2(d_1)}{\phi(d_1)} \left\lfloor \frac{1}{\rho} \right\rfloor \end{aligned}$$

Αν $\rho \neq 1$, τότε όλο το άθροισμα είναι μηδέν, επομένως και $C(x) = 0$. Ισχύει: $\rho \neq 1 \Leftrightarrow l \neq k \Leftrightarrow l \neq \frac{n}{r} \Leftrightarrow ord(x) \neq r$ Ενώ αν $\rho = 1$ έχουμε:

$$C(x) = k \sum_{d_1 | r'} \frac{\mu^2(d_1)}{\phi(d_1)}.$$

Όταν το $\rho = 1$, τότε $r' = r$, $d_2 = 1$, και $d = d_1$. Έτσι:

$$C(x) = k \sum_{d|r} \frac{\mu^2(d)}{\phi(d)}$$

Ισχύει:

$$\sum_{d|r} \frac{\mu^2(d)}{\phi(d)} = \frac{r}{\phi(r)} \tag{3.1.2}$$

Πράγματι, έστω $g(r) = \sum_{d|r} \frac{\mu^2(d)}{\phi(d)}$. Η $g(r)$ είναι πολλαπλασιαστική συνάρτηση αφού η συνάρτηση *Möbius* μ και η συνάρτηση *Euler* είναι πολλαπλασιαστικές. Αρκεί λοιπόν να υπολογίσουμε το $g(p^a)$ όπου p ένας οποιοσδήποτε πρώτος και $a \geq 1$ οποιοσδήποτε ακέραιος. Έχουμε λοιπόν:

$$g(p^a) = \sum_{d|p^a} \frac{\mu^2(d)}{\phi(d)} = \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} = 1 + \frac{(-1)^2}{p-1} = \frac{p}{p-1}$$

Άρα

$$g(r) = \prod_{p|r} g(p^a) = \prod_{p|r} \frac{p}{p-1}$$

Όμως:

$$\phi(r) = r \prod_{p|r} \left(1 - \frac{1}{p}\right) = r \prod_{p|r} \frac{p-1}{p} \quad \Leftrightarrow \quad \frac{r}{\phi(r)} = \prod_{p|r} \frac{p}{p-1}$$

Επομένως:

$$g(r) = \frac{r}{\phi(r)}$$

Έτσι, η $C(x)$ με τη βοήθεια της σχέσης 3.1.2 γράφεται:

$$C(x) = k \cdot \frac{r}{\phi(r)} = \frac{n}{\phi(r)}$$

□

Για να συμπληρώσουμε την Πρόταση 1, θα υπολογίσουμε ένα άθροισμα το οποίο περιέχει τις απόλυτες τιμές κάθε όρου του αθροίσματος 3.1.1. Στη συνέχεια θα συμβολίσουμε με W(m) το πλήθος των διαιρετών ενός θετικού ακεραίου m που είναι ελεύθεροι τετραγώνων.

Λήμμα 1. *Έστω m θετικός ακέραιος. Τότε:*

$$\sum_{d|m} \frac{|\mu(d)|}{\phi(d)} \sum_{\substack{e|m \\ (d,m/e)=1}} \phi(de) = m \cdot W(m) \tag{3.1.3}$$

Απόδειξη

Παρατηρώντας την σχέση 3.1.3 συμπαιραίνουμε ότι οι μη μηδενικοί όροι του αθροίσματος είναι αυτοί όπου οι διαιρέτες d του m είναι ελεύθεροι τετραγώνου. Γράφουμε το m ως $m = m_1 m_2$, όπου ο παράγοντας m_1 αποτελείται από τους πρώτους του m (στην αντίστοιχη δύναμη που εμφανίζονται στο m), και περιέχονται συγχρόνως στο d , ενώ $(d, m_2) = 1$. Προφανώς ισχύει και $(m_1, m_2) = 1$. Όμοια γράφουμε και το e ως $e = e_1 e_2$. Ισχύει: $d|m \Leftrightarrow d|m_1 m_2 \Leftrightarrow d|m_1$ και

$\left(d, \frac{m}{e}\right) = \left(d, \frac{m_1 m_2}{e_1 e_2}\right) = \left(d, \frac{m_1}{e_1}\right)$. Επίσης, $e|m \Leftrightarrow e_1 e_2 | m_1 m_2 \Leftrightarrow e_1 | m_1$ και $e_2 | m_2$. Έτσι έχουμε:

$$\begin{aligned} T: &= \sum_{\substack{e|m \\ (d,m/e)=1}} \phi(de) = \sum_{\substack{e_1|m_1 \\ e_2|m_2 \\ (d,m_1/e_1)=1}} \phi(de_1e_2) = \sum_{\substack{e_1|m_1 \\ (d,m_1/e_1)=1}} \phi(de_1) \sum_{e_2|m_2} \phi(e_2) \\ &= m_2 \sum_{\substack{e_1|m_1 \\ (d,m_1/e_1)=1}} \phi(de_1) \end{aligned}$$

Στο τελευταίο άθροισμα θα πρέπει οι διαιρέτες e_1 του m_1 να είναι τέτοιοι ώστε να ισχύει $\left(d, \frac{m_1}{e_1}\right) = 1$. Αυτό μπορεί να συμβεί μόνο εάν $e_1 = m_1$. Τότε:

$$T = m_2 \phi(dm_1)$$

Ισχύει ότι $\phi(dm_1) = m_1 \phi(d)$. Πράγματι, έστω $d = p_1^{a_1} ... p_k^{a_k}$. Τότε $m_1 = p_1^{b_1} ... p_k^{b_k}$. Είναι:

$$\phi(dm_1) = dm_1 \left(1 - \frac{1}{p_1}\right) .... \left(1 - \frac{1}{p_k}\right) = m_1 \phi(d)$$

Επομένως,

$$T = m_2 m_1 \phi(d) = m\phi(d)$$

Άρα,

$$\sum_{d|m} \frac{|\mu(d)|}{\phi(d)} \sum_{\substack{e|m \\ (d,m/e)=1}} \phi(de) = m \sum_{d|m} \frac{|\mu(d)|}{\phi(d)} \phi(d) = m \sum_{d|m} |\mu(d)| = m \cdot W(m)$$

□

Πρόταση 2. *Έστω r ένας διαιρέτης του θετικού ακέραιου n και $k = \frac{n}{r}$. Τότε:*

$$(S :=) \sum_{d|r} \frac{|\mu(d)|}{\phi(d)} \sum_{\substack{e|k \\ (d,k/e)=1}} \phi(de) = k \cdot W(r) \tag{3.1.4}$$

Απόδειξη

Γράφουμε το n ως $n = n_0 n_1 n_2$ όπου τα $n_0,\ n_1,\ n_2$ (ανά δύο σχετικά πρώτοι) είναι τέτοιοι ώστε: (i) το $n_0|r$ και $(n_0, k) = 1$, (ii) το $n_2|k$ και $(n_2, r) = 1$, (iii) το n_1 αποτελείται από τους πρώτους του n (στην αντίστοιχη δύναμη που εμφανίζονται στο n) και περιέχονται συγχρόνως στον μ.κ.δ.(r, k). Δηλαδή, αν

$$n = \underbrace{p_1^{a_1} ... p_t^{a_t}}\ \underbrace{p_{t+1}^{a_{t+1}} ... p_l^{a_l}}\ \underbrace{p_{l+1}^{a_{l+1}} ... p_s^{a_s}}$$

η ανάλυση του $n = n_0 n_1 n_2$ σε πρώτους όπου $p_i \neq p_j$ για $i \neq j$, τότε οι πρώτοι $p_1, ..., p_t$ περιέχονται μόνο στο r, οι πρώτοι $p_{l+1}, ..., p_s$ περιέχονται μόνο στο k, ενώ οι πρώτοι $p_{t+1}, ..., p_l$ περιέχονται και στο r και στο k.

Παρατηρώντας τη σχέση 3.1.4 συμπεραίνουμε ότι μόνο οι ελεύθεροι τετραγώνου διαιρέτες d του r μας ενδιαφέρουν. Τώρα, οι ελεύθεροι τετραγώνου διαιρέτες του r είναι ακριβώς οι ελεύθεροι τετραγώνου διαιρέτες του $n_0 n_1$. Άρα,

$$W(n_0 n_1) = W(r), \tag{3.1.5}$$

και

$$S_1 := \sum_{d|r} \frac{|\mu(d)|}{\phi(d)} = \sum_{d|n_0 n_1} \frac{|\mu(d)|}{\phi(d)}.$$

Θέτουμε $d = d_0 c$ όπου $d_0|n_0$ και $c|n_1$. Τότε $(d_0, c) = 1$ και το S_1 γράφεται:

$$S_1 = \sum_{\substack{d_0|n_0 \\ c|n_1}} \frac{|\mu(d_0 c)|}{\phi(d_0 c)} = \sum_{d_0|n_0} \frac{|\mu(d_0)|}{\phi(d_0)} \sum_{c|n_1} \frac{|\mu(c)|}{\phi(c)}$$

Οι ελεύθεροι τετραγώνου διαιρέτες του n_1 είναι ακριβώς οι ελεύθεροι τετραγώνου διαιρέτες του $\frac{k}{n_2}$. Άρα,

$$W(n_1) = W\left(\frac{k}{n_2}\right) \tag{3.1.6}$$

Επίσης,

$$S_1 = \sum_{d_0|n_0} \frac{|\mu(d_0)|}{\phi(d_0)} \sum_{c|(k/n_2)} \frac{|\mu(c)|}{\phi(c)} \tag{3.1.7}$$

Έστω e ένας διαιρέτης του k. Επειδή $d_0|n_0$ και $(n_0,k)=1$, έπεται ότι $(d_0,k)=1$. Άρα και $(d_0,k/e)=1$. Έτσι, $(d,k/e)=(d_0c,k/e)=(c,k/e)$. Άρα:

$$S_2 : = \sum_{\substack{e|k\\(d,k/e)=1}} \phi(de) = \sum_{\substack{e|k\\(c,k/e)=1}} \phi(d_0ce) = \phi(d_0) \sum_{\substack{e|k\\(c,k/e)=1}} \phi(ce)$$

Θέτουμε $e=e_1e_2$ και $k=\frac{k}{n_2}\cdot n_2$ με $e_1|\frac{k}{n_2}$ και $e_2|n_2$. Είναι:

$$\left(c,\frac{k}{e}\right)=\left(c,\frac{\frac{k}{n_2}\cdot n_2}{e_1e_2}\right)=\left(c,\frac{\frac{k}{n_2}}{e_1}\right)=\left(c,\frac{k}{e_1n_2}\right)$$

διότι $c|n_1$ επομένως $\left(c,\frac{n_2}{e_2}\right)=1$. Άρα:

$$S_2=\phi(d_0)\sum_{\substack{e_1|\frac{k}{n_2}\\e_2|n_2\\(c,\frac{k}{e_1n_2})=1}}\phi(ce_1e_2)=\phi(d_0)\sum_{\substack{e_1|\frac{k}{n_2}\\(c,\frac{k}{e_1n_2})=1}}\phi(ce_1)\sum_{e_2|n_2}\phi(e_2)$$

Δηλαδή,

$$S_2=\phi(d_0)n_2\sum_{\substack{e_1|\frac{k}{n_2}\\(c,\frac{k}{e_1n_2})=1}}\phi(ce_1) \tag{3.1.8}$$

Άρα από τις σχέσεις 3.1.7 και 3.1.8 παίρνουμε:

$$\begin{aligned} S &= \sum_{d_0|n_0}\frac{|\mu(d_0)|}{\phi(d_0)}\sum_{c|(k/n_2)}\frac{|\mu(c)|}{\phi(c)}\cdot\phi(d_0)n_2\sum_{\substack{e_1|\frac{k}{n_2}\\(c,\frac{k}{e_1n_2})=1}}\phi(ce_1)\\ &= n_2\sum_{d_0|n_0}|\mu(d_0)|\sum_{c|(k/n_2)}\frac{|\mu(c)|}{\phi(c)}\sum_{\substack{e_1|\frac{k}{n_2}\\(c,\frac{k}{e_1n_2})=1}}\phi(ce_1)\end{aligned}$$

Χρησιμοποιώντας τώρα το Λήμμα 1 προκύπτει ότι:

$$S=n_2\sum_{d_0|n_0}|\mu(d_0)|\cdot\frac{k}{n_2}\cdot W\left(\frac{k}{n_2}\right)=kW(n_0)W(n_1)=kW(n_0n_1)=kW(r)$$

όπου στην 3η και 5η ισότητα χρησιμοποιήσαμε τις σχέσεις 3.1.6 και 3.1.5 αντίστοιχα.

□

3.2 Η απόδειξη του Θεωρήματος

Έστω $f_1(x), ..., f_r(x) \in \mathbb{F}_{q^n}[x]$ και $h(x) = \sum_{i=1}^{r} c_i f_i(x)$ όπου $c_i \in \mathbb{F}_q$, $i = 1, ..., r$ και $\deg h(x) = s$. Υποθέτουμε ότι είτε:

(i) $(s, q) = 1$ για όλα τα διαφορετικά πολυώνυμα $h(x)$ που παράγονται καθώς τα c_i, $i = 1, ..., r$ διατρέχουν τα στοιχεία του $\mathbb{F}_q$, είτε γενικότερα:

(ii) το πολυώνυμο $z^q - z - h(x)$ είναι ανάγωγο σε μία αλγεβρική θήκη του $\mathbb{F}_{q^n}$ για όλα τα διαφορετικά πολυώνυμα $h(x)$.

Έστω επίσης $t_1, ..., t_r \in \mathbb{F}_q$ και l ένας διαιρέτης του $q^n - 1$. Θέτουμε $L = \frac{q^n-1}{l}$. Ορίζουμε ως $N_{l,r}$ το πλήθος των (μη μηδενικών) στοιχείων $\gamma \in \mathbb{F}_{q^n}$ τάξης L, των οποίων τα ίχνη καθορίζονται από τη σχέση 1.0.1 , δηλαδή

$$Tr_n\left(f_i(\gamma)\right) = t_i, \quad i = 1, ..., r$$

Για να μπορέσουμε να διαχειριστούμε τη συνθήκη τάξης, ορίζουμε ως Λ_l να είναι η χαρακτηριστική συνάρτηση των στοιχείων του $\mathbb{F}_{q^n}^*$ τάξης L, δηλαδή για κάθε $\xi \in \mathbb{F}_{q^n}^*$

$$\Lambda_l(\xi) = \begin{cases} 1 & \alpha\nu \quad ord(\xi) = L \\ 0 & \delta\iota\alpha\varphi o\rho\varepsilon\tau\iota\kappa\alpha \end{cases}$$

Από την Πρόταση 1 μπορούμε να πάρουμε τη χαρακτηριστική συνάρτηση Λ_l συναρτήση των χαρακτήρων χ της πολλαπλασιαστικής ομάδας $\mathbb{F}_{q^n}^*$. Κάθε τέτοιος χαρακτήρας επεκτείνεται στο $\mathbb{F}_{q^n}$ ορίζοντας $\chi(0) = 0$. Έτσι, αν $\xi \in \mathbb{F}_{q^n}$ σύμφωνα με τη σχέση 3.1.1 έχουμε:

$$\Lambda_l(\xi) = \frac{\phi(L)}{q^n - 1} \sum_{d|L} \frac{\mu(d)}{\phi(d)} \sum_{\substack{e|l \\ (d,l/e)=1}} \sum_{ord\chi = de} \chi(\xi) \tag{3.2.1}$$

Επίσης η χαρακτηριστική συνάρτηση λ_t για τα στοιχεία $\xi \in \mathbb{F}_{q^n}$ με δεδομένο ίχνος $t \in \mathbb{F}_q$ είναι:

$$\lambda_t(\xi) = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \psi_1\left(c\left(Tr_n(\xi) - t\right)\right) = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \overline{\psi_1}(ct)\psi(c\xi) \tag{3.2.2}$$

όπου ψ_1 είναι ο κανονικός προσθετικός χαρακτήρας του $\mathbb{F}_q$ και ψ ο κανονικός προσθετικός χαρακτήρας του $\mathbb{F}_{q^n}$.

Πράγματι, από τη σχέση 2.2.1 έχουμε ότι $\psi = \psi_1 \circ Tr_n$. Έχουμε λοιπόν:

$$\lambda_t(\xi) = \begin{cases} 1 & \alpha\nu \ \ Tr_n(\xi) = t \\ 0 & \delta\iota\alpha\varphi o\rho\varepsilon\tau\iota\kappa\alpha \end{cases}$$

Έστω $\alpha \in \mathbb{F}_q$ με $\alpha \neq 0$. Τότε από τη σχέση 2.2.2 έχουμε ότι

$$\sum_{c\in\mathbb{F}_q} \psi_\alpha(c) = 0$$

ενώ αν $\alpha = 0$, τότε $\sum_{c\in\mathbb{F}_q} \psi_0(c) = \sum_{c\in\mathbb{F}_q} 1 = q$. Άρα:

$$\begin{aligned} \lambda_t(\xi) &= \frac{1}{q}\sum_{c\in\mathbb{F}_q} \psi_{Tr_n(\xi)-t}(c) = \frac{1}{q}\sum_{c\in\mathbb{F}_q} \psi_1\left((Tr_n(\xi)-t)\,c\right) \\ &= \frac{1}{q}\sum_{c\in\mathbb{F}_q} \psi_1\left(cTr_n(\xi)\right)\psi_1\left(-ct\right) = \frac{1}{q}\sum_{c\in\mathbb{F}_q} \psi_1\left(Tr_n(c\xi)\right)\overline{\psi_1}\left(ct\right) \\ &= \frac{1}{q}\sum_{c\in\mathbb{F}_q} \psi(c\xi)\overline{\psi_1}\left(ct\right) \end{aligned}$$

Το πλήθος των μη μηδενικών στοιχείων $\gamma \in \mathbb{F}_{q^n}$ τάξης L των οποίων τα ίχνη καθορίζονται από τη σχέση 1.0.1 μπορεί να εκφραστεί ως:

$$N_{l,r} = \sum_{\xi\in\mathbb{F}_{q^n}} \Lambda_l(\xi)\lambda_{t_1}(f_1(\xi))...\lambda_{t_r}(f_r(\xi))$$

Τώρα με τη βοήθεια των σχέσεων 3.2.1 και 3.2.2 παίρνουμε:

$$\begin{aligned} N_{l,r} &= \sum_{\xi\in\mathbb{F}_{q^n}} \frac{\phi(L)}{q^n-1}\sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l \\ (d,l/e)=1}}\sum_{ord\chi=de}\chi(\xi)\prod_{i=1}^{r}\frac{1}{q}\sum_{c_i\in\mathbb{F}_q}\overline{\psi_1}(c_it_i)\psi(c_if_i(\xi)) \\ &= \frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l \\ (d,l/e)=1}}\sum_{ord\chi=de}\sum_{\xi\in\mathbb{F}_{q^n}}\chi(\xi)\prod_{i=1}^{r}\sum_{c_i\in\mathbb{F}_q}\overline{\psi_1}(c_it_i)\psi(c_if_i(\xi)) \end{aligned}$$

Είναι:

$$\begin{aligned} \prod_{i=1}^{r}\sum_{c_i\in\mathbb{F}_q}\overline{\psi_1}(c_it_i)\psi(c_if_i(\xi)) &= \sum_{(c_1,...,c_r)\in\mathbb{F}_q^r}\overline{\psi_1}(c_1t_1)\psi(c_1f_1(\xi))...\overline{\psi_1}(c_rt_r)\psi(c_rf_r(\xi)) \\ &= \sum_{(c_1,...,c_r)\in\mathbb{F}_q^r}\overline{\psi_1}(c_1t_1+...+c_rt_r)\psi\left(\sum_{i=1}^{r}c_if_i(\xi)\right) \end{aligned}$$

Επομένως το πλήθος $N_{l,r}$ γράφεται:

$$\begin{aligned} N_{l,r} &= \frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{\xi\in\mathbb{F}_{q^n}}\chi(\xi)\sum_{(c_1,...,c_r)\in\mathbb{F}_q^r}\overline{\psi_1}(c_1t_1+...+c_rt_r)\psi(\sum_{i=1}^{r}c_if_i(\xi)) \\ &= \frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,...,c_r)\in\mathbb{F}_q^r}\overline{\psi_1}(c_1t_1+...+c_rt_r)\sum_{\xi\in\mathbb{F}_{q^n}}\chi(\xi)\psi(\sum_{i=1}^{r}c_if_i(\xi)) \end{aligned}$$

Θέτουμε:

$$h(x)=\sum_{i=1}^{r}c_if_i(x)\in\mathbb{F}_{q^n}[x],\ c_i\in\mathbb{F}_q,\ i=1,...,r$$

και

$$S_n(h,\chi)=\sum_{\xi\in\mathbb{F}_{q^n}}\chi(\xi)\psi(h(\xi))$$

Να σημειώσουμε ότι η απεικόνιση $h(x)$ μεταβάλεται καθώς τα $c_1,...,c_r$ διατρέχουν τα στοιχεία του $\mathbb{F}_q$. Με τους συμβολισμούς αυτούς το $N_{l,r}$ παίρνει τη μορφή:

$$N_{l,r}=\frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,...,c_r)\in\mathbb{F}_q^r}\overline{\psi_1}(c_1t_1+...+c_rt_r)S_n(h,\chi) \tag{3.2.3}$$

Θεώρημα 7. *(Φράγμα Weil) Έστω χ πολλαπλασιαστικός χαρακτήρας του $\mathbb{F}_q$ με $\chi\neq\chi_0$ τάξης d όπου $d|q-1$ και ψ προσθετικός χαρακτήρας του $\mathbb{F}_q$ με $\psi\neq\psi_0$. Έστω επίσης $f(x),g(x)\in\mathbb{F}_q[x]$ πολυώνυμα τέτοια ώστε το $f(x)$ να έχει ακριβώς m διακριτές ρίζες και το $g(x)$ να έχει βαθμό s. Υποθέτουμε ότι είτε:*

(i) $(d,\deg f)=(s,q)=1$ είτε γενικότερα:

(ii) τα πολυώνυμα $y^d-f(x)$ και $z^q-z-g(x)$ είναι ανάγωγα σε μία αλγεβρική θήκη του $\mathbb{F}_q$.

Τότε:

$$\left|\sum_{x\in\mathbb{F}_q}\chi(f(x))\psi(g(x))\right|\leq(m+s-1)q^{\frac{1}{2}} \tag{3.2.4}$$

□

Θα εφαρμόσουμε τώρα το Θεώρημα 7 στην δική μας περίπτωση. Έστω χ πολλαπλασιαστικός χαρακτήρας του $\mathbb{F}_{q^n}$ διαφορετικός του τετριμμένου χαρακτήρα χ_0. Θέλουμε να έχει τάξη de όπου $de|(q^n-1)$ (Πράγματι, $d|L=\frac{q^n-1}{l} \Leftrightarrow dl|(q^n-1)$ και $e|l$. Άρα $de|(q^n-1)$). Επίσης έχουμε συμβολίσει με ψ τον κανονικό προσθετικό χαρακτήρα του $\mathbb{F}_{q^n}$ (που είναι διαφορετικός του ψ_0). Έστω $f(x) \in \mathbb{F}_{q^n}[x]$ πολυώνυμο με $f(x)=x$ το οποίο έχει ακριβώς 1 ρίζα και έστω $h(x)=\sum_{i=1}^{r} c_i f_i(x) \in \mathbb{F}_{q^n}[x],\ c_i \in \mathbb{F}_q,\ i=1,...,r$ με βαθμό s. Έχουμε υποθέσει ότι το πολυώνυμο $z^{q^n}-z-h(x)$ είναι ανάγωγο για όλους τους $\mathbb{F}_q-$γραμμικούς συνδιασμούς των $f_1,...,f_r$.

Θα δείξουμε ότι το πολυώνυμο $y^{de}-x$ είναι επίσης ανάγωγο σε μία αλγεβρική θήκη του $\mathbb{F}_{q^n}$. Πράγματι, έστω όχι. Τότε $y^{de}-x=g_1(x,y)g_2(x,y)$, όπου $g_1,g_2 \in \mathbb{F}_{q^n}[x]$ όχι σταθερά πολυώνυμα. Είναι $deg(y^{de}-x)=1$ ως πολυώνυμο του x. Άρα θα πρέπει είτε $g_1(x,y)=g_1(y)$ είτε $g_2(x,y)=g_2(y)$. Έστω $g_1(x,y)=g_1(y)=a_k y^k+...+a_1 y+a_0,\quad a_i \in \mathbb{F}_{q^n},\ i=1,...,k$ και $g_2(x,y)=b_m y^m+...+b_1 y+b_0+cx$. Είναι:

$$g_1(y)g_2(x,y)=a_k b_m y^{k+m}+...+b_0 a_0+(a_k y^k+...+a_1 y+a_0)cx$$

Θα πρέπει $(a_k y^k+...+a_1 y+a_0)c=-1$. Άρα $a_k=...=a_1=0$ και $a_0 c=-1$. Δηλαδή $g_1(y)=a_0$. Άτοπο διότι τα g_1,g_2 δεν είναι σταθερά πολυώνυμα.

Επομένως ικανοποιείται η προυπόθεση (ii) του Θεωρήματος 7. Η προυπόθεση (i) ικανοποιείται με προφανή τρόπο. Άρα από την σχέση 3.2.4 για $\chi \neq \chi_0$ προκύπτει ότι:

$$|S_n(h,\chi)|=\left|\sum_{\xi \in \mathbb{F}_{q^n}} \chi(\xi)\psi(h(\xi))\right| \leq (1+s-1)q^{\frac{n}{2}}=sq^{\frac{n}{2}} \qquad (3.2.5)$$

Στη συνέχεια διατυπώνουμε το Θεώρημα Weil το οποίο θα μας βοηθήσει να εξετάσουμε τι συμβαίνει με το $S_n(h,\chi)$ όταν το $\chi=\chi_0$.

Θεώρημα 8. *(Φράγμα Weil) Έστω ψ προσθετικός χαρακτήρας του $\mathbb{F}_q$ με $\psi \neq \psi_0$. Έστω επίσης $g(x) \in \mathbb{F}_q[x]$ πολυώνυμο βαθμού s. Υποθέτουμε ότι είτε:*

(i) $s<q$ και $(s,q)=1$, είτε γενικότερα:

(ii) το πολυώνυμο $z^q - z - g(x)$ είναι ανάγωγο σε μία αλγεβρική θήκη του $\mathbb{F}_q$.

Τότε:

$$\left| \sum_{x \in \mathbb{F}_q} \psi(g(x)) \right| \leq (s-1) q^{\frac{1}{2}} \tag{3.2.6}$$

□

Έχουμε λοιπόν:

$$\begin{aligned} S_n(h, \chi_0) &= \sum_{\xi \in \mathbb{F}_{q^n}} \chi_0(\xi)\psi(h(\xi)) = \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi_0(\xi)\psi(h(\xi)) + \chi_0(0)\psi(h(0)) \\ &= \sum_{\xi \in \mathbb{F}_{q^n}^*} 1 \cdot \psi(h(\xi)) + 0 = \sum_{\xi \in \mathbb{F}_{q^n}^*} \psi(h(\xi)) \end{aligned}$$

Εφαρμόζοντας το Θεώρημα 8 για το πολυώνυμο $h(x) = \sum_{i=1}^{r} c_i f_i(x) \in \mathbb{F}_{q^n}[x]$, $c_i \in \mathbb{F}_q$, $i = 1, ..., r$ με βαθμό s και ψ τον κανονικό προσθετικό χαρακτήρα του $\mathbb{F}_{q^n}$, από τη σχέση 3.2.6 παίρνουμε:

$$\begin{aligned} |S_n(h, \chi_0)| &= \left| \sum_{\xi \in \mathbb{F}_{q^n}^*} \psi(h(\xi)) \right| = \left| \sum_{\xi \in \mathbb{F}_{q^n}} \psi(h(\xi)) - \psi(h(0)) \right| \\ &\leq \left| \sum_{\xi \in \mathbb{F}_{q^n}} \psi(h(\xi)) \right| + |\psi(h(0))| \leq (s-1) q^{\frac{n}{2}} + 1 \leq s q^{\frac{n}{2}} \end{aligned}$$

Τώρα συνδιάζοντας την τελευταία σχέση και τη σχέση 3.2.5 προκύπτει ότι για οποιοδήποτε χαρακτήρα χ του $\mathbb{F}_{q^n}$ ισχύει:

$$|S_n(h, \chi)| \leq s q^{\frac{n}{2}} \tag{3.2.7}$$

Υπενθυμίζουμε ότι έχουμε θέσει

$$S = \max_{i=1,...,r} \deg f_i(x) = \max_{(c_1,...,c_r) \in \mathbb{F}_q^r} \deg \left(\sum_{i=1}^{r} c_i f_i(x) \right)$$

Αφού το πολυώνυμο $h(x)$ μεταβάλεται καθώς τα $c_1, ..., c_r$ διατρέχουν τα στοιχεία του $\mathbb{F}_q$, όμοια μεταβάλεται και ο βαθμός του s. Όμως $s \leq S$ για όλους τους διαφορετικούς βαθμούς s των διαφορετικών $h(x)$. Επομένως η σχέση 3.2.7 παίρνει τη μορφή:

$$|S_n(h, \chi)| \leq S q^{\frac{n}{2}} \tag{3.2.8}$$

Θεώρημα 9. *Έστω* $f_1(x), ..., f_r(x) \in \mathbb{F}_{q^n}[x]$ *και* $h(x) = \sum_{i=1}^{r} c_i f_i(x)$ *όπου* $c_i \in \mathbb{F}_q$, $i = 1, ..., r$ *και* $\deg h(x) = s$. *Υποθέτουμε ότι είτε:*

(*i*) $(s, q) = 1$ *για όλα τα διαφορετικά πολυώνυμα* $h(x)$ *που παράγονται καθώς τα* c_i, $i = 1, ..., r$ *διατρέχουν τα στοιχεία του* $\mathbb{F}_q$, *είτε γενικότερα:*

(*ii*) *το πολυώνυμο* $z^q - z - h(x)$ *είναι ανάγωγο σε μία αλγεβρική θήκη του* $\mathbb{F}_{q^n}$ *για όλα τα διαφορετικά πολυώνυμα* $h(x)$.

Έστω επίσης $t_1, ..., t_r \in \mathbb{F}_q$ *και* l *ένας οποιοσδήποτε διαιρέτης του* $q^n - 1$. *Τότε:*

$$N_{l,r} \geq \frac{\phi(L) q^{\frac{n}{2}-r}}{q^n - 1} \left\{ \frac{q^n - 1}{q^{\frac{n}{2}}} - (q^r - 1) SlW(L) \right\}$$

Απόδειξη. Θέτουμε

$$M = \sum_{d|L} \frac{\mu(d)}{\phi(d)} \sum_{\substack{e|l \\ (d,l/e)=1}} \sum_{ord\chi = de} \sum_{(c_1,...,c_r) \in \mathbb{F}_q^r} \overline{\psi_1}(c_1 t_1 + ... + c_r t_r) S_n(h, \chi)$$

Δηλαδή η σχέση 3.2.3 γράφεται: $N_{l,r} = \frac{\phi(L)}{(q^n-1)q^r} \cdot M$. Όταν όλα τα c_i, $i = 1, ..., r$ είναι μηδέν, τότε το $h(x)$ είναι το μηδενικό πολυώνυμο. Είναι:

$$S_n(0, \chi) = \sum_{\xi \in \mathbb{F}_{q^n}} \chi(\xi) \psi(0) = \sum_{\xi \in \mathbb{F}_{q^n}} \chi(\xi) = \sum_{\xi \in \mathbb{F}_{q^n}^*} \chi(\xi) = \begin{cases} q^n - 1 & \text{αν } \chi = \chi_0 \\ 0 & \text{αν } \chi \neq \chi_0 \end{cases},$$

όπως προκύπτει από τη 2.2.3 σχέση ορθογωνιότητας. Άρα:

$$
\begin{aligned}
M &= \sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,\ldots,0)}\overline{\psi_1}(c_1t_1+\ldots+c_rt_r)S_n(h,\chi)+\\
&+ \sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}S_n(0,\chi)\\
&= \sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,\ldots,0)}\overline{\psi_1}(c_1t_1+\ldots+c_rt_r)S_n(h,\chi)+\\
&+ \sum_{\substack{d|L\\d>1}}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}S_n(0,\chi)+\sum_{e|l}\sum_{ord\chi=e}S_n(0,\chi)\\
&= \sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,\ldots,0)}\overline{\psi_1}(c_1t_1+\ldots+c_rt_r)S_n(h,\chi)+\\
&+ 0+\sum_{\substack{e|l\\e>1}}\sum_{ord\chi=e}S_n(0,\chi)+(q^n-1)\\
&= \sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,\ldots,0)}\overline{\psi_1}(c_1t_1+\ldots+c_rt_r)S_n(h,\chi)+\\
&+ 0+(q^n-1)
\end{aligned}
$$

Δηλαδή,

$$
M = \sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,\ldots,0)}\overline{\psi_1}(c_1t_1+\ldots+c_rt_r)S_n(h,\chi)+(q^n-1)
$$

Έτσι το $N_{l,r}$ γράφεται:

$$
N_{l,r}=\frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,\ldots,0)}\overline{\psi_1}(c_1t_1+\ldots+c_rt_r)S_n(h,\chi)+\frac{\phi(L)}{q^r}
$$

Άρα:

$$\begin{aligned}
\left|N_{l,r}-\frac{\phi(L)}{q^r}\right| &= \left|\frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{\mu(d)}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,.0)}\overline{\psi_1}(c_1t_1+\ldots+c_rt_r)S_n(h,\chi)\right| \\
&\leq \frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{|\mu(d)|}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}\sum_{(c_1,\ldots,c_r)\in\mathbb{F}_q^r\setminus(0,\ldots,0)}|S_n(h,\chi)| \\
&\leq \frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{|\mu(d)|}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\sum_{ord\chi=de}Sq^{\frac{n}{2}}(q^r-1) \\
&= \frac{\phi(L)}{(q^n-1)q^r}\sum_{d|L}\frac{|\mu(d)|}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\phi(de)Sq^{\frac{n}{2}}(q^r-1) \\
&= \frac{\phi(L)}{(q^n-1)q^r}Sq^{\frac{n}{2}}(q^r-1)\sum_{d|L}\frac{|\mu(d)|}{\phi(d)}\sum_{\substack{e|l\\(d,l/e)=1}}\phi(de) \\
&= \frac{\phi(L)}{(q^n-1)q^r}Sq^{\frac{n}{2}}(q^r-1)lW(L)
\end{aligned}$$

όπου στην τελευταία ισότητα χρησιμοποιούμε την Πρόταση 2. Έχουμε λοιπόν:

$$\begin{aligned}
N_{l,r} &\geq \frac{\phi(L)}{q^r}-\frac{\phi(L)}{(q^n-1)q^r}Sq^{\frac{n}{2}}(q^r-1)lW(L) \\
&= \frac{\phi(L)q^{\frac{n}{2}-r}}{q^n-1}\left\{\frac{q^n-1}{q^{\frac{n}{2}}}-(q^r-1)SlW(L)\right\}
\end{aligned}$$

□

Είμαστε έτοιμοι τώρα να αποδείξουμε το Θεώρημα 1. Για να το αποδείξουμε αρκεί να δείξουμε ότι $N_{l,r}>0$. Αρκεί λοιπόν να δείξουμε ότι:

$$\frac{q^n-1}{q^{\frac{n}{2}}}>(q^r-1)SlW(L)\ \Leftrightarrow\ W(L)<\frac{q^n-1}{q^{\frac{n}{2}}(q^r-1)Sl}$$

Έστω m θετικός ακέραιος. Συμβολίζουμε με $\omega(m)$ το πλήθος των διαφορετικών πρώτων παραγόντων του m, ενώ έχουμε συμβολίσει με $W(m)$ το πλήθος των διαιρετών του m που είναι ελεύθεροι τετραγώνου.

Λήμμα 2. *Για κάθε* $m \in \mathbb{N}$ *ισχύει:*

$$W(m) = 2^{\omega(m)} \leq 4.9m^{\frac{1}{4}}$$

Απόδειξη

Έστω $m = p_1^{a_1}...p_k^{a_k}$ όπου $p_i \neq p_j$ για $i \neq j$ και $p_1 < p_2 < ... < p_k$. Τότε $\omega(m) = k$. Οι ελεύθεροι τετραγώνων διαιρέτες του m είναι οι $p_1, ..., p_k, p_1p_2, ..., p_{k-1}p_k, ..., p_1...p_k$. Άρα:

$$W(m) = \left(\begin{array}{c} k \\ 1 \end{array} \right) + \left(\begin{array}{c} k \\ 2 \end{array} \right) + ... + \left(\begin{array}{c} k \\ k \end{array} \right) = 2^k = 2^{\omega(m)}$$

Επίσης είναι $m \geq p_1...p_k$. Έστω $p_1, ..., p_s \leq 2^4$, δηλαδή $p_1, ..., p_s \in A$ όπου $A = \{2, 3, 5, 7, 11, 13\}$. Είναι $s \leq 6$. Τότε:

$$m \geq p_1...p_s(2^4)^{k-s} \quad \Leftrightarrow \quad 2^{4k} \leq \frac{m2^{4s}}{p_1...p_s} \quad \Leftrightarrow \quad 2^k \leq \frac{m^{\frac{1}{4}}2^s}{(p_1...p_s)^{\frac{1}{4}}}$$

Ισχυρισμός:

$$\frac{2^s}{(p_1...p_s)^{\frac{1}{4}}} \leq 4.9, \quad s = 1, ..., 6$$

Πράγματι, για $s = 1$, έχουμε $\frac{2}{p_1^{1/4}}$ όπου $p_1 \in A$. Είναι:

$$\frac{2}{p_1^{1/4}} \leq \frac{2}{2^{1/4}} \simeq 1.6818$$

Για $s = 2$, έχουμε $\frac{2^2}{(p_1p_2)^{1/4}}$ όπου $p_1, p_2 \in A$. Είναι:

$$\frac{2^2}{(p_1p_2)^{1/4}} \leq \frac{2^2}{(2 \cdot 3)^{1/4}} = \frac{4}{6^{1/4}} \simeq 2.5558$$

Για $s = 3$, έχουμε $\frac{2^3}{(p_1p_2p_3)^{1/4}}$ όπου $p_1, p_2, p_3 \in A$. Είναι:

$$\frac{2^3}{(p_1p_2p_3)^{1/4}} \leq \frac{2^3}{(2 \cdot 3 \cdot 5)^{1/4}} = \frac{8}{30^{1/4}} \simeq 3.4183$$

Για $s = 4$, έχουμε $\frac{2^4}{(p_1p_2p_3p_4)^{1/4}}$ όπου $p_1, p_2, p_3, p_4 \in A$. Είναι:

$$\frac{2^4}{(p_1p_2p_3p_4)^{1/4}} \leq \frac{2^4}{(2 \cdot 3 \cdot 5 \cdot 7)^{1/4}} = \frac{16}{210^{1/4}} \simeq 4.203$$

Για $s=5$, έχουμε $\frac{2^5}{(p_1p_2p_3p_4p_5)^{1/4}}$ όπου $p_1,p_2,p_3,p_4,p_5 \in A$. Είναι:

$$\frac{2^5}{(p_1p_2p_3p_4p_5)^{1/4}} \leq \frac{2^5}{(2\cdot 3\cdot 5\cdot 7\cdot 11)^{1/4}} = \frac{32}{2310^{1/4}} \simeq 4.0153$$

Για $s=6$, έχουμε $\frac{2^6}{(p_1p_2p_3p_4p_5p_6)^{1/4}}$ όπου $p_1,p_2,p_3,p_4,p_5,p_6 \in A$. Είναι:

$$\frac{2^6}{(p_1p_2p_3p_4p_5p_6)^{1/4}} = \frac{2^6}{(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13)^{1/4}} = \frac{64}{30030^{1/4}} \simeq 4.8617$$

□

Έτσι ο ισχυρισμός αποδείχθηκε. Από το Λήμμα 2 προκύπτει λοιπόν ότι:

$$W(L) \leq 4.9\left(\frac{q^n-1}{l}\right)^{\frac{1}{4}} < 4.9\left(\frac{q^n}{l}\right)^{\frac{1}{4}}$$

Επομένως, αρκεί να δείξουμε ότι:

$$4.9\left(\frac{q^n}{l}\right)^{\frac{1}{4}} \leq \frac{q^n-1}{q^{n/2}(q^r-1)Sl}$$

Έχουμε:

$$n>r \;\Leftrightarrow\; q^n>q^r \;\Leftrightarrow\; q^{n+r}-q^n<q^{n+r}-q^r \;\Leftrightarrow\; q^n(q^r-1)<q^r(q^n-1) \;\Leftrightarrow$$

$$\Leftrightarrow\; \frac{q^n}{q^r}<\frac{q^n-1}{q^r-1} \;\Leftrightarrow\; \frac{q^n}{q^{n/2}q^rSl}<\frac{q^n-1}{q^{n/2}(q^r-1)Sl}$$

Άρα αρκεί να δείξουμε ότι:

$$4.9\frac{q^{n/4}}{l^{1/4}} \leq \frac{q^n}{q^{n/2}q^rSl} \;\Leftrightarrow\; 4.9Sl^{3/4} \leq q^{n/4-r} \;\Leftrightarrow\; \frac{n}{4}-r \geq \log_q 4.9Sl^{3/4} \;\Leftrightarrow$$

$$\Leftrightarrow\; n \geq 4\left[r+\log_q 4.9Sl^{3/4}\right]$$

το οποίο ισχύει από την υπόθεση του Θεωρήματος 1.

3.3 Παραδείγματα

Παράδειγμα 2. *Έστω $q=2$ και $f_1(x)=x$, $f_2(x)=x^3+x+1$, $f_3(x)=x^5+x^2+1$ πολυώνυμα του $\mathbb{F}_{2^n}$. Θέτουμε $h(x)=\sum_{i=1}^{3}c_if_i(x)$ όπου $c_i \in \mathbb{F}_2$,*

$i = 1, ..., 3$. *Τότε* $\deg h(x) = 1$ *ή* 3 *ή* 5, *δηλαδή* $(\deg h(x), 2) = 1$ *και* $S = 5$. *Άρα ικανοποιείται η προυπόθεση* (i) *του Θεωρήματος 1. Ας θέσουμε* $l = 1$, *οπότε* $L = \frac{2^n-1}{1} = 2^n - 1$, *δηλαδή θα εξετάσουμε την ύπαρξη πρωταρχικών στοιχείων. Σύμφωνα με το Θεώρημα 1 για* n *τέτοιο ώστε:*

$$n > 4\left[r + log_q 4.9 l^{3/4} S\right]$$

$$n > 4\left[3 + log_2 4.9 \cdot 1^{3/4} \cdot 5\right]$$

$$n \geq 31,$$

και για κάθε $t_1, t_2, t_3 \in \mathbb{F}_2$ *υπάρχει ένα πρωταρχικό στοιχείο* $\gamma \in \mathbb{F}_{2^n}$ *τέτοιο ώστε:*

$$Tr_n\left(f_1(\gamma)\right) = t_1 \text{ και } Tr_n\left(f_2(\gamma)\right) = t_2 \text{ και } Tr_n\left(f_3(\gamma)\right) = t_3$$

Χρησιμοποιώντας το Θεώρημα 9 μπορούμε να εκτιμήσουμε το πλήθος των πρωταρχικών στοιχείων του $\mathbb{F}_{2^n}$ *με τις παραπάνω ιδιότητες από τη σχέση:*

$$N_{l,r} \geq \frac{\phi(L) q^{\frac{n}{2}-r}}{q^n - 1}\left\{\frac{q^n - 1}{q^{\frac{n}{2}}} - (q^r - 1) S \cdot l \cdot W(L)\right\}$$

όπου στο παράδειγμα μας παίρνει τη μορφή:

$$N_{1,3} \geq \frac{\phi(2^n - 1) 2^{\frac{n}{2}-3}}{2^n - 1}\left\{\frac{2^n - 1}{2^{\frac{n}{2}}} - 35 W(2^n - 1)\right\}$$

Για διάφορες τιμές του n *παίρνουμε το παρακάτω πίνακα:*

n	$N_{1,3}$
31	*268232714*
32	*263847936*

Παράδειγμα 3. *Έστω* $q = 3$ *και* $f_1(x) = x$, $f_2(x) = x^2 + x + 1$ *πολυώνυμα του* $\mathbb{F}_{3^n}$. *Θέτουμε* $h(x) = \sum_{i=1}^{3} c_i f_i(x)$ *όπου* $c_i \in \mathbb{F}_3$, $i = \{1, 2\}$. *Τότε* $\deg h(x) = 1$ *ή* 2 , *δηλαδή* $(\deg h(x), 3) = 1$ *και* $S = 2$. *Άρα ικανοποιείται η προυπόθεση* (i) *του Θεωρήματος 1. Θέτουμε και πάλι* $l = 1$, *οπότε* $L = \frac{3^n-1}{1} = 3^n - 1$. *Άρα από το Θεώρημα 1 για* n *τέτοιο ώστε:*

$$n > 4\left[2 + log_3 4.9 \cdot 1^{3/4} \cdot 2\right]$$

$$n \geq 17,$$

και για κάθε $t_1, t_2 \in \mathbb{F}_3$ *υπάρχει ένα πρωταρχικό στοιχείο* $\gamma \in \mathbb{F}_{3^n}$ *τέτοιο ώστε:*

$$Tr_n\left(f_1(\gamma)\right) = t_1 \text{ } \kappa\alpha\iota \text{ } Tr_n\left(f_2(\gamma)\right) = t_2,$$

ενώ από το Θεώρημα 9 έχουμε:

$$N_{1,2} \geq \frac{\phi(3^n-1)3^{\frac{n}{2}-2}}{3^n-1}\left\{\frac{3^n-1}{3^{\frac{n}{2}}} - 16W(3^n-1)\right\}$$

Για διάφορες τιμές του n *παίρνουμε το παρακάτω πίνακα:*

n	$N_{1,3}$
17	*8065626*
18	*17634103*

Βιβλιογραφία

[1] S.D. Cohen, Finite Fiel Elements with Specified Order and Traces, Designs Codes and Cryptography, Vol.36 (2005) pp.331-340

[2] S.D. Cohen, The orders of releted elements of a finite field, Ramanujan Journal, Vol.7 (2003) pp.173-201

[3] Wolfgang M. Schmidt, Lecture Notes in Mathematics, Equations over Finite Fields, An Elementary Approach, Springer

[4] R. Lidl, H. Niederreiter, Encyclopedia of Mathematics and its applications, Finite fields, Cambridge University Press

[5] Ferruh Ozbudak, Designs Codes and ,Cryptography, Elements of Prescribed Order, Prescribed Traces and Systems of Rational Functions Over Finite Fields, Vol.34 (2005) pp.35-54