Κοκκίνου Χριστίνα

Πρωταρχικές κανονικές βάσεις πεπερασμένων σωμάτων

Πανεπιστήμιο Κρήτης
Τμήμα Μαθηματικών

Περιεχόμενα

0.1 Εισαγωγή

Έστω $q > 1$ μια δύναμη πρώτου αριθμού. Συμβολίζουμε ένα πεπερασμένο σώμα με q στοιχεία ως $\mathbb{F}_q$. Με τον όρο κανονική βάση του $\mathbb{F}_{q^m}$ πάνω απ΄το $\mathbb{F}_q$ εννοούμε μια βάση της μορφής

$$(a, a^q, a^{q^2}, ..., a^{q^{m-1}}),$$

με $a \in \mathbb{F}_{q^m}$. Συμβολίζουμε με $\mathbb{F}_{q^m}^*$ τη πολλαπλασιαστική ομάδα του $\mathbb{F}_{q^m}$. Είναι γνωστό ότι η ομάδα $\mathbb{F}_{q^m}^*$ είναι κυκλική. Ονομάζουμε πρωταρχικό στοιχείο του σώματος $\mathbb{F}_{q^m}$ ένα γεννήτορα της ομάδας αυτής, δηλαδή ένα στοιχείο τάξης $q^m - 1$.

Στόχος μας είναι να αποδείξουμε το εξής θεώρημα: «Σχεδόν για κάθε» ζεύγος (q, m), όπου q είναι δύναμη πρώτου και $m \in \mathbb{N}$, υπάρχει πρωταρχικό στοιχείο $a \in \mathbb{F}_{q^m}$ τέτοιο ώστε η $(a, a^q, a^{q^2}, ..., a^{q^{m-1}})$ να είναι κανονική βάση του $\mathbb{F}_{q^m}$. Με την έκφραση «σχεδόν για κάθε» εννοούμε για κάθε εκτός απο ένα πεπερασμένο πλήθος. Μια τέτοια βάση θα την ονομάζουμε πρωταρχική κανονική βάση της επέκτασης $\mathbb{F}_{q^m}/\mathbb{F}_q$.

Στο κεφάλειο 1 δίνουμε τους ορισμούς και αποδεικνύουμε τις βασικές ιδιότητες των αριθμητικών συναρτήσεων, όπως του Euler και του Moebius, που θα χρησιμοποιήσουμε στη συνέχεια. Επίσης ορίζουμε την ομάδα των χαρακτήρων μιας πεπερασμένης αβελιανής ομάδας και αποδεικνύουμε τις βασικές σχέσεις ορθογωνιότητας.

Στο κεφάλειο 2 μελετάμε την δομή των $\mathbb{F}_{q^m}^*$ και $\mathbb{F}_{q^m}$ βλέποντας τα ως $\mathbb{Z}$ και $\mathbb{F}_q[X]$ modules αντίστοιχα. Και στις δύο περιπτώσεις δείχνουμε ότι τα modules είναι κυκλικά. Άμεση συνέπεια είναι η ύπαρξη πρωταρχικών στοιχείων και κανονικών βάσεων.

Στο κεφάλειο 3 δίνουμε τις χαρακτηριστικές συναρτήσεις των πρωταρχικών στοιχείων καθώς και των στοιχείων που παράγουν κανονικές βάσεις. Στη συνέχεια χρησιμοποιούμε τις χαρακτηριστικές συναρτήσεις για να αποδείξουμε ότι πρωταρχικές κανονικές βάσεις υπάρχουν εφόσον ικανοποιήται μια συνθήκη, η οποία σχετίζεται με τα q και m. Τελειώνουμε την εργασία με μια σειρά αναλυτικών υπολογισμών που δείχνουν ότι η συνθήκη ικανοποιήται για «σχεδόν όλα» τα q και m.

Για την εργασία αυτή χρησιμοποιήσαμε τα άρθρα [1, 2] και το βιβλίο [3].

Κεφάλαιο 1

Η συνάρτηση του *Mobius* και η ομάδα των χαρακτήρων

1.1 Η συνάρτηση του *Mobius*

Θα ορίσουμε τη συνάρτηση του *Mobius* τόσο για τα πολυώνυμα όσο και για τους φυσικούς αριθμούς.
Θα περιορίσουμε όμως τις αποδείξεις μας μόνο στην περίπτωση των πολυωνύμων, καθότι για τους φυσικούς αριθμούς οι αποδείξεις είναι ανάλογες.

Ορισμός.
Η συνάρτηση του *Mobius* για τα πολυώνυμα καθορίζεται ως εξής:
Έστω $f \neq 0 \in \mathbb{F}_q[x]$ τότε,
$M(f) = 1$ αν $\deg f = 0$
Αν $f = f_1^{p_1} \cdots f_k^{p_k}$ και $\deg f \geq 1$ τότε:
$M(f) = (-1)^k$ αν $p_1 = \cdots = p_k = 1$
$M(f) = 0$ αν $\exists p_i, i = 1, .., k$ τ.ω. $p_i \neq 1$

Όμοια για τους φυσικούς αριθμούς έχουμε:
$\mu(1) = 1$
Αν $n = n_1^{a_1} \cdots n_k^{a_k}$, $n_i, i = 0, .., k$ πρώτοι και $n \geq 1$ τότε:
$\mu(n) = (-1)^k$ αν $a_1 = \cdots = a_k = 1$
$\mu(n) = 0$ αν $\exists a_i, i = 1, .., k$ τ.ω. $a_i \neq 1$

Θεώρημα 1.1 *Έστω $f, g \in \mathbb{F}_q[x]$ πολυώνυμα, g μονικό και $f \neq 0$ τότε:*
$\sum_{g|f} M(g) = 1$ *αν* $\deg f = 0$ *ενώ*
$\sum_{g|f} M(g) = 0$ *αν* $\deg f \geq 1$.
Αντίστοιχα:
Έστω n, m φυσικοί αριθμοί,
Αν $n \geq 1$ τότε:
$\sum_{d|n} \mu(d) = 1$ *αν* $n = 1$ *ενώ*
$\sum_{d|n} \mu(d) = 0$ *αν* $n > 1$.

Απόδειξη. Έστω $\deg f \geq 1$ και $f = f_1^{p_1} \cdots f_k^{p_k}$.
Στο άθροισμα $\sum_{g|f} M(g)$ οι μόνοι μη μηδενικοί όροι είναι τα πολυώνυμα, στων οποίων την κανονική ανάλυση δεν υπάρχουν δυνάμεις.
Επομένως:

$$\sum_{g|f} M(g) = M(1)+M(f_1)+\cdots+M(f_k)+M(f_1f_2)+\cdots+M(f_{k-1}f_k)+\cdots+M(f_1\cdots f_k) =$$

$$1 + k(-1) + \frac{k!}{(k-2)!2!}(-1)^2 + \cdots + \frac{k!}{(k-j)!j!}(-1)^j + \cdots + \frac{k!}{k!}(-1)^k = (1-1)^k = 0$$

Αν $\deg f = 0$ τότε f, g σταθερά πολυώνυμα.
Για $f \neq 1$ έχουμε:

$$\sum_{g|f} M(g) = M(f) + \sum_{g|f, g\neq f} M(g) = 1 + 0 = 1$$

□

Θεώρημα 1.2 *Έστω $f, g \in \mathbb{F}_q[x]$ μη μηδενικά πολυώνυμα με μκδ(f, g)=1, τότε:*
$M(fg) = M(f)M(g)$
Όμοια,
Έστω n, m φυσικοί αριθμοί με, τότε:
$\mu(nm) = \mu(n)\mu(m)$

Απόδειξη. Έστω $f = f_1^{p_1} \cdots f_k^{p_k}, g = g_1^{a_1} \cdots g_l^{a_l}$
$M(fg) = M(f_1^{p_1} \cdots f_k^{p_k} g_1^{a_1} \cdots g_l^{a_l}) = (-1)^{k+l}$ αν $p_i = a_j = 1, \forall i = 1, .., k, j = 1, .., l$
ή $M(fg) = 0$ αν $\exists p_i \neq 1$ ή $s_j \neq 1$, $i = 1, .., k, j = 1, .., l$
και
$M(f)M(g) = 0$ αν $\exists p_i \neq 1$ ή $s_j \neq 1$, $i = 1, .., k, j = 1, .., l$
ή $M(f)M(g) = (-1)^k(-1)^l = (-1)^{k+l}$ αν $p_i = a_j = 1 \forall i = 1, .., k, j =, .., l$

□

1.2 Η συνάρτηση του *Euler*

Θα δούμε κάποια αποτελέσματα για τη συνάρτηση του *Euler* τόσο για τα πολυώνυμα όσο και για τους φυσικούς αριθμούς.
Θα περιορίσουμε όμως τις αποδείξεις μας μόνο στην περίπτωση των πολυωνύμων, καθότι για τους φυσικούς αριθμούς οι αποδείξεις είναι ανάλογες.
Έστω $f \in \mathbb{F}_q[x]$ μονικό ορίζουμε τότε $\Phi(f) = \sharp(\mathbb{F}_q[x]/f\mathbb{F}_q[x])^*$, $N(f) = \sharp(\mathbb{F}_q[x]/f\mathbb{F}_q[x]) = q^{\deg(f)}$ και θα αποδείξουμε:

Πρόταση 1.3 *Έστω $f, g \in \mathbb{F}_q[x]$ πολυώνυμα, τότε*
a) $\sum_{g|f} \Phi(g) = N(f)$

β) $\Phi(f) = N(f)\prod_{g|f}(1-\frac{1}{N(g)})$, όπου g μονικά ανάγωγα στο $\mathbb{F}_q[x]$ και $\deg(f) = n > 1$

Όμοια έστω $n \in \mathbb{N}$ τότε,
1) $\varphi(n) = n\prod_{p|n}(1-\frac{1}{p})$, όπου p πρώτος
2)$\sum_{d|n}\varphi(d) = n$

Θα δούμε όμως πρώτα ένα λήμμα το οποίο θα μας φανεί χρήσιμο στην απόδειξη του β).

Λήμμα 1.4 *Έστω $f, g \in \mathbb{F}_q[x]$ μονικά και $(f, g) = 1$, τότε $\Phi(fg) = \Phi(f)\Phi(g)$.*

Απόδειξη. Έστω $\Phi(f)=s$ και $\Phi(g) = t$. Ονομάζουμε $f_1, .., f_s$ και $g_1, .., g_t$, τα πολυώνυμα των οποίων το πλήθος ορίζουν οι συναρτήσεις $\Phi(f)$ και $\Phi(g)$ αντίστοιχα.
Έτσι:
$(f_i, f) = 1$ με $\deg(f_i) < \deg(f) \quad \forall i = 1, .., s$ και $(g_j, g) = 1$ με $\deg(g_j) < \deg(g)$ $\forall j = 1, .., t$
Λαμβάνουμε ένα $h \in \mathbb{F}_q[x]$ με $\deg(h) < \deg(fg)$ και $(fg, h) = 1$
Άρα $(f, h) = (g, h) = 1$
Συμπεραίνουμε λοιπόν ότι $h \equiv f_i \pmod f$ και $h \equiv g_i \pmod g$ για κάποιο μοναδικό ζεύγος (i, j), $1 \le i \le s, 1 \le j \le t$
Αντίστροφα:
Αν μας δωθεί ένα ζευγάρι (i, j), το κινέζικο θεώρημα υπολοίπων του $\mathbb{F}_q[x]$ μας δείχνει ότι:
$\exists! h \in \mathbb{F}_q[x]$ με $h \equiv f_i \pmod f, h \equiv g_i \pmod g$ και $\deg(h) < \deg(fg)$
Αυτό το h ικανοποιεί $(f, h) = (g, h) = 1$ αφού $(f_i, f) = 1$ και $(g_j, g) = 1$. Άρα $(fg, h) = 1$

Έστω τώρα $A = \{(i, j) : 1 \le i \le s, 1 \le j \le t\}$ και $B = \{h \in \mathbb{F}_q[x] : \deg(h) < \deg(fg), (fg, h) = 1\}$
Ορίζουμε τη συνάρτηση

$$\begin{aligned} \text{H: } A &\longrightarrow B \\ (i, j) &\longmapsto h \end{aligned}$$

Σύμφωνα με τα προηγούμενα, παρατηρούμε ότι η H είναι ένα προς ένα. Άρα $\sharp A = \sharp B$. Όμως $\sharp B = \Phi(fg)$ και $\sharp A = st$.
Τελικά $\Phi(fg) = st = \Phi(f)\Phi(g)$

□

Ας περάσουμε τώρα στην απόδειξη της πρότασης 1.3

Απόδειξη. Για το α) :
Έστω A= $\mathbb{F}_q[x]/f\mathbb{F}_q[x] = \{h \in \mathbb{F}_q[x] : \deg(h) < \deg(f)\}$
Κάνουμε μία διαμέριση του A σε ξένα σύνολα ως εξής:
Για κάθε μονικό πολυώνυμο g που διαιρεί το f ορίζουμε
$A_g = \{h \in \mathbb{F}_q[x] : (h, f) = g, \deg(h) < \deg(f)\}$ και έστω $\sharp A_g = \lambda(g)$.
Βλέπουμε ότι:
Αν $g_1, g_2 \in \mathbb{F}_q[x], g_1 \ne g_2$ διαιρέτες του f τότε $A_{g_1} \bigcap A_{g_2} = \varnothing$ και $\bigcup_{g|f} A_g = A$.
Επομένως $\sum_{g|f} \lambda(g) = N(f)$ (13).

Όμως $(h,f)=g \iff (\frac{h}{g},\frac{f}{g})=1$ και $\deg(h)<\deg(f) \iff \deg(\frac{h}{g})<\deg(\frac{f}{g})$
Θέτουμε $p=\frac{h}{g}$ και $B=\{p\in\mathbb{F}_q[x] : (p,\frac{f}{g})=1, \deg(p)<\deg(\frac{f}{g})\}$ και ορίζουμε τη συνάρτηση

$$\begin{array}{c} L : A_g \longrightarrow B \\ h \longmapsto p \end{array}$$

Για την L παρατηρούμε το εξής:
Έστω $p_1=p_2 \Longrightarrow \frac{h_1}{g}=\frac{h_2}{g} \Longrightarrow h_1=h_2$. Άρα η L είναι ένα προς ένα και φανερά είναι επι.
Συνεπώς $\lambda(g)=\Phi(\frac{f}{g})$ και έτσι η (13) γίνεται $\sum_{g|f}\Phi(\frac{f}{g})=N(f)$.
Αυτό όμως είναι ισοδύναμο με $\sum_{g|f}\Phi(g)=N(f)$ διότι καθώς το g 'τρέχει' σε όλους τους διαιρέτες του f το ίδιο γίνεται και με το $\frac{f}{g}$.

Αποδεικνύουμε τώρα το β):

Έστω $f={f_1}^{p_1}\cdots{f_k}^{p_k}$ η κανονική ανάλυση του f.
Τότε $\Phi(f)=\Phi({f_1}^{p_1}...{f_k}^{p_k})=\Phi({f_1}^{p_1})\cdots\Phi({f_k}^{p_k})$ (14)
Έστω τώρα ένα ανάγωγο πολυώνυμο $s\in\mathbb{F}_q[x], \deg(s)=m$ και $0<e\in\mathbb{N}$.
Τα πολυώνυμα $h\in\mathbb{F}_q[x]$ με $\deg(h)<\deg(s^e)=em, (h,s^e)\neq 1$ είναι ακριβώς αυτά τα οποία διαιρούνται απο το s.
Επομένως μπορούν να γραφούν στη μορφή $h=sg$, όπου $\deg(h)=\deg(sg)=\deg(s)+\deg(g) \Longrightarrow \deg(g)=\deg(h)-\deg(s)<\deg(s^e)-\deg(s)=em-m$.
Άρα υπάρχουν q^{em-m} διαφορετικές επιλογές για το g.
Έτσι οδηγούμαστε στο εξής αποτέλεσμα:
$\Phi(s^e)=q^{em}-q^{em-m}=q^{em}(1-q^{-m})$.
Οπότε η (14) παίρνει τη μορφή:

$$\Phi(f)=\Phi({f_1}^{p_1})\cdots\Phi({f_k}^{p_k})=q^{p_1\deg(f_1)}\cdots q^{p_k\deg(f_k)}(1-q^{-\deg(f_1)})..(1-q^{-\deg(f_k)})=$$

$$q^{p_1\deg(f_1)+\cdots+p_k\deg(f_k)}(1-\frac{1}{q^{\deg(f_1)}})\cdots(1-\frac{1}{q^{\deg(f_k)}})=q^{\deg(f_1^{p_1})+..+\deg(f_k^{p_k})}\prod_{g|f,g\alpha\nu\alpha\gamma\omega\gamma o}(1-\frac{1}{N(g)})=$$

$$q^{\deg(f)}\prod_{g|f,g\alpha\nu\alpha\gamma\omega\gamma o}(1-\frac{1}{N(g)})=N(f)\prod_{g|f}(1-\frac{1}{N(g)})$$

□

1.3 Η ομάδα των χαρακτήρων

Έστω G μία πεπερασμένη αβελιανή ομάδα τάξης $|G|$ με ταυτοτικό στοιχείο το 1_G
Θα ονομάζουμε χαρακτήρα χ της G, έναν ομομορφισμό απο την G στην πολλαπλασιαστική ομάδα $\mathbb{C}^*$ των μιγαδικών αριθμών με απόλυτη τιμή 1.
Δηλαδή,

$$\chi\colon G \longrightarrow \mathbb{C}^*$$
$$\chi(g_1g_2)=\chi(g_1)\chi(g_2)$$

Παρατηρούμε ότι:
$\chi(1_G)=\chi(1_G)\chi(1_G)\Longrightarrow\chi(1_G)=1$ και
$(\chi(\gamma))^{|G|} = \chi(\gamma^{|G|}) = \chi(1_G) = 1, \qquad \forall g \in G$. Επομένως οι τιμές του χ είναι όλες $|G|$-οστές ρίζες της μονάδας.

Επίσης:
$\chi(g)\chi(g^{-1})=\chi(gg^{-1})=\chi(1_G)=1 \Longrightarrow$
$\chi(g^{-1})=(\chi(g))^{-1}:= \overline{\chi(g)}, \qquad \forall g \in G$
Τον χαρακτήρα $\overline{\chi}$ θα τον ονομάζουμε συζυγή χαρακτήρα του χ.
Μέσα στο σύνολο των χαρακτήρων της G περιέχεται ο τετριμμένος χαρακτήρας χ_0 όπου:
$\chi_0(g)=1\ , \qquad \forall g \in G$
Οι υπόλοιποι χαρακτήρες ονομάζονται μη τετριμμένοι.

Αν μας δωθούν πεπερασμένοι το πλήθος χαρακτήρες $\chi_1,..,\chi_n$ της G, μπορούμε να ορίσουμε το γινόμενο $\chi_1\cdots\chi_n$ θέτοντας:
$(\chi_1\cdots\chi_n)(g)= \chi_1(g)\cdots\chi_n(g), \qquad \forall g \in G$
Θα συμβολίζουμε το σύνολο των χαρακτήρων μιας πεπερασμένης ομάδας G με $\hat{G}$.
Απο όσα προαναφέρθηκαν , είναι φανερό οτι η $\hat{G}$ είναι μια αβελιανή ομάδα.

Παράδειγμα 1.1 Έστω G μια πεπερασμένη κυκλική ομάδα τάξης n και g ένας γεννήτορας της G.
Για $j \in \mathbb{Z}, 0 \leq j \leq n-1$ η συνάρτηση

$$\chi_j(g^k) = e^{2\pi ijk/n}, k = 0, 1, ..., n-1$$

ορίζει έναν χαρακτήρα της G. Αντίστροφα, αν χ είναι ένας χαρακτήρας της G, τότε το $\chi(g)$ θα πρέπει να είναι n-οστή ρίζα της μονάδας, δηλαδή $\chi(g)=e^{2\pi ij/n}$ για κάποιο $j, 0 \leq j \leq n-1$.
Άρα $\chi=\chi_j$. Επομένως η $\hat{G}$ αποτελείται ακριβώς απο τους χαρακτήρες $\chi_1,\chi_2,\cdots,\chi_{n-1}$

Θεώρημα 1.5 *Έστω H υπο-ομάδα της πεπερασμένης αβελιανής ομάδας G και έστω ψ χαρακτήρας της H.Τότε ο ψ μπορεί να επεκταθεί σε ένα χαρακτήρα της G. Δηλαδή,*
$\exists\ \chi \in \hat{G}$ *με* $\chi(h)=\psi(h), \forall h \in H$

Απόδειξη. Έστω $H \subsetneq G$. Επιλέγουμε $a \in G$ με $a \notin H$.
Έστω H_1 η υποομάδα της G που γεννάται απο την H και το a. Έστω m ο μικρότερος

θετικός ακέραιος τ.ω. $a^m \in H$. Τότε,
$\forall g \in H_1$: $g = a^j h$, $0 \leq j < m$ και $h \in H$.
Ορίζουμε τότε μια συνάρτηση ψ_1 που λαμβάνει τιμές της H_1 ως εξής:
$\psi_1(g) = \omega^j \psi(h)$, $\omega \in \mathbb{C}$ και $\omega^m = \psi(a^m)$

Ελέγχουμε οτι ψ_1 είναι χαρακτήρας:
Έστω $g_1 = a^k h_1, \qquad 0 \leq k < m, h_1 \in H$
Αν $j + k < m$ τότε $\psi_1(gg_1) = \omega^{j+k}\psi(hh_1) = \psi_1(g)\psi_1(g_1)$
Αν $j + k \geq m$ τότε $gg_1 = a^{j+k-m}(a^m hh_1)$ και
$\psi_1(gg_1) = \omega^{j+k-m}\psi(a^m hh_1) = \omega^{j+k}\psi(hh_1) = \psi_1(g)\psi_1(g_1)$

Φανερά $\psi_1(h) = \psi(h), \qquad \forall h \in H$.
Αν $H_1 = G$ τότε τελειώσαμε.
Διαφορετικά, εκτελόντας την ίδια διαδικασία και μετά απο πεπερασμένο πλήθος βημάτων λαμβάνουμε μια επέκταση του ψ στην G

□

Λήμμα 1.6 *Για κάθε δύο διαφορετικά στοιχεία $g_1, g_2 \in G$ υπάρχει χαρακτήρας χ της G με $\chi(g_1) \neq \chi(g_2)$*

Απόδειξη. Θα δείξουμε οτι για $h = g_1 {g_2}^{-1} \neq 1_G$, $\exists\ \chi \in \hat{G}$ με $\chi(h) \neq 1$
Αυτό όμως προκύπτει άμεσα απ'το παράδειγμα 1.1 και το θεώρημα 1.5 αν θέσουμε H να είναι η κυκλική υποομάδα της G που γεννάται απ'το h.
Άρα $1 \neq \chi(h) = \chi(g_1 {g_2}^{-1}) = \chi(g_1)\chi({g_2}^{-1}) = \chi(g_1)\chi(g_2)^{-1}$
$\Longrightarrow \chi(g_1) \neq \chi(g_2)$

□

Θεώρημα 1.7 *Αν ο χαρακτήρας χ μιας πεπερασμένης αβελιανής ομάδας G είναι μη τετριμμένος τότε:*

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

Αν $g \in G$ με $g \neq 1$ τότε:

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

Απόδειξη. Εφ'οσον ο χ είναι μη-τετριμμένος $\exists h \in G$ με $\chi(h) \neq 1$.

Έτσι $\chi(h)\sum_{g \in G}\chi(g) = \sum_{g \in G}\chi(hg) = \sum_{g \in G}\chi(g)$

διότι καθώς το g 'τρέχει' στην ομάδα G, το ίδιο γίνεται και με το hg.
Επομένως
$(\chi(h)\text{-}1)\sum_{g \in G}\chi(g) = 0 \Longrightarrow \sum_{g \in G}\chi(g) = 0 \qquad (1)$

Για το δεύτερο μέρος:
Ορίζουμε τη συνάρτηση $\hat{g}$ με $\hat{g}(\chi) = \chi(g)$, $\chi \in \hat{G}$

Παρατηρούμε οτι ο $\hat{g}$ είναι χαρακτήρας της πεπερασμένης αβελιανής ομάδας $\hat{G}$
Αυτός ο χαρακτήρας είναι μη-τετριμμένος, αφού απο το λήμμα 1.6 γνωρίζουμε πως υπάρχει χαρακτήρας $\chi \in \hat{G}$, $\chi(g) \neq 1_G$

Επομένως απο την (1) βλέπουμε οτι:
$\sum_{\chi\in\hat{G}}\chi(g)=\sum_{\chi\in\hat{G}}\hat{g}(\chi)= 0$

□

Παρατηρούμε οτι:
αν $\chi=\chi_0$ τότε $\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi_0(g) = |G|$ και
αν $g = 1_G$ τότε $\sum_{\chi\in\hat{G}}\chi(g) = \sum_{\chi\in\hat{G}} 1_G = |\hat{G}|$

Θεώρημα 1.8 *Το πλήθος των χαρακτήρων μιας πεπερασμένης αβελιανής ομάδας ισούται με $|G|$.*

Απόδειξη. $|\hat{G}| = \sum_{g\in G}\sum_{\chi\in\hat{G}}\chi(g) = \sum_{\chi\in\hat{G}}\sum_{g\in G}\chi(g) = |G|$

□

Θεώρημα 1.9 *Μια πεπερασμένη αβελιανή ομάδα G είναι ισόμορφη με την ομάδα $\hat{G}$ των χαρακτήρων της.*

Απόδειξη. Γνωρίζουμε οτι:
$G = C_1 \times \cdots \times C_n$, όπου $C_1, .., C_n$ κυκλικές ομάδες.
Έστω τώρα $C =< a >$ και $|C| = m$
Ορίζουμε

$$\begin{aligned} \chi_{a^k} : C &\longrightarrow \mathbb{C}^* \\ a &\longmapsto e^{\frac{2\pi i}{m}k} \end{aligned} \qquad , 0 \leq k \leq m-1$$

Βλέπουμε οτι, αν

$$\begin{aligned} \varphi\colon C &\longrightarrow \hat{C} \\ a^k &\longmapsto \chi_{a^k} \end{aligned}$$

μια συνάρτηση, τότε:
1) Η φ είναι ομομορφισμός:
$\chi_{a^k a^n}(a) = e^{\frac{2\pi i}{m}(k+n)} = e^{\frac{2\pi i}{m}k}e^{\frac{2\pi i}{m}n} = \chi_{a^k}\chi_{a^n}(a)$
2) Η φ είναι ένα προς ένα:
Αν $\chi_{a^k}(a) = \chi_{a^n}(a) \Longrightarrow e^{\frac{2\pi i}{m}k} = e^{\frac{2\pi i}{m}n} \Longrightarrow k \equiv n \pmod m \Longrightarrow a^k = a^n$
3) Η φ είναι φανερά επί.
Επομένως η φ είναι ισομορφισμός.

Αν πάρουμε $G_1 = C_1 \times C_2$ με $C_1 =< a_1 >, C_2 =< a_2 >$ μπορούμε να ορίσουμε τοτε:

$$\chi_{a_1{}^{k_1}a_2{}^{k_2}} : G_1 \longrightarrow \mathbb{C}^*$$

$\chi_{{a_1}^{k_1}{a_2}^{k_2}}(a_1a_2) := \chi_{{a_1}^{k_1}}(a_1)\chi_{{a_2}^{k_2}}(a_2)$ και

$$\begin{array}{c}\varphi_1 : G_1 \longrightarrow \hat{G}_1 = C_1 \hat{\times} C_2 \\ {a_1}^{k_1}{a_2}^{k_2} \longmapsto \chi_{a_1^{k_1}}\chi_{a_2^{k_2}}\end{array}$$

Παρατηρούμε τώρα οτι:
1) Η φ_1 είναι φανερά επί.
2) Η φ_1 είναι ένα προς ένα:
Αν $\chi_{{a_1}^{k_1}{a_2}^{k_2}} = \chi_{{a_1}^{l_1}{a_2}^{l_2}} \Longrightarrow$
$\chi_{{a_1}^{k_1}{a_2}^{k_2}}(x) = \chi_{{a_1}^{l_1}{a_2}^{l_2}}(x), \quad \forall x \in C_{m_1} \Longrightarrow \chi_{{a_1}^{k_1}}(x) = \chi_{{a_1}^{l_1}}(x), \quad \forall x \in C_{m_1} \Longrightarrow$
$\chi_{{a_1}^{k_1}} = \chi_{{a_1}^{l_1}} \quad (2)$
Αφού $C_{m_1} \simeq \hat{C_{m_1}} \quad (2) \Longrightarrow {a_1}^{k_1} = {a_1}^{l_1}$
Ομοίως:
$\chi_{{a_1}^{k_1}{a_2}^{k_2}} = \chi_{{a_1}^{l_1}{a_2}^{l_2}} \Longrightarrow$
$\chi_{{a_1}^{k_1}{a_2}^{k_2}}(y) = \chi_{{a_1}^{l_1}{a_2}^{l_2}}(y), \quad \forall y \in C_{m_2} \Longrightarrow \chi_{{a_1}^{k_1}}(y) = \chi_{{a_1}^{l_1}}(y), \quad \forall y \in C_{m_2} \Longrightarrow$
$chi_{{a_2}^{k_2}} = \chi_{{a_2}^{l_2}} \quad (3)$
Αφού $C_{m_2} \simeq \hat{C_{m_2}} \quad (3) \Longrightarrow {a_2}^{k_2} = {a_2}^{l_2}$
3) Η φ_1 είναι ομομορφισμός:
$\chi_{{a_1}^{k_1}{a_2}^{k_2}}\chi_{{a_1}^{l_1}{a_2}^{l_2}} = \chi_{{a_1}^{k_1}}\chi_{{a_2}^{k_2}}\chi_{{a_1}^{l_1}}\chi_{{a_2}^{l_2}} = \chi_{{a_1}^{k_1}{a_1}^{l_1}}\chi_{{a_2}^{k_2}{a_2}^{l_2}} := \chi_{{a_1}^{k_1}{a_2}^{k_2}{a_1}^{l_1}{a_2}^{l_2}}$
Άρα φ_1 ισομορφισμός.

Επαγωγικά δείχνουμε οτι:
Αν $G = C_{m_1} \times \cdots \times C_{m_n}$ τότε $G \simeq \hat{G} = C_{m_1} \times \hat{\cdots} \times C_{m_n}$

□

Θεώρημα 1.10 *Έστω H υποομάδα μιας πεπερασμένης αβελιανής ομάδας G. Το σύνολο $A = \{\chi \in \hat{G} : \quad \chi(h) = 1, \quad \forall h \in H\}$ είναι υποομάδα της $\hat{G}$ με τάξη $\frac{|G|}{|H|}$.*

Απόδειξη. Φανερά το Α είναι υποομάδα της $\hat{G}$.
Έστω τώρα

$$\begin{array}{c}\vartheta\colon A \longrightarrow \hat{G/H} \\ \chi \longmapsto \bar{\chi}\end{array}$$

όπου $\bar{\chi}(aH) = \chi(a)$.
Η ϑ είναι καλώς ορισμένη καθ'οτι $\chi|_H$=1 και ο $\bar{\chi}$ είναι χαρακτήρας αφού:
Αν $aH = bH$ τότε $a = bh, \quad h \in H$.
Επομένως $\bar{\chi}(aH) = \chi(a) = \chi(bh) = \chi(b) = \bar{\chi}(bH)$.
Επίσης $\overline{\chi_1\chi_2}(aH) = \chi_1\chi_2(a) = \chi_1(a)\chi_2(a) = \bar{\chi_1}(aH)\bar{\chi_2}(aH)$
Άρα $\bar{\chi}$ ομομορφισμός.
Για τη ϑ παρατηρούμε τα εξής:
Αν $\bar{\chi_1} = \bar{\chi_2} \Longleftrightarrow \bar{\chi_1}(aH) = \bar{\chi_2}(aH) \Longleftrightarrow \chi_1(a) = \chi_2(a) \Longleftrightarrow \chi_1 = \chi_2$
Άρα η ϑ είναι ένα προς ένα.
Αν μ είναι ένας χαρακτήρας της G/H τότε ορίζουμε $\chi(g)$=μ(gH) και $\chi(h)$=1 $\quad \forall h \in H$.
Άρα $\chi \in A$

Καταλήγουμε λοιπόν οτι η ϑ είναι επί και αφού είναι και ένα προς ένα τότε υπάρχει αντιστοιχεία της A με την ομάδα των χαρακτήρων $G\hat{/}H$.
Επομένως η τάξη του A είναι ίση με την τάξη της $G\hat{/}H$ η οποία όπως έχουμε δεί είναι $|G|/|H|$

□

Έστω q πρώτος και $m \in \mathbb{Z}$. Σ'ενα πεπερασμένο σώμα $\mathbb{F}_{q^m}$, υπάρχουν δύο πεπερασμένες αβελιανές ομάδες, η προσθετική ομάδα και η πολλαπλασιαστική ομάδα του σώματος.Έτσι διαφοροποιούμε τους χαρακτήρες σε προσθετικούς και πολλαπλασιαστικούς αντίστοιχα.
Έστω η απεικόνιση του ίχνους

$$\begin{aligned} Tr : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_q \\ a &\longmapsto a + a^q + \cdots + a^{q^{m-1}} \end{aligned}$$

Η συνάρτηση χ_1 για την οποία $\chi_1(c) = e^{2\pi i Tr(c)/p}, \forall c \in \mathbb{F}_{q^m}$ είναι ένας χαρακτήρας της προσθετικής ομάδας του $\mathbb{F}_{q^m}$,αφού για $c_1, c_2 \in \mathbb{F}_{q^m}$ έχουμε $\chi_1(c_1 + c_2) = \chi_1(c_1)\chi_1(c_2)$ (αρκεί να δούμε ότι $Tr(c_1 + c_2) = Tr(c_1) + Tr(c_2)$).

Ορίζοντας $\chi_b(c) = \chi_1(bc), \quad \forall c \in \mathbb{F}_q$ για $b \in \mathbb{F}_q^m$, είναι φανερό ότι ο χ_b είναι προσθετικός χαρακτήρας Θέτοντας $b = 0$ στο παραπάνω θεώρημα, προκύπτει ο τετριμμένος χαρακτήρας χ_0

1.3.1 Αθροίσματα *Gauss*

Έστω χ χαρακτήρας της προσθετικής και ψ χαρακτήρας της πολλαπλασιαστικής ομάδας του $\mathbb{F}_{q^m}$. Μπορούμε να επεκτείνουμε τους χαρακτήρες της $\mathbb{F}_{q^m}^*$ σε ολόκληρο το $\mathbb{F}_{q^m}$ θέτοντας $\psi(0)=0$ για $\psi \neq \psi_0$ και $\psi_0(0)=1$.
Το άθροισμα *Gauss* ορίζεται τότε ως εξής:

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_{q^m}} \psi(c)\chi(c)$$

Βλέπουμε εύκολα ότι:
Αν $\psi = \psi_0, \chi = \chi_0$ τότε:
$G(\psi, \chi) = \sum_{c \in \mathbb{F}_{q^m}} \psi_0(c)\chi_0(c) = \sum_{c \in \mathbb{F}_{q^m}} 1 = q^m$
Αν $\psi = \psi_0, \chi \neq \chi_0$ τότε:
$G(\psi, \chi) = \sum_{c \in \mathbb{F}_{q^m}} \psi_0(c)\chi(c) = \sum_{c \in \mathbb{F}_{q^m}} \chi(c) = 0$
Αν $\psi \neq \psi_0, \chi = \chi_0$ τότε:
$G(\psi, \chi) = \sum_{c \in \mathbb{F}_{q^m}} \psi(c)\chi_0(c) = \sum_{c \in \mathbb{F}_{q^m}} \psi(c) = \sum_{c \in \mathbb{F}_{q^m}} \psi(c) = 0$

Τι γίνεται όταν $\psi \neq \psi_0, \chi \neq \chi_0$
Θα αποδείξουμε οτι σε αυτή τη περίπτωση $|G(\psi, \chi)| = q^{m/2}$
Παρατηρούμε το εξής:

$$|G(\psi, \chi)|^2 = \overline{G(\psi, \chi)}G(\psi, \chi) = \sum_{c \in \mathbb{F}_{q^m}} \sum_{c_1 \in \mathbb{F}_{q^m}} \overline{\psi(c)\chi(c)}\psi(c_1)\chi(c_1) = \sum_{c \in \mathbb{F}_{q^m}} \sum_{c_1 \in \mathbb{F}_{q^m}} \psi(c^{-1}c_1)\chi(c_1 - c)$$

Θέτουμε $c^{-1}c_1 = d$.Τότε:

$$|G(\psi,\chi)|^2 = \sum_{c\in\mathbb{F}_{q^m}} \sum_{d\in\mathbb{F}_{q^m}} \psi(d)\chi(c(d-1)) = \sum_{d\in\mathbb{F}_{q^m}} \psi(d) \sum_{c\in\mathbb{F}_{q^m}} \chi(c(d-1))$$

Το εσωτερικό άθροισμα έχει τιμή ίση με q^m αν $d = 1$ και 0 αν $d \neq 1$, όπως προκύπτει απο το Θεώρημα 1.7
Επομένως $|G(\psi,\chi)|^2 = \psi(1)q^m = q^m$.

Κεφάλαιο 2

Η κυκλική δομή των πεπερασμένων σωμάτων

Έστω $q > 1$ μια δύναμη πρώτου αριθμού, συμβολίζουμε την αλγεβρική θήκη του $\mathbb{F}_q$ με $\overline{\mathbb{F}_q}$ και ορίζουμε τον αυτομορφισμό του $Frobenius$:

$$\sigma : \overline{\mathbb{F}_q} \longrightarrow \overline{\mathbb{F}_q}$$

$$a \longmapsto a^q \qquad , \forall a \in \overline{\mathbb{F}_q}$$

Έστω τώρα $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{F}_q[x], f_i \in \overline{\mathbb{F}_q}$ και $a \in \overline{\mathbb{F}_q}$, ορίζουμε:

$$f \circ a = \sum_{i=0}^{n} f_i \sigma^i(a)$$

Θα δείξουμε οτι η προσθετική ομάδα της $\overline{\mathbb{F}_q}$ εφοδιασμένη με την εξωτερική πράξη $f \circ a$ είναι ένα $\mathbb{F}_q[x] - module$.
Για το σκοπό αυτό όμως θα χρειαστούμε τα εξής 2 λήμματα:

Λήμμα 2.1 *Ο $\sigma^i, i \in \mathbb{N}$ είναι αυτομορφισμός και σταθεροποιεί το $\mathbb{F}_q$.*

Απόδειξη. Ο σ είναι αυτομορφισμός, άρα και ο $\sigma \circ \sigma = \sigma^2$ είναι αυτομορφισμός. Επαγωγικά δείχνει κανείς ότι σ^i είναι αυτομορφισμός. Ακόμη παρατηρούμε ότι για $\alpha \in \mathbb{F}_q$, $\sigma(\alpha) = \alpha^q = \alpha$ και επαγωγικά, $\sigma^i(\alpha) = \sigma^{i-1}(\sigma(\alpha)) = \sigma^{i-1}(\alpha) = \alpha$.

□

Με τη βοήθεια του παραπάνω αποτελέσματος βλέπουμε τώρα το εξής:

$$(a_1 + a_2 + \cdots + a_m)^{q^i} = \sigma^i(a_1 + a_2 + \cdots + a_m) = \sigma^i(a_1 + (a_2 + \cdots + a_m)) =$$
$$\sigma^i(a_1) + \sigma^i(a_2 + (a_3 + \cdots + a_m)) = \cdots = \sigma^i(a_1) + \cdots + \sigma^i(a_m) =$$
$$a_1{}^{q^i} + \cdots + a_m{}^{q^i} \qquad (5)$$

Λήμμα 2.2 *Έστω* $f_j, g_i \in \overline{\mathbb{F}_q}, \quad j = 0, .., n, i = 0, .., m$ *τότε:*

$$\sum_{j=0}^{n} f_j \sum_{i=0}^{m} g_i = \sum_{s=0}^{n+m} (\sum_{t=0}^{s} f_t g_{s-t})$$

Απόδειξη.

$$\sum_{j=0}^{n} f_j \sum_{i=0}^{m} g_i = \sum_{j=0}^{n} f_j (g_0 + \cdots + g_m) = \sum_{j=0}^{n} f_j g_0 + \cdots + \sum_{j=0}^{n} f_j g_m (6)$$

Κάνουμε τη σύμβαση $f_j = 0$ για $j > n$ και $g_i = 0$ για $i > m$, έτσι:

$$(6) = \sum_{j=0}^{n+m} f_j g_0 + \cdots + \sum_{j=0}^{n+m} f_j g_m = \sum_{j=0}^{n+m} f_j g_0 + \cdots + \sum_{j=0}^{n+m} f_j g_{n+m} =$$

$$(f_0 g_0 + f_1 g_0 + \cdots + f_{n+m} g_0) + \cdots + (f_0 g_{n+m} + f_1 g_{n+m} + \cdots + f_{n+m} g_{n+m} (7)$$

$$\sum_{s=0}^{n+m} (\sum_{t=0}^{s} f_t g_{s-t}) = f_0 g_0 + (\sum_{t=0}^{1} f_t g_{1-t}) + \cdots + (\sum_{t=0}^{1} f_t g_{n+m-t}) =$$

$$f_0 g_0 + (f_0 g_1 + f_1 g_0) + (f_0 g_2 + f_1 g_1 + f_2 g_0) + \cdots + (f_0 g_{n+m} + f_1 g_{n+m-1} + \cdots + f_{n+m} g_0) (8)$$

Παρατηρώντας την ισότητα των σχέσεων (7) και (8) καταλήγουμε στο ζητούμενο.

□

Είμαστε λοιπόν τώρα σε θέση να δείξουμε οτι οτι η προσθετική ομάδα της $\overline{\mathbb{F}_q}$ εφοδιασμένη με την εξωτερική πράξη $f \circ a$, ικανοποιεί τις ιδιότητες ενός *module*. Έχουμε λοιπόν:

1) $f_i \in \overline{\mathbb{F}_q}$ και $\sigma^i(a) \in \overline{\mathbb{F}_q}, \quad \forall i = 0, .., n.$ Άρα $f \circ a \in \overline{\mathbb{F}_q}$.

2)

$$f \circ (a + b) = \sum_{i=0}^{n} f_i \sigma^i (a + b) = \sum_{i=0}^{n} f_i (\sigma^i (a) + \sigma^i (b)) = \sum_{i=0}^{n} (f_i \sigma^i (a) + f_i \sigma^i (b)) =$$

$$\sum_{i=0}^{n} f_i \sigma^i (a) + \sum_{i=0}^{n} f_i \sigma^i (b) = f \circ a + f \circ b.$$

$3) g = \sum_{i=0}^{m} g_i x^i$.Έστω χωρίς περιορισμό της γενικότητας οτι $max(m, n) = n$, με τη σύμβαση $g_i = 0$ για $i = m + 1, .., n$ παίρνουμε $g = \sum_{i=0}^{n} g_i x^i$ και έτσι έχουμε:

$$(f + g) \circ a = \sum_{i=0}^{max(m,n)} (f_i + g_i) \sigma^i (a) = \sum_{i=0}^{n} (f_i \sigma^i (a) + g_i \sigma^i (a)) =$$

$$\sum_{i=0}^{n} f_i\sigma^i(a) + \sum_{i=0}^{n} g_i\sigma^i(a) = f \circ a + g \circ a$$

4)Κάνουμε τη σύμβαση $f_j = 0$ για $j > n$ και $g_i = 0$ για $i > m$, συνεπώς:

$$(fg) \circ a = (\sum_{i=0}^{n+m}(\sum_{j=0}^{i} f_j g_{i-j})x^i) \circ a = \sum_{i=0}^{n+m}(\sum_{j=0}^{i} f_j g_{i-j})\sigma^i(a)$$

.

$$f \circ (g \circ a) = f \circ (\sum_{i=0}^{m} g_i\sigma^i(a)) = \sum_{j=0}^{n} f_j\sigma^j(\sum_{i=0}^{m} g_i\sigma^i(a)) =$$

απο σχέση (5)

$$\sum_{j=0}^{n} f_j \sum_{i=0}^{m} \sigma^j(g_i\sigma^i(a)) = \sum_{j=0}^{n} f_j \sum_{i=0}^{m} {g_i}^{q^j}(a^{q^i})^{q^j} = \sum_{j=0}^{n} f_j \sum_{i=0}^{m} {g_i}^{q^j} a^{q^{i+j}} =$$

(απο λήμμα 2.1)

$$\sum_{j=0}^{n} f_j \sum_{i=0}^{m} g_i a^{q^{i+j}} =$$

(απο λήμμα 2.2)

$$\sum_{s=0}^{n+m}(\sum_{t=0}^{s} f_t g_{s-t})\sigma^s(a)$$

Στη συνέχεια θα δούμε την αντιστοιχεία μεταξύ γνωστών ιδιοτήτων της πολλαπλασιαστικής ομάδας της $\overline{\mathbb{F}_q}$ με την προσθετική ομάδα της $\overline{\mathbb{F}_q}$ όταν την βλέπουμε ως $\mathbb{F}_q[x] - module$
Για την πολλαπλασιαστική ομάδα λοιπόν:
Έστω $m \in \mathbb{N}$ και $\mathbb{F}_{q^m}$ το μοναδικό υπόσωμα της $\overline{\mathbb{F}_q}$, τάξης q^m.Για $0 \neq a \in \overline{\mathbb{F}_q}$ έχουμε:

$$a \in \mathbb{F}_{q^m} \iff \sigma^m(a) = a^{q^m} = a \iff a^{q^m-1} = 1$$

Αυτό μας δείχνει οτι η πολλαπλασιαστική τάξη του a (την οποία θα συμβολίζουμε με $ord(a)$),είναι πεπερασμένη και πρώτη προς το $q \quad \forall 0 \neq a \in \overline{\mathbb{F}_q}$ και ισχύει οτι:

$$a \in \mathbb{F}_{q^m} \iff ord(a)|q^m - 1 \iff q^m - 1 \equiv 0 \pmod{ord(a)}$$

Θα συμβολίζουμε το βαθμό του ανάγωγου πολυωνύμου ενός στοιχείου $a \in \overline{\mathbb{F}_q}$ πάνω απ΄το $\mathbb{F}_q$ με $\deg(a)$.
Σύμφωνα με τα προηγούμενα βλέπουμε ότι:

Ο $\deg(a)$ είναι το μικρότερο m ώστε για $0 \neq a \in \mathbb{F}_q[x]/p_a = \mathbb{F}_{q^{\deg(a)}} = \mathbb{F}_{q^m}, \quad p_a = min(a, \mathbb{F}_q)$,τότε

$$q^m \equiv 1 \pmod{ord(a)} \quad (9)$$

Μπορούμε λοιπόν τώρα να δείξουμε οτι:
Αν $0 \neq a \in \overline{\mathbb{F}_q}, ord(a) = n$, τότε $\deg(a)$ είναι ίσο με την πολλαπλασιαστική τάξη του $(q \pmod n)$ στην ομάδα $(\mathbb{Z}/nZ)^*$.
Αυτό προκύπτει αν παρατηρήσουμε οτι η τάξη του $(q \pmod n) = q+(n)$ είναι το μικρότερο $s \in \mathbb{N}$ τέτοιο ώστε:
$(q+(n))^s = 1+(n) \iff q^s+(n) = 1+(n) \iff q^s \equiv 1 \pmod n$
Απο (9) συμπεραίνουμε οτι $s = m$ αφου $s \leq m$ (ως ελάχιστο) και $s \geq m$ (ως ελάχιστο)

Ας δούμε τώρα τα αντίστοιχα αποτελέσματα για τη προσθετική ομάδα της $\overline{\mathbb{F}_q}$.

Έστω $a \in \mathbb{F}_q^m \iff \sigma^m(a) = a$ επομένως:
$(X^m-1) \circ a = \sigma^m(a) - \sigma^0(a) = a^{q^m} - a^{q^0} = a - a = 0, \quad \forall a \in \overline{\mathbb{F}_q}$ (10)

Ας κοιτάξουμε το εξής σύνολο:

$$I_a = \{f \in \mathbb{F}_q[x] : f \circ a = 0\}$$

1) Αν $f \in I_a$ και $g \in \mathbb{F}_q[x]$ τότε:
$(fg) \circ a = (gf) \circ a = g \circ (f \circ a) = g \circ 0 = 0 \Longrightarrow gf, fg \in I_a$
2) Α $f, g \in I_a$ τότε:
$(f-g) \circ a = f \circ a - g \circ a = 0 \Longrightarrow f - g \in I_a$

Απο 1) και 2) βλέπουμε λοιπόν οτι I_a είναι ιδεώδες του $\mathbb{F}_q[x]$ και εφ'οσον το $\mathbb{F}_q[x]$ είναι ευκλείδειος δακτύλιος επάγουμε οτι το I_a είναι κύριο και έτσι $I_a =< f >$.Απο (10) παρατηρούμε οτι αυτο το f είναι διαιρέτης του $X^m - 1$ και $f \neq 1$.
Θα συμβολίζουμε με $Ord(a)$ το μοναδικό μονικό πολυώνυμο $f \in \mathbb{F}_q[x]$ το οποίο γεννάει αυτό το ιδεώδες.Απο (10) έχουμε:

$$a \in \mathbb{F}_q^m \iff Ord(a) | X^m - 1$$

και αρα $Ord(a)$ είναι πρώτο προς το X.

Κατάναλογία με την πολλαπλασιαστική ομάδα δείχνουμε ότι:
Αν $a \in \overline{\mathbb{F}_q}$ και $Ord(a) = f$ τότε ο $\deg(a)$ είναι ίσος με την πολλαπλασιαστική τάξη του $(X \pmod f)$ στην ομάδα $(\mathbb{F}_q[x]/f\mathbb{F}_q[x])^*$.

Η τάξη του $X \pmod f = X + (f)$ είναι ο μικρότερος $l \in \mathbb{N}$ τέτοιος ώστε:
$(X+(f))^l = 1+(f) \iff X^l+(f) = 1+(f) \iff X^l \equiv 1 \pmod f$.
Άρα $(X^l-1) \circ a = (1-1) \circ a = 0 \circ a = 0 (11)$ και $(X^l-1) \circ a = a^{q^l} - a (12)$
Απο (11),(12) βλέπουμε πως το l είναι ο μικρότερος θετικός ακέραιος ώστε $a^{q^l} = a$.
Όμως αυτός είναι το $\deg(a)$.Άρα $l = \deg(a)$.

Στη συνέχεια θα μελετήσουμε, κάνοντας χρήση της συνάρτησης Φ του $Euler$, κάποια αποτελέσματα για τη προσθετική ομάδα της $\overline{\mathbb{F}_q}$ ακριβώς όμοια με αυτά της πολλαπλασιαστικής.
Ας κοιτάξουμε εν συντομία τι μας είναι γνωστό για την $\overline{\mathbb{F}_q}^*$:
Γνωρίζουμε ότι $\varphi(n)=\sharp\{a \in \overline{\mathbb{F}_q}^* : ord(a) = n, 1 < n \in \mathbb{N}, (n,q) = 1\}$.
Έτσι για $n = q^m - 1$, βλέπουμε ότι στοιχεία $a \in \overline{\mathbb{F}_{q^m}}^*$ με $ord(a) = n$ υπάρχουν (το πλήθος τους είναι ίσο με $\varphi(q^m - 1)$) και είναι ακριβώς οι πρωταρχικές ρίζες του $\mathbb{F}_{q^m}$.

Για την προσθετική ομάδα τώρα:
Έστω ένα πολυώνυμο $f = \sum_{i=0}^{n} b_i X^i \in \mathbb{F}_q[x]$, ορίζουμε τότε:

$$f^* = \sum_{i=0}^{n} b_i X^{q^i}$$

Φανερά, $f^*(a) = \sum_{i=0}^{n} b_i a^{q^i} = f \circ a \quad \forall a \in \overline{\mathbb{F}_q}$
Επομένως το πλήθος των $a \in \overline{\mathbb{F}_q}$ με $Ord(a)|f$ είναι ίσο με το πλήθος των διαφορετικών ριζών του f^* αφού $Ord(a)|f \iff f \circ a = 0$.

Το πολυώνυμο f^* έχει το πολύ $q^{\deg(f)}$ ρίζες και βλέπουμε οτι:
Όταν $(f, X) = 1$ τότε $\frac{df^*}{dX} = b_0 \neq 0 \Longrightarrow (f^*, (f^*)') = 1$.
Συνεπώς όλες οι ρίζες του f^* είναι απλές.
Συμπεραίνουμε λοιπόν οτι το f^* έχει ακριβώς $q^{\deg(f)}$ ρίζες.

Ορίζουμε για $f|X^n - 1$:
$A_f = \{a \in \overline{\mathbb{F}_q} : Ord(a) = f\}$
Βλέπουμε οτι:
$a \in A_f \Longrightarrow f \circ a = 0 \Longrightarrow (X^n - 1) \circ a = 0 \Longrightarrow a^{q^n} = a \Longrightarrow a \in \mathbb{F}_q^n$
και αφού $A_{g_1} \bigcap A_{g_2} = \varnothing$ για $g_1 \neq g_2$, έχουμε:
$\sum_{g/f} \sharp A_g = \sharp \bigcup_{g/f} A_g = \sharp\{a \in \mathbb{F}_{q^n} : Ord(a)|f\} = N(f)$

Θεώρημα 2.3 $\sharp A_f = \Phi(f)$

Απόδειξη. Αν $f|X^n - 1$ και $\deg(f) = 1$ τότε:

$$q = q^{\deg(f)} = \sum_{g|f} \sharp A_g = \sharp A_1 + \sharp A_f = 1 + \sharp A_f \Longrightarrow \sharp A_f = q - 1 = \Phi(f)$$

Υποθέτω οτι για $f|X^n - 1$ με $\deg(f) \leq k - 1$ ισχύει.
Έστω $f|X^n - 1$ και $\deg(f) = k$, τότε:

$$N(f) = \sum_{g|f} \sharp A_g = \sum_{g|f, \deg(g) < \deg(f)} \sharp A_g + \sharp A_f = \sum_{g|f, \deg(g) < k} \Phi(g) + \sharp A_f$$

Όμως

$$N(f) = \sum_{g|f, \deg(g) < k} \Phi(g) + \Phi(f) \Longrightarrow \sum_{g|f, \deg(g) < k} \Phi(g) = N(f) - \Phi(f)$$

Επομένως:

$$N(f) = \sum_{g|f,\deg(g)<k} \Phi(g) + \sharp A_f = N(f) - \Phi(f) + \sharp A_f \Longrightarrow \Phi(f) = \sharp A_f$$

□

Κάνουμε τώρα την εξής παρατήρηση:
Για $a \in \mathbb{F}_q^m$ η οικογένεια $(a, a^q, ..., a^{q^{m-1}})$ είναι βάση του $\mathbb{F}_{q^m}$ πάνω απ'το $\mathbb{F}_q$ αν και μόνο αν τα $a, a^q, ..., a^{q^{m-1}}$ είναι γραμμικά ανεξάρτητα, δηλαδή αν και μόνο αν:

$$\nexists \sum_{i=0}^{\deg(f)} b_i X^i = f \in \mathbb{F}_q[x], f \text{ μη μηδενικό}, \quad \deg(f) < m \text{ με } f \circ a = 0$$

Οδηγούμαστε λοιπόν στο παρακάτω:
Για $a \in \overline{\mathbb{F}_q}$, η οικογένεια $(a, a^q, .., a^{q^{m-1}})$ είναι βάση του $\mathbb{F}_{q^m}$ πάνω απ'το $\mathbb{F}_q$ αν και μόνο αν $Ord(a) = X^m - 1$ και το $\mathbb{F}_q[x] - υπομodule$ του $\overline{\mathbb{F}_q}$ που γεννάται απο το a είναι ίσο με το $\mathbb{F}_{q^m}$.
Μαζί με τη γνώση του Θεωρήματος 2.3 προκύπτει οτι κανονικές βάσεις του $\mathbb{F}_{q^m}$ πάνω απ'το $\mathbb{F}_q$ υπάρχουν.
Αυτό το συμβολίζουμε με :

$$\mathbb{F}_{q^m} \cong \mathbb{F}_q[x]/(X^m - 1)\mathbb{F}_q[x] \text{ ως } \mathbb{F}_q[x] - modules.$$

Το οποίο είναι ανάλογο με :

$$\mathbb{F}_{q^m}^* \cong \mathbb{Z}/(q^m - 1)\mathbb{Z} \text{ ως } \mathbb{Z} - modules$$

Με όσα είδαμε μέχρι τώρα, είμαστε σε θέση να επαναδιατυπώσουμε το κεντρικό μας θεώρημα:

Θεώρημα 2.4 *Σχεδόν για κάθε' ζεύγος (q, m), q =πρώτος,$m \in \mathbb{N}$ υπάρχει στοιχείο $a \in \mathbb{F}_{q^m}^*$ με*

$$Ord(a) = X^m - 1 \text{ και } ord(a) = q^m - 1$$

Κεφάλαιο 3

Απόδειξη του θεωρήματος 2.4

Με όσα είδαμε στο κεφάλαιο 1, είμαστε σε θέση να μελετήσουμε την εξής συναρτήση:

$$\omega(a) = \sum_{d|n} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in \hat{G}, ord(\chi)=d} \chi(a) \quad (15)$$

όπου $a \in G, G$ πεπερασμένη αβελιανή κυκλική ομάδα, $|G| = n, ord(\chi)$ ειναι η τάξη του χ στην $\hat{G}$ η οποία είναι επίσης κυκλική.
Ας ξεκινήσουμε τη μελέτη της συνάρτησης μας δείχνοντας ότι:

$$f(d) = \sum_{ord(\chi)=d} \chi(a) = \sum_{ord(\chi_1)=d_1} \chi_1(a) \sum_{ord(\chi_2)=d_2} \chi_2(a) = f(d_1)f(d_2)$$

όπου $(d_1, d_2) = 1$ και $d = d_1 d_2$.
Ορίζω την απεικόνιση:

$$\begin{aligned} Y : \hat{G_{d_1}} \times \hat{G_{d_2}} &\longrightarrow \hat{G_d} \\ (\chi_1, \chi_2) &\longmapsto \chi_1\chi_2 = \chi \end{aligned}$$

όπου με $\hat{G_{d_1}}, \hat{G_{d_2}}, \hat{G_d}$ συμβολίζουμε τα υποσύνολα των χαρακτήρων που έχουν τάξη d_1, d_2 και d αντίστοιχα.

Η απεικόνιση αυτή είναι καλώς ορισμένη αφού:
$\chi^d = (\chi_1\chi_2)^d = \chi_1^d\chi_2^d = (\chi_1^{d_1})^{d_2}(\chi_2^{d_2})^{d_1} = \chi_0 \Longrightarrow ord(\chi)|d$
$\chi_0 = \chi^{ord(\chi)} = (\chi_1\chi_2)^{ord(\chi)} = \chi_1^{ord(\chi)}\chi_2^{ord(\chi)} \Longrightarrow \chi_1^{d_2 ord(\chi)} = \chi_0$ και $\chi_2^{d_1 ord(\chi)} = \chi_0 \Longrightarrow$
$d_1|ord(\chi)$ και $d_2|ord(\chi) \Longrightarrow d|ord(\chi)$
Επομένως $d = ord(\chi)$

Έστω τώρα $\chi_1\chi_2 = \chi_1'\chi_2' \Longleftrightarrow (\chi_1\chi_2)^{d_2} = (\chi_1'\chi_2')^{d_2} \Longleftrightarrow \chi_1^{d_2} = \chi_1'^{d_2} \Longleftrightarrow \chi_1 = \chi_1'$
όπου η τελευταία συνεπαγωγή ισχύει διότι $d_2^{-1}d_2 = 1 \pmod{d_1}$. Όμοια:
$\chi_1\chi_2 = \chi_1'\chi_2' \Longleftrightarrow (\chi_1\chi_2)^{d_1} = (\chi_1'\chi_2')^{d_1} \Longleftrightarrow \chi_2^{d_1} = \chi_2'^{d_1} \Longleftrightarrow \chi_2 = \chi_2'$
όπου η τελευταία συνεπαγωγή ισχύει διότι $d_1^{-1}d_1 = 1 \pmod{d_2}$.
Άρα η Y είναι ένα προς ένα.

$(d_1,d_2)=1 \Longrightarrow \exists x,y\in\mathbb{Z}$ τ.ω. $1=d_1x+d_2y$
ορίζω $\chi_1=\chi^{d_2y}$ και $\chi_2=\chi^{d_1y}$. Τότε:
$\chi=\chi^{d_1x+d_2y}=\chi_1\chi_2$
Επομένως η Y είναι επί. Έτσι:

$$f(d)=\sum_{ord(\chi)=d}\chi(a)=\sum_{ord(\chi_1)=d_1,ord(\chi_2)=d_2}\chi_1\chi_2(a)=\sum_{ord(\chi_1)=d_1,ord(\chi_2)=d_2}\chi_1(a)\chi_2(a)=$$
$$\sum_{ord(\chi_1)=d_1}\chi_1(a)\sum_{ord(\chi_2)=d_2}\chi_2(a)=f(d_1)f(d_2)$$

Θα δείξουμε τώρα οτι αν $(n,m)=1$ και $\gamma(mn)=\gamma(n)\gamma(m)$ τότε $\delta(nm)=\sum_{d|nm}\gamma(d)=\delta(n)\delta(m)$

Αφού $(d_1,d_2)=1$ έπεται οτι:

$$\delta(nm)=\sum_{d|nm}\gamma(d)=\sum_{d_1|n,d_2|m}\gamma(d_1d_2)=\sum_{d_1|n}\sum_{d_2|m}\gamma(d_1)\gamma(d_2)=\sum_{d_1|n}\gamma(d_1)\sum_{d_2|m}\gamma(d_2)=\delta(n)\delta(m)$$

Με όσα είδαμε είμαστε σε θέση να αντιληφθούμε ότι:
για $n=p_1^{a_1}\cdots p_k^{a_k}$ όπου p_i πρώτος,$i=1,..,k$

$$g(n)=\sum_{d|n}\frac{\mu(d)}{\phi(d)}\sum_{\chi\in\hat{G},ord(\chi)=d}\chi(a)=\prod_{p|n}\sum_{d|p^{a_p}}\frac{\mu(d)}{\phi(d)}f(d)=$$

$$\prod_{p|n}\sum_{i=0}^{a_p}\frac{\mu(p^i)}{\phi(p^i)}\sum_{ord(\chi)=p^i}\chi(a)=\prod_{p|n}(\frac{\mu(p^0)}{\phi(p^0)}\sum_{ord(\chi)=p^0}\chi(a)+\sum_{i=0}^{a_p}\frac{\mu(p^i)}{\phi(p^i)}\sum_{ord(\chi)=p^i}\chi(a))(16)$$

$\mu(p^i)=0$ αν $i>1$ άρα :

$$(16)=\prod_{p|n}(1+\frac{\mu(p)}{\phi(p)}\sum_{ord(\chi)=p}\chi(a))=\prod_{p|n}(1-\frac{1}{p-1}f(p))(17)$$

Σε αυτό το σημείο μπορούμε να δούμε τα εξής:
1)Αν $ord(a)\neq n$ τότε $\exists\gamma\in G$ τ.ω.:
$a=\gamma^{\omega_1^{a_1}\ldots\omega_t^{a^t}}=(\gamma^{\omega_1^{a_1-1}\ldots\omega_t^{a^t}})^{\omega_1}=\beta^{\omega_1}$ όπου $\omega_i=$πρώτος,$\omega_i|n,i=1,..,t$
Βλέπουμε επομένως ότι $\exists$ πρώτος $p,p|n$ και $\beta\in G$ τ.ω. $a=\beta^p$. Επομένως
$\chi(a)=\chi(\beta^p)=(\chi(\beta))^p=1$ όταν $\chi^p=1$
Άρα

$$\sum_{\chi\in\hat{G},ord(\chi)=p,p|n}\chi(a)=\sum_{\chi\in\hat{G},ord(\chi)=p,p|n}\chi^p(\beta)=\phi(p)=p-1$$

Συνεπώς

$$(17) = \prod_{p|n, p=\pi\rho\omega\tau ος} (1 - \frac{p-1}{p-1}) = 0$$

2)Αν τώρα $ord(a) = n$ παρατηρώ ότι:

$$\sum_{ord(\chi)=p, p=\pi\rho\omega\tau ος} \chi(a) = \sum_{ord(\chi)|p, p=\pi\rho\omega\tau ος} \chi(a) - \chi_0(a) = -1$$

Έστω $H = \{a^p : a \in G\} \leq G$ και $A = \{\chi \in \hat{G} : ord(\chi)|p\} = \{\chi \in \hat{G} : \chi(h) = 1 \forall h \in H\}$
Επομένως σύμφωνα με το θεώρημα 1.10 $A \cong \frac{\hat{\mathbb{F}_q^*}}{H}$ Ας μη ξεχνάμε ότι:
$\sum_{\chi \in \hat{G}} \chi(a) = 0$ αν $a \neq 1$ ή $|G|$ αν $a = 1$
Επομένως
$\sum_{\chi \in A} \chi(a) = \sum_{\bar{\chi} \in \frac{\hat{\mathbb{F}_q^*}}{H}} \bar{\chi}(aH) = 0$ αν $aH \neq H$ ή $, \frac{\mathbb{F}_q^*}{H},$ αν $aH = H$.
Βλέπουμε ότι $aH = H \Longrightarrow a \in H \Longrightarrow a = \beta^p$
Όμως έχουμε $ord(a) = n$ και $p|n$, επομένως $a \neq aH$ και έτσι:
$\sum_{\chi \in A} \chi(a) = 0 \Longrightarrow \sum_{\chi \in \hat{G}, ord(\chi)=p} \chi(a) = -1$ και τότε:

$$(17) = \prod_{p|n} (1 - \frac{1}{p-1}(-1)) = \prod_{p|n} (\frac{p}{p-1}) = \frac{n}{\phi(n)}$$

αφού $\frac{n}{\phi(n)} = \frac{p_1^{a_1} \cdots p_k^{a_k}}{p_1^{a_1-1} \cdots p_k^{a_k-1}(p_1-1)\cdots(p_k-1)} = \frac{p_1}{p_1-1} \cdots \frac{p_k}{p_k-1}$

Εφαρμόζοντας όσα είδαμε για $G = \mathbb{F}_{q^m}^*, n = q^m - 1$ τότε
$\omega : \mathbb{F}_{q^m}^* \longrightarrow \mathbb{C}, \quad \omega(a) = \sum_{d|q^m-1} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in \hat{G}, ord(\chi)=d} \chi(a), \chi \in \hat{\mathbb{F}_{q^m}^*}$.

Συνεχίζοντας θα δούμε την αναλογία της $\omega(a)$ για την προσθετίκη ομάδα της $\mathbb{F}_{q^m}$.
Έστω $\hat{\mathbb{F}_{q^m}}$ ο δυϊκός της προσθετικής ομάδας της $\mathbb{F}_{q^m}$.Ορίζουμε:
$(\lambda^f)(a) = \lambda(f \circ a)$ για $\lambda \in \hat{\mathbb{F}_{q^m}}, f \in \mathbb{F}_q[x], a \in \mathbb{F}_{q^m}$.
Τότε:
1) $\lambda \in \hat{\mathbb{F}_{q^m}}, f \circ a \in \mathbb{F}_{q^m} \lambda^f(a+b) = \lambda(f \circ (a+b)) = \lambda((f \circ a) + (f \circ b)) = \lambda(f \circ a)\lambda(f \circ b) = \lambda^f(a)\lambda^f(b)$.Έτσι $\lambda^f \in \hat{\mathbb{F}_{q^m}}$
2)$(\lambda_1\lambda_2)^f(a) = (\lambda_1\lambda_2)(f \circ a) = \lambda_1(f \circ a)\lambda_2(f \circ a) = \lambda_1^f(a)\lambda_2^f(a)$.
3) $\lambda^{f+g}(a) = \lambda((f+g) \circ a) = \lambda((f \circ a) + (g \circ a)) = \lambda(f \circ a)\lambda(g \circ a) = \lambda^f(a)\lambda^g(a)$.
4) $\lambda^{fg}(a) = \lambda((fg) \circ a) = \lambda(f \circ (g \circ a)) = \lambda^f(g \circ a) = (\lambda^f)^g(a)$
Επομένως η προσθετική ομάδα $\hat{\mathbb{F}_{q^m}}$ εφοδιασμένη με την εξωτερική πράξη $\lambda^f(a)$ είναι ένα $\mathbb{F}_q[x] - module$.Μπορούμε λοιπόν να παρατηρήσουμε τα εξής:

Αν $a \in \mathbb{F}_{q^m}$ τότε: $\lambda^{X^m-1}(a) = \lambda((X^m-1) \circ a) = \lambda(0) = 1$ (18)

Ας δούμε το σύνολο:

$$J_a = \{f \in \mathbb{F}_q[x] : \lambda^f = 1\}.$$

1)Αν $f \in J_a$ και $g \in \mathbb{F}_q[x]$ τότε $\lambda^{gf} = \lambda^{fg} = (\lambda^f)^g = 1^g = 1$. Επομένως $fg, gf \in J_a$.
2)Αν $f, g \in J_a$ τότε $\lambda^{f+g} = \lambda^f \lambda^g = 1$. Άρα $f + g \in J_a$.

Συνεπώς το J_a είναι ιδεώδες του $\mathbb{F}_q[x]$. Όμως το $\mathbb{F}_q[x]$ είναι ευκλείδιος δακτύλιος και έτσι J_a είναι κύριο. Δηλαδή $J_a =< f >$.
Θα καλούμε $Ord(\lambda)$ ενός χαρακτήρα λ το μονικό πολυώνυμο f, το οποίο γεννάει το J_a.
Απο την (18) βλέπουμε οτι $f|X^m - 1$.

Θεώρημα 3.1 *Έστω f μονικός διαφέτης του $X^m - 1 \in \mathbb{F}_q[x]$. Τότε υπάρχουν $\Phi(f)$ χαρακτήρες $\lambda \in \hat{\mathbb{F}_{q^m}}$ με $Ord(\lambda) = f$.*

Για την απόδειξη του θεωρήματος θα χρειαστούμε το εξής λήμμα:

Λήμμα 3.2 *Έστω f, g πολυώνυμα τότε:*
$\sum_{g|f} \sharp\{\lambda : Ord(\lambda) = g\} = N(f)$

Απόδειξη. $\sum_{g/f} \sharp\{\lambda : Ord(\lambda) = g\} = \sharp\{\lambda : \lambda^f = 1\}$.
Τι μπορούμε να πούμε για το σύνολο $H = \{\lambda : \lambda^f = 1\}$·
Φανερά το Η είναι υποσύνολο της $\hat{\mathbb{F}_{q^m}}$ και
$H = \{\lambda : \lambda^f = 1\} = \{\lambda \in \hat{\mathbb{F}_{q^m}} : \lambda^f(b) = 1, \forall b \in \mathbb{F}_{q^m}\} = \{\lambda \in \hat{\mathbb{F}_{q^m}} : \lambda(f \circ b) = 1, \forall b \in \mathbb{F}_{q^m}, f \in \mathbb{F}_q[x]\}$

Έστω $H_1 = \{b \in \mathbb{F}_{q^m} : b = (f \circ a)$ για κάποιο $a \in \mathbb{F}_{q^m}\} \subseteq \mathbb{F}_{q^m}$ τότε:
$H = \{\lambda \in \hat{\mathbb{F}_{q^m}} : \lambda|_{H_1} = 1\}$.
Έπομένως απο το θεώρημα 1.10
$H \cong \frac{\hat{\mathbb{F}_q}}{H_1}$ και $|H| = |\frac{\hat{\mathbb{F}_q}}{H_1}| = |\frac{\mathbb{F}_{q^m}}{H_1}| = \frac{q^m}{|H_1|}$.
Για να βρούμε την $|H_1|$ ορίζουμε την απεικόνιση:

$$\begin{aligned} L : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_{q^m} \\ a &\longmapsto f^*(a) \end{aligned}$$

Η γνώση όσων έχουμε δεί μέχρι τώρα για το $f^*(a)$ μας οδηγεί άμεσα στο ότι L γραμμική.
Ακομά:
$ImL = H_1, kerL = \{a \in \mathbb{F}_{q^m} : f^*(a) = 0, f \in \mathbb{F}_q[x]\}$ και
$a \in kerL \iff f^*(a) = 0 \iff f \circ a = 0 \iff Ord(a)|f$
Εχουμε δείξει όμως οτι το πλήθος των $a \in \mathbb{F}_{q^m}$ με $Ord(a)|f$ είναι ίσο με το πλήθος των διαφορετικών ριζών του $f^*, f^* = \sum_{i=0}^{m} b_i X^{q^i}$. Συνεπώς,
$\sharp\{a \in \mathbb{F}_{q^m} : f^*(a) = 0, f \in \mathbb{F}_q[x]\} = q^{\deg(f)}$
Επομένως,
$dimkerL + dimImL = m \Longrightarrow deg(f) + dimImL = m \Longrightarrow dimImL = m - \deg(f)$

Έτσι $|H_1| = q^{m-\deg(f)}$
Άρα $|H| = \frac{q^m}{q^{m-\deg(f)}} = q^{\deg(f)} = N(f)$

□

Αποδεικνύουμε τώρα το θεώρημα 3.1

Απόδειξη. Ας θυμηθούμε οτι θέλουμε να δείξουμε:
$\Phi(f) = \sharp\{\lambda \in \hat{\mathbb{F}_{q^m}} : Ord(\lambda) = f\} := |B_f|$
Παρατηρούμε το εξής:
$\sum_{g|f} |B_g| = |\bigcup_{g|f} B_g| = \sharp\{\lambda \in \hat{\mathbb{F}_{q^m}} : Ord(\lambda)|f\} = N(f)$
Όπου η πρώτη ισότητα ισχύει διότι $B_{g_1} \bigcap B_{g_2} = \varnothing$ για $g_1 \neq g_2$

Δείχνουμε ότι $|B_f| = \Phi(f)$ με επαγωγή στο $\deg(f)$
Αν $f|X^m - 1$ και $\deg(f) = 1$ τότε:
$q = q^{\deg(f)} = \sum_{g|f} |B_g| = |B_1| + |B_f| = 1 + |B_f| \Longrightarrow |B_f| = q - 1 = \Phi(f)$
Υποθέτω οτι για $f|X^m - 1$ με $\deg(f) \leq k - 1$ ισχύει.
Έστω $f|X^m - 1$ και $\deg(f) = k$ τότε:
$N(f) = \sum_{g|f} |B_g| = \sum_{g|f, \deg(g) < \deg(f)} |B_g| + |B_f| = \sum_{g|f, \deg(g) < n} \Phi(g) + |B_f|.$

Όμως $N(f) = \sum_{g|f, \deg(g) < n} \Phi(g) + \Phi(f) \Longrightarrow \sum_{g|f, \deg(g) < n} \Phi(g) = N(f) - \Phi(f).$
Επομένως
$N(f) = \sum_{g|f, \deg(g) < n} \Phi(g) + |B_f| = N(f) - \Phi(f) + |B_f| \Longrightarrow \Phi(f) = |B_f|$

□

Προχωρόντας ορίζουμε αναλόγως με το $\omega(a)$.
$\Omega : \mathbb{F}_{q^m} \longrightarrow \mathbb{C}$
με $\Omega(a) = \sum_{g|X^m-1} \frac{M(g)}{\Phi(g)} \sum_{\lambda, Ord(\lambda)=g} \lambda(a), \lambda \in \hat{\mathbb{F}_{q^m}}$.
Έστω $F(g) = \sum_{Ord(\lambda)=g} \lambda(a)$
Για $g = g_1 g_2$ και $(g_1, g_2) = 1$
Ορίζω την απεικόνιση:

$$Z : \hat{G_{g_1}} \times \hat{G_{g_2}} \longrightarrow \hat{G_g}$$
$$(\lambda_1, \lambda_2) \longmapsto \lambda_1 \lambda_2 = \lambda$$

όπου με $\hat{G_{g_1}}, \hat{G_{g_2}}, \hat{G_g}$ συμβολίζουμε την ομάδα των χαρακτήρων που έχουν $Ord g_1, g_2$ και g αντίστοιχα.
Τι ισχύει για τη Z ·
1) καλώς ορισμένη:
$\lambda^g = (\lambda_1 \lambda_2)^g = \lambda_1^g \lambda_2^g = \lambda_0 \Longrightarrow Ord(\lambda)|g$
$\lambda_0 = \lambda^{Ord(\lambda)} = (\lambda_1 \lambda_2)^{Ord(\lambda)} \Longrightarrow \lambda_1^{Ord(\lambda)} = \lambda_2^{-Ord(\lambda)} \Longrightarrow \lambda_1^{g_2 Ord(\lambda)} = \lambda_0$ και $\lambda_2^{g_1 Ord(\lambda)} = \lambda_0 \Longrightarrow g_1 | g_2 Ord(\lambda)$ και $g_2 | g_1 Ord(\lambda) \Longrightarrow g_1 | Ord(\lambda)$ και $g_2 | Ord(\lambda) \Longrightarrow g | Ord(\lambda)$.
Άρα $Ord(\lambda) = g$
2) Ένα προς ένα:
Αν $\lambda_1 \lambda_2 = \lambda_1' \lambda_2' \Longrightarrow (\lambda_1 \lambda_2)^{g_2} = (\lambda_1' \lambda_2')^{g_2}$
$\Longrightarrow \lambda_1^{g_2} = \lambda_1'^{g_2} \Longrightarrow \lambda_1 = \lambda_1'$
Όπου η τελευταία ισοδυναμία ισχύει διότι:
$(g_1, g_2) = 1$ άρα το g_2 έχει αντίστροφο $mod ulo g_1$ δηλαδή αν g_2^{-1} ο αντίστροφος του g_2 τότε $g_2^{-1} g_2 = 1 mod(g_1)$.

Ομοίως δείχνουμε:
$\lambda_1\lambda_2 = \lambda_1'\lambda_2' \Longrightarrow \lambda_2 = \lambda_2'$.
3) Επί:
$(g_1, g_2) = 1 \Longrightarrow \exists h_1, h_2 \in \mathbb{F}_q[x]$ τ.ω. $1 = g_1h_1 + g_2h_2$
Ορίζω $\lambda_1 = \lambda^{g_2h_2}$ και $\lambda_2 = \lambda^{g_1h_1} \Longrightarrow \lambda = \lambda^{g_2h_2+g_1h_1} = \lambda_1\lambda_2$.
Έτσι:

$$\sum_{\lambda\in\hat{\mathbb{F}_{q^m}}, Ord(\lambda)=g} \lambda(a) = \sum_{\lambda_1\in\hat{\mathbb{F}_{q^m}}, Ord(\lambda_1)=g_1} \lambda_1(a) \sum_{\lambda_2\in\hat{\mathbb{F}_{q^m}}, Ord(\lambda_2)=g_2} \lambda_2(a)$$

Όπως πριν είναι εύκολο να αποδείξουμε οτι:
Αν $(g,h) = 1$ και $\Gamma(gh) = \Gamma(g)\Gamma(h)$ τότε $\Delta(gh) = \sum_{f/gh}\Gamma(f) = \Delta(g)\Delta(h)$
Καταλήγουμε λοιπόν ότι:
$X^m - 1 = h_1^{p_1}\cdots h_k^{p_k}$, $h_1, .., h_k$ μονικά ανάγωγα.

$$\Omega(a) = \sum_{g|X^m-1} \frac{M(g)}{\Phi(g)} \sum_{\lambda, Ord(\lambda)=g} \lambda(a) = \prod_{h|X^m-1} \sum_{g|h^{p_h}} \frac{M(g)}{\Phi(g)} \sum_{\lambda, Ord(\lambda)=g} \lambda(a) =$$

$$\prod_{h|X^m-1} \sum_{i=0}^{p_h} \frac{M(h^i)}{\Phi(h^i)} \sum_{Ord(\lambda)=h^i} \lambda(a) = \prod_{h|X^m-1} (1 + \frac{M(h)}{\Phi(h)} \sum_{Ord(\lambda)=h} \lambda(a))$$

(αφου $M(h^i) = 0$ αν $i > 1$)

$$= \prod_{h|X^m-1} (1 - \frac{1}{q^{degh} - 1} \sum_{\lambda, Ord(\lambda)=h} \lambda(a))(20)$$

Αν $Ord(a) \neq X^m - 1$ τότε $\exists h | X^m - 1$ και $\gamma \in \mathbb{F}_{q^m}$ τ.ω. $a = f\circ\beta = (hg)\circ\beta = h\circ(g\circ\beta) = h\circ\gamma$
Άρα $\lambda(a) = \lambda(h\circ\gamma) = \lambda^h(\gamma) = 1$ όταν $Ord(\lambda) = h$
Άρα

$$\sum_{\lambda\in\mathbb{F}_{q^m}, Ord(\lambda)=h} \lambda(a) = \sum_{\lambda, Ord(\lambda)=h} \lambda(h\circ\gamma) = \sum_{\lambda, Ord(\lambda)=h} \lambda^h(\gamma) = \Phi(h) = q^{\deg h} - 1$$

Έτσι (20)=0
Αν τώρα $Ord(a) = X^m - 1$ τότε
$\sum_{Ord(\lambda)=h, h\,\mu ονικο\,\alpha ναγωγο} \lambda(a) = \sum_{Ord(\lambda)|h, h\,\mu ονικο\,\alpha ναγωγο} \lambda(a) - \lambda_0(a)$
Έστω
$H = \{\beta \in \mathbb{F}_{q^m} : \beta = h\circ a, h \in \mathbb{F}_q[x]\} \subseteq \mathbb{F}_{q^m}$ φανερά και $B = \{\lambda \in \hat{\mathbb{F}_{q^m}} : \lambda^h = 1\} = \{\lambda \in \hat{\mathbb{F}_{q^m}} : \lambda^h(\beta) = 1 \forall \beta \in H\}$
Απο θεώρημα 1.10 έχουμε:
$B \cong \frac{\hat{\mathbb{F}_q^m}}{H} \cong \frac{\mathbb{F}_q^m}{H}$
$\sum_{\lambda\in B}\lambda(a) = \sum_{\bar{\lambda}\in\frac{\hat{\mathbb{F}_q^m}}{H}} \bar{\lambda}(a + H)(21)$
αν $a + H \neq H$ τότε (21)=0 ενώ αν $a + H = H$ τότε (21)=$\sharp\frac{\mathbb{F}_{q^m}}{h\circ\mathbb{F}_{q^m}}$
Αν $a + H = H \Longrightarrow a \in H \Longrightarrow a = h\circ b$
Όμως $Ord(a) = X^m - 1$ και $h|X^m - 1$. Άρα $a \neq a + H$

Συνεπώς:

$$\sum_{\lambda\in\mathbb{F}_{q^m},Ord(\lambda)=h}\lambda(a)=\sum_{\lambda\in B}\lambda(a)-1=-1$$

και

$$(20)=\prod_{h|X^m-1}(1-\frac{1}{q^{\deg h-1}}(-1))=\prod_{h|X^m-1}(1+\frac{1}{q^{\deg h-1}})=\prod_{h|X^m-1}(\frac{q^{\deg h}}{q^{\deg h-1}})=\frac{q^m}{\Phi(X^m-1)}$$

Όπου η τελευταία ισότητα αληθεύει διότι:

$$\frac{q^m}{\Phi(X^m-1)}=\frac{q^m}{q^m\prod_{h|X^m-1}(1-\frac{1}{q^{\deg h}})}=\prod_{h|X^m-1}(\frac{1}{\frac{q^{\deg h-1}}{q^{\deg h}}})=\prod_{h|X^m-1}(\frac{q^{\deg h}}{q^{\deg h}-1})$$

Ας προσπαθήσουμε να συνδιάσουμε τα αποτελέσματά μας:
Έχουμε λοιπόν $\omega(a)=0$ αν $ord(a)\neq q^m-1$, $\Omega(a)=0$ αν $Ord(a)\neq X^m-1$
Επομένως $\omega(a)\Omega(a)=0$ αν $ord(a)\neq q^m-1$ και $Ord(a)\neq X^m-1$
Θέτοντας $\chi(0)=0$ για $\chi\neq 1$ και $\chi_0(0)=1$ επεκτείνουμε τους χαρακτήρρες της $\mathbb{F}^*_{q^m}$ σε όλο το $\mathbb{F}_{q^m}$
Έτσι $\omega(0)\Omega(0)=0$

Πρόταση 3.3 *Έστω s το πλήθος των διαφορετικών πρώτων διαιρετών του q^m-1 και t το πλήθος των διαφορετικών μονικών αναγώγων πολυωνύμων του $X^m-1\in\mathbb{F}_q[x]$.*
Έστω οτι ισχύει:
$(2^s-1)(2^t-1)<q^{m/2}$
Τότε $\exists a\in\mathbb{F}^*_{q^m}$ με $Ord(a)=X^m-1$ και $ord(a)=q^m-1$.

Απόδειξη. Έστω οτι δεν ισχύει,τότε απ'οσα έχουμε δεί:

$$\omega(a)\Omega(a)=0\forall a\in\mathbb{F}_{q^m}$$

και

$$\sum_{a\in\mathbb{F}_{q^m}}\omega(a)\Omega(a)=0(21)$$

Όμως

$$\begin{aligned}\sum_{a\in\mathbb{F}_{q^m}}\omega(a)\Omega(a) &= \sum_{d|q^m-1}\sum_{g|X^m-1}\frac{\mu(d)M(g)}{\phi(d)\Phi(g)}\sum_{\chi,ord(\chi)=d}\sum_{\psi,Ord(\psi)=g}G(\psi,\chi)\\ &= \sum_{d|q^m-1,d\neq1}\frac{\mu(d)}{\phi(d)}\sum_{g|X^m-1,g\neq1}\frac{M(g)}{\Phi(g)}\sum_{ord(\chi)=d}\sum_{Ord(\psi)=g}G(\psi,\chi)\\ &+ \sum_{g|X^m-1,g\neq1}\frac{M(g)}{\Phi(g)}\sum_{Ord(\psi)=g}G(\psi,\chi_0)\\ &+ \sum_{d|q^m-1,d\neq1}\frac{\mu(d)}{\phi(d)}\sum_{ord(\chi)=d}G(\psi_0,\chi)+G(\psi_0,\chi_0)\end{aligned}$$

$$= \sum_{d|q^m-1,d\neq 1} \frac{\mu(d)}{\phi(d)} \sum_{g|X^m-1,g\neq 1} \frac{M(g)}{\Phi(g)} \sum_{ord(\chi)=d} \sum_{Ord(\psi)=g} G(\psi,\chi) + q^m$$

$$\Longrightarrow$$

$$\sum_{a\in\mathbb{F}_{q^m}} \omega(a)\Omega(a) - q^m = \sum_{d|q^m-1,d\neq 1} \frac{\mu(d)}{\phi(d)} \sum_{g|X^m-1,g\neq 1} \frac{M(g)}{\Phi(g)} \sum_{ord(\chi)=d} \sum_{Ord(\psi)=g} G(\psi,\chi)$$

Και με τη βοήθεια της (21) καταλήγουμε λοιπόν ότι:

$$-q^m = \sum_{d|q^m-1,d\neq 1} \frac{\mu(d)}{\phi(d)} \sum_{g|X^m-1,g\neq 1} \frac{M(g)}{\Phi(g)} \sum_{ord(\chi)=d} \sum_{Ord(\psi)=g} G(\psi,\chi)$$

Όπως έχουμε δει υπάρχουν $\phi(d)$ χαρακτήρες χ με $ord(\chi) = d$ και $\Phi(g)$ χαρακτήρες ψ με $Ord(\psi) = g$.Άρα

$$\begin{aligned}
q^m = |-q^m| &= |\sum_{d|q^m-1,d\neq 1} \frac{\mu(d)}{\phi(d)} \sum_{g|X^m-1,g\neq 1} \frac{M(g)}{\Phi(g)} \sum_{ord(\chi)=d} \sum_{Ord(\psi)=g} G(\psi,\chi)| \\
&\leq \sum_{d|q^m-1,d\neq 1} |\frac{\mu(d)}{\phi(d)}| \sum_{g|X^m-1,g\neq 1} |\frac{M(g)}{\Phi(g)}| \sum_{ord(\chi)=d} \sum_{Ord(\psi)=g} |G(\psi,\chi)| \\
&\leq \sum_{d|q^m-1,d\neq 1} \frac{|\mu(d)|}{\phi(d)} \sum_{g|X^m-1,g\neq 1} \frac{|M(g)|}{\Phi(g)} q^{m/2} \sum_{ord(\chi)=d} \sum_{Ord(\psi)=g} 1 \\
&= \sum_{d|q^m-1,d\neq 1} \frac{|\mu(d)|}{\phi(d)} \sum_{g|X^m-1,g\neq 1} \frac{|M(g)|}{\Phi(g)} q^{m/2}\phi(d)\Phi(g) \\
&= q^{m/2} \sum_{d|q^m-1,d\neq 1} |\mu(d)| \sum_{g|X^m-1,g\neq 1} |M(g)| = q^{m/2}(2^s-1)(2^t-1)
\end{aligned}$$

Άτοπο!
Για να κατανοήσουμε την τελευταία ισότητα ας δούμε το εξής:
Έστω $q^m - 1 = q_1^{a_1} \cdots q_s^{a_s}$ και $d|q^m - 1$.Επειδή $\mu(d) \neq 0$ μόνο αν στην ανάλυση του d δεν υπάρχουν δυνάμεις,μας αρκεί να δούμε πόσα d υπάρχουν τ.ω. $d|q_1 \cdots q_s$
Το πλήθος αυτών όμως είναι:
$1 + s + \frac{s!}{(s-2)!2} + \cdots + \frac{s!}{(s-k)!k!} + \cdots + s + 1 = 2^s$
και επειδή $d \neq 1$ έχουμε $\sum_{d|q^m-1,d\neq 1} |\mu(d)| = 2^s - 1$
Ακριβώς όμοια βλέπουμε οτι $\sum_{g|X^m-1,g\neq 1} |M(g)| = 2^t - 1$.

□

Για να αξιοποιήσουμε την παραπάνω πρόταση θα χρειαστούμε κάποια φράγματα για τα s, t. Ας ξεκινήσουμε μελετόντας το t.

Λήμμα 3.4 *Έστω q μια δύναμη πρώτου > 1 και $m \in \mathbb{N}$.Τότε το πλήθος t των μονικών αναγώγων παραγόντων του $X^m - 1$ στο $\mathbb{F}_q[X]$ δίδεται απο:*

$$t = \sum_{d|m,(d,q)=1} \frac{\phi(d)}{k(d)},$$

$k(d)$ είναι η τάξη του $q \pmod d$) στο $(\mathbb{Z}/d\mathbb{Z})^*$

Απόδειξη. Θεωρούμε γνωστό οτι η ανάλυση του X^m-1 είναι η εξής:
$X^m-1=\prod_{d|m}\Phi_d, \Phi_d=\prod_{a\in\mathbb{F}_q^-,ord(a)=d}(X-a)$
Είδαμε οτι υπάρχουν $\phi(d)$ στοιχεία με $ord(a)=d$ επομένως ο βαθμός του Φ_d είναι $\phi(d)$. Εφ'οσων $k(d)$ είναι η τάξη του $q \pmod d$ στο $(\mathbb{Z}/d\mathbb{Z})^*$ και γνωρίζουμε οτι αυτό συνεπάγεται $\deg(a)=k(d)$, αντιλαμβανόμαστε οτι κάθε ανάγωγος παράγοντας του Φ_d έχει βαθμό $k(d)$.Επομένως το Φ_d έχει $\frac{\phi(d)}{k(d)}$ ανάγωγους παράγοντες και επειδή $X^m-1=\prod_{d|m}\Phi_d$ συμπεραίνουμε οτι $t=\sum_{d|m,(d,q)=1}\frac{\phi(d)}{k(d)}$

□

Λήμμα 3.5 *Έστω q,m,t όπως πριν και $e\in\mathbb{N}$. Έστω D ένα σύνολο απο θετικούς διαιρέτες του m έτσι ώστε $\forall d\in D$ να ισχύει $(d,q)=1$ και το D να περιέχει όλους τους θετικούς διαιρέτες του μκδ$(m,q^{e'}-1)$ $\forall e'\in\mathbb{N},e'<e$. Τότε:*

$$t\le\frac{m}{e}+\sum_{d\in D}\phi(d)(\frac{1}{k(d)}-\frac{1}{e})$$

Απόδειξη. Αρχικά παρατηρούμε ότι $\forall d|m,d\notin D\Longrightarrow k(d)\ge e$.
Το βλέπουμε αυτό ως εξής:
Έστω $d|m,d\notin D$ και $k(d)<e$. Αφού $q^{k(d)}\equiv 1 \pmod d\Longrightarrow q^{k(d)}-1\equiv 0 \pmod d\Longrightarrow d|q^{k(d)}-1\Longrightarrow d|$μκδ$(m,q^{k(d)}-1)$(αφου $d|m$).
Άρα $d\in D$. Άτοπο!
Επομένως:

$$t=\sum_{d|m,d\notin D}\frac{\phi(d)}{k(d)}+\sum_{d\in D}\frac{\phi(d)}{k(d)}\le\sum_{d|m,d\notin D}\frac{\phi(d)}{e}+\sum_{d\in D}\frac{\phi(d)}{k(d)}=\sum_{d|m}\frac{\phi(d)}{e}-\sum_{d\in D}\frac{\phi(d)}{e}+\sum_{d\in D}\frac{\phi(d)}{k(d)}=$$
$$\frac{m}{e}+\sum_{d\in D}\phi(d)(\frac{1}{k(d)}-\frac{1}{e})$$

□

Η αμέσως επόμενη σχέση που θα δείξουμε ώστε να αξιοποιήσουμε τα αποτελέσματά μας αφορά το s.

Λήμμα 3.6 *$\forall m>0,m\in\mathbb{R}$ ισχύει $2^{\omega(m)}\le 4.9m^{1/4}$*
όπου $\omega(m)$ είναι το πλήθος των διαφορετικών πρώτων του m και $2^{\omega(m)}$ το πλήθος των διαιρετών του m των οποίων η ανάλυση δεν έχει τετράγωνα.

Απόδειξη. Έστω $m=m_1^{a_1}\cdots m_k^{a_k}$ η ανάλυση του m σε πρώτους παράγοντες, τότε $m>m_1\cdots m_k$.(22)
Στην ανάλυση του m επιλέγω m_i διαφορετικούς πρώτους, μικρότερους απο 16.Επομένως:

$$(22)>m_1\cdots m_s2^{4(k-s)}\Longrightarrow 2^4k<\frac{2^{4s}}{m_1\ldots m_s}m\Longrightarrow 2^k<\frac{2^s}{(m_1\ldots m_s)^{1/4}}m^{1/4}$$

Με τη χρήση του υπολογιστή μπορούμε να δείξουμε ότι $\forall m\in\mathbb{N}$ έχουμε $\frac{2^s}{(m_1\cdots m_s)^{1/4}}<4.9$

απ'οπου έπεται και το ζητούμενο.

□

Θα κάνουμε τώρα ορισμένες εκτιμήσεις για το πλήθος t των μονικών αναγώγων διαιρετών του $X^m - 1$ και θα δούμε οτι η απαίτηση $(2^s - 1)(2^t - 1) < q^{\frac{m}{2}}$ της πρότασης 3.3 ικανοποιείται 'σχεδόν για κάθε' ζεύγος (q, m). Άρα 'σχεδόν για κάθε' ζεύγος (q, m) θα $\exists a \in \mathbb{F}^*_{q^m}$ με $Ord(a) = X^m - 1$ και $ord(a) = q^m - 1$, έτσι θα έχουμε αποδείξει και το κεντρικό μας θεώρημα.

Θέλουμε να ικανοποιείται $(2^s - 1)(2^t - 1) < q^{\frac{m}{2}}$, όμως:

$$(2^s - 1)(2^t - 1) < 2^s 2^t < 4.9 q^{\frac{m}{4}} 2^t < 2^{2.4} q^{\frac{m}{4}} 2^t$$

Επομένως αρκεί

$$2^{2.4} q^{\frac{m}{4}} 2^t < q^{\frac{m}{2}} \Longrightarrow 2^{2.4} 2^t < q^{\frac{m}{4}}$$

Επιλέγουμε $e = 3$ στο λήμμα 3.5, μπορούμε έτσι να κάνουμε τις εξής εκτιμήσεις:

$$t \leq \frac{m}{3} + \sum_{d|(m,q-1)} \phi(d)(1 - \frac{1}{3}) + \sum_{d|(m,q^2-1)} \phi(d)(\frac{1}{2} - \frac{1}{3}) \qquad (22)$$

★ Αν $m \geq q^2$ τότε,

$$(22) < \frac{m}{3} + \sum_{d|q-1} \phi(d)\frac{2}{3} + \sum_{d|q^2-1} \phi(d)\frac{1}{6} = \frac{m}{3} + \frac{2}{3}(q-1) + \frac{1}{6}(q^2-1)$$

και έτσι ζητάμε,

$$2^{2.4} 2^{\frac{m}{3} + \frac{2}{3}(q-1) + \frac{1}{6}(q^2-1)} < q^{\frac{m}{4}}$$

Δηλαδή θέλουμε,

$$2.4 + \frac{m}{3} + (q-1)\frac{2}{3} + (q^2-1)\frac{1}{6} < \log_2 q^{\frac{m}{4}}$$

οπότε αρκεί

$$1.6 + \frac{q^2 + 4q}{6} < \frac{m}{4}\log_2 q - \frac{m}{3} = \frac{m}{12}(3\log_2 q - 4)$$

και επειδή $m \geq q^2$ θέλουμε τελικά,

$$\begin{aligned} 1.6 + \frac{q^2 + 4q}{6} &< \frac{q^2}{12}(3\log_2 q - 4) \Longleftrightarrow \\ \frac{19.2}{q^2} + \frac{8}{q} + 2 &< 3\log_2 q - 4 \Longleftrightarrow \\ \frac{19.2}{q^2} + \frac{8}{q} + 6 &< 3\log_2 q \qquad (23) \end{aligned}$$

Έστω οτι ικανοποιείται η (23) για κάποιο q και έχουμε $q' > q > 0$ τότε,

$$\frac{19.2}{(q')^2} + \frac{8}{q'} + 6 < \frac{19.2}{q^2} + \frac{8}{q} + 6 < 3\log_2 q < 3\log_2 q'$$

Αρκεί λοιπόν να βρούμε κάποιο q που να ικανοποιεί την (23) και τότε $\forall q' > q$ θα ικανοποιείται.
Παρατηρούμε μετά απο δοκιμές ότι για $q = 7$ ικανοποείται.
Πράγματι,

$$\frac{19.2}{q^2} + \frac{8}{q} + 6 = \frac{19.2}{7^2} + \frac{8}{7} + 6 < 0.4 + 1.15 + 6 = 7.55 < 3\log_2 7 = 3\log_2 q$$

★ Αν $q - 1 \leq m < q^2$ τότε,

$$(22) < \frac{m}{3} + \sum_{d|q-1} \phi(d)\frac{2}{3} + \sum_{d|m} \phi(d)\frac{1}{6} = \frac{m}{2} + \frac{2}{3}(q-1)$$

και έτσι ζητάμε

$$2^{2.4} 2^{\frac{m}{2} + \frac{2}{3}(q-1)} < q^{\frac{m}{4}}$$

Δηλαδή θέλουμε,

$$2.4 + \frac{m}{2} + (q-1)\frac{2}{3} < \log_2 q^{\frac{m}{4}}$$

οπότε αρκεί

$$1.74 + \frac{2q}{3} < \frac{m}{4}\log_2 q - \frac{m}{2} = \frac{m}{4}(\log_2 q - 2)$$

και επειδή $m \geq q - 1$ τελικά αρκεί

$$\begin{aligned} 1.74 + \frac{2q}{3} &< \frac{q-1}{4}(\log_2 q - 2) \iff \\ \frac{6.96}{q-1} + \frac{8q}{3(q-1)} &< \log_2 q - 2 \iff \\ \frac{6.96}{q-1} + \frac{8}{3(q-1)} + \frac{8}{3} + 2 &< \log_2 q \qquad (24) \end{aligned}$$

Έστω οτι ικανοποιείται η (24) για κάποιο q και έχουμε $q' > q > 0$ τότε,

$$\frac{6.96}{q'-1} + \frac{8}{3(q'-1)} + \frac{14}{3} < \frac{6.96}{q-1} + \frac{8}{3(q-1)} + \frac{14}{3} < \log_2 q < \log_2 q'$$

Αρκεί λοιπόν να βρούμε κάποιο q που να ικανοποιεί την (24) και τότε $\forall q' > q$ θα ικανοποιείται.

Παρατηρούμε μετά απο δοκιμές ότι για $q = 33$ ικανοποείται.
Πράγματι,

$$\frac{6.96}{q-1} + \frac{8}{3(q-1)} + \frac{14}{3} < \frac{6.96}{32} + \frac{8}{96} + 4.7 < 0.22 + 0.09 + 4.7 = 5.01 < \log_2 33 = \log_2 q$$

Καθώς όμως θέλουμε το q να είναι δύναμη πρώτου συμεραίνουμε οτι $q \geq 37$

★ Αν $2 \leq m < q-1$ τότε,

$$(22) < \frac{m}{3} + \sum_{d|m} \phi(d)(\frac{2}{3}) + \sum_{d|m} \phi(d)(\frac{1}{6}) = \frac{m}{3} + \frac{2}{3}m + \frac{m}{6} = \frac{7m}{6}$$

και έτσι ζητάμε

$$2^{2.4} 2^{\frac{7m}{6}} < q^{\frac{m}{4}}$$

Δηλαδή θέλουμε,

$$\begin{aligned} 2.4 + \frac{7m}{6} &< \log_2 q^{\frac{m}{4}} \iff \\ 2.4 &< \frac{m}{4}\log_2 q - \frac{7m}{6} = \frac{m}{12}(3\log_2 q - 14) \end{aligned}$$

και επειδή $m \geq 2$ θέλουμε τελικά,

$$\begin{aligned} 2.4 &< 2(3\log_2 q - 14) \iff \\ 1.2 &< 3\log_2 q - 14 \iff \\ 15.2 &< 3\log_2 q \qquad (25) \end{aligned}$$

Έστω οτι ικανοποιείται η (25) για κάποιο q και έχουμε $q' > q > 0$ τότε,

$$15.2 < 3\log_2 q < 3\log_2 q'$$

Αρκεί λοιπόν να βρούμε κάποιο q που να ικανοποιεί την (25) και τότε $\forall q' > q$ θα ικανοποιείται.
Παρατηρούμε οτι,

$$5.06 < \frac{15.2}{3} < \log_2 q \iff q \geq 34$$

Καθώς όμως θέλουμε το q να είναι δύναμη πρώτου συμεραίνουμε οτι $q \geq 37$
Αν τώρα επιλέξουμε $e = 4$ στο λήμμα 3.5 θα έχουμε:

$$t \leq \frac{m}{4} + \sum_{d|(m,q-1)} \phi(d)(1 - \frac{1}{4}) + \sum_{d|(m,q^2-1)} \phi(d)(\frac{1}{2} - \frac{1}{4}) + \sum_{d|(m,q^3-1)} \phi(d)(\frac{1}{3} - \frac{1}{4})$$

$$< \frac{m}{4} + \sum_{d|q-1} \phi(d)(\frac{3}{4}) + \sum_{d|q^2-1} \phi(d)(\frac{1}{4}) + \sum_{d|(q^3-1)} \phi(d)(\frac{1}{12})$$

$$= \frac{m}{4} + (q-1)\frac{3}{4} + (q^2-1)\frac{1}{4} + (q^3-1)\frac{1}{12}$$

Έτσι θέλουμε :

$$\begin{aligned} 2^{2.4}2^{\frac{m}{4}+(q-1)\frac{3}{4}+(q^2-1)\frac{1}{4}+(q^3-1)\frac{1}{12}} &< q^{\frac{m}{4}} \iff \\ 2.4 + \frac{m}{4} + (q-1)\frac{3}{4} + (q^2-1)\frac{1}{4} + (q^3-1)\frac{1}{12} &< \log_2 q^{\frac{m}{4}} \iff \\ 2.4 + (q-1)\frac{3}{4} + (q^2-1)\frac{1}{4} + (q^3-1)\frac{1}{12} &< \frac{m}{4}\log_2 q - \frac{m}{4} \iff \\ 2.4 + (q-1)\frac{3}{4} + (q^2-1)\frac{1}{4} + (q^3-1)\frac{1}{12} &< \frac{m}{4}(\log_2 q - 1) \qquad (26) \end{aligned}$$

Έπομένως,

★ για $q = 3$

$$\begin{aligned} (26) = 2.4 + \frac{3}{2} + 2 + \frac{13}{6} &< \frac{m}{4}(\log_2 3 - 1) \iff \\ \frac{24.2}{3} &< \frac{m}{4}(\log_2 3 - 1) \iff \\ \frac{96.8}{3} &< m(\log_2 3 - 1) \iff \end{aligned}$$

Όμως $1.5 < \log_2 3$ επομένως αρκεί,

$$\begin{aligned} \frac{96.8}{3} &< m(1.5 - 1) \iff \\ 64,5 &< m \end{aligned}$$

★ για $q = 4$

$$\begin{aligned} (26) = 2.4 + \frac{9}{4} + \frac{15}{4} + \frac{21}{4} &< \frac{m}{4}(\log_2 4 - 1) \iff \\ \frac{54.6}{4} &< \frac{m}{4}(\log_2 4 - 1) \iff \\ 54.6 &< m(\log_2 4 - 1) \iff \\ 54.6 &< m \end{aligned}$$

★ για $q = 5$

$$\begin{aligned}(26) = 2.4 + 3 + 6 + \frac{31}{3} &< \frac{m}{4}(\log_2 5 - 1) \Longleftrightarrow \\ \frac{34.2}{3} &< \frac{m}{4}(\log_2 5 - 1) \Longleftrightarrow \\ \frac{136.8}{3} &< m(\log_2 5 - 1) \Longleftrightarrow\end{aligned}$$

Όμως $2.3 < \log_2 5$ επομένως αρκεί,

$$\begin{aligned}\frac{136.8}{3} &< m(2.3 - 1) \Longleftrightarrow \\ 35,1 &< m\end{aligned}$$

Επιλέγοντας τώρα $e = 5$ στο λήμμα 3.5 θα έχουμε:

$$t \leq \frac{m}{5} + \sum_{d|(m,q-1)} \phi(d)(1-\frac{1}{5}) + \sum_{d|(m,q^2-1)} \phi(d)(\frac{1}{2}-\frac{1}{5}) + \sum_{d|(m,q^3-1)} \phi(d)(\frac{1}{3}-\frac{1}{5}) + \sum_{d|(m,q^4-1)} \phi(d)(\frac{1}{4}-\frac{1}{5})$$

$$< \frac{m}{5} + \sum_{d|q-1} \phi(d)(\frac{4}{5}) + \sum_{d|q^2-1} \phi(d)(\frac{3}{10}) + \sum_{d|(q^3-1)} \phi(d)(\frac{2}{15}) + \sum_{d|(q^4-1)} \phi(d)(\frac{1}{20})$$

$$= \frac{m}{5} + (q-1)\frac{4}{5} + (q^2-1)\frac{3}{10} + (q^3-1)\frac{2}{15} + (q^4-1)\frac{1}{20}$$

Έτσι θέλουμε :

$$\begin{aligned}2^{2.4} 2^{\frac{m}{5} + (q-1)\frac{4}{5} + (q^2-1)\frac{3}{10} + (q^3-1)\frac{2}{15} + (q^4-1)\frac{1}{20}} &< q^{\frac{m}{4}} \Longleftrightarrow \\ 2.4 + \frac{m}{5} + (q-1)\frac{4}{5} + (q^2-1)\frac{3}{10} + (q^3-1)\frac{2}{15} + (q^4-1)\frac{1}{20} &< \log_2 q^{\frac{m}{4}} \Longleftrightarrow \\ 2.4 + (q-1)\frac{4}{5} + (q^2-1)\frac{3}{10} + (q^3-1)\frac{2}{15} + (q^4-1)\frac{1}{20} &< \frac{m}{4}\log_2 q - \frac{m}{5} \Longleftrightarrow \\ 2.4 + (q-1)\frac{4}{5} + (q^2-1)\frac{3}{10} + (q^3-1)\frac{2}{15} + (q^4-1)\frac{1}{20} &< \frac{m}{20}(5\log_2 q - 4) \qquad (27)\end{aligned}$$

Έπομένως,
★ για $q = 2$

$$\begin{aligned}(27) = 2.4 + \frac{4}{5} + \frac{9}{10} + \frac{14}{15} + \frac{15}{20} &< \frac{m}{20}(5\log_2 2 - 4) \Longleftrightarrow \\ \frac{347}{60} &< \frac{m}{20} \Longleftrightarrow \\ 115.7 &< m\end{aligned}$$

Στον επόμενο πίνακα συνοψίζουμε τις τιμές των q και m για τις οποίες αποδείξαμε ότι υπάρχει πρωταρχική κανονική βάση του $\mathbb{F}_{q^m}$ πάνω από το $\mathbb{F}_q$. Παρατητεί κανείς ότι η ύπαρξη τέτοιων βάσεων δεν έχει δειχθεί για πεπερασμένο πλήθος ζευγών (q, m).

$q = 2$	$m \geq 116$
$q = 3$	$m \geq 65$
$q = 4$	$m \geq 55$
$q = 5$	$m \geq 36$
$31 \geq q \geq 7$	$m \geq q^2$
$q \geq 37$	$\forall m$

Βιβλιογραφία

[1] S.D. Cohen and S. Huczynska. The primitive normal basis theorem—without a computer. *J. London Math. Soc.*, 2(67):41–56, 2003.

[2] H.W. Lenstra Jr. and R. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.

[3] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and Its Applications*. Addison-Wesley, Reading, Mass., 1983.