Γιωργος Τζανακης

ΤΟ ΘΕΩΡΗΜΑ ΤΟΥ DIRICHLET ΓΙΑ ΠΟΛΥΩΝΥΜΑ ΣΕ ΑΡΙΘΜΗΤΙΚΗ ΠΡΟΟΔΟ

Πτυχιακή Εργασία

Παρουσιάσθηκε στις 6-6-2008

Επιβλέπων Καθηγητής: Θεόδουλος Γαρεφαλάκης

Εξεταστική Επιτροπή: Ι. Αντωνιάδης, Θ. Γαρεφαλάκης, Μ. Παπαδημητράκης

Τμήμα Μαθηματικών

Πανεπιστήμιο Κρήτης - Ηράκλειο

2008

Εισαγωγή

Ένα κλασσικό θεώρημα της Θεωρίας Αριθμών είναι το εξής.

Θεώρημα του Dirichlet. *Υπάρχουν άπειροι πρώτοι σε κάθε ακολουθία της μορφής* $a + nb$*, όπου* a, b *θετικοί ακέραιοι πρώτοι μεταξύ τους και* $n > 0$.

Το θεώρημα με άλλα λόγια μας λέει οτι υπάρχουν άπειροι πρώτοι στην κλάση του $a \pmod b$. Λόγω της ομοιότητας των δακτυλίων $\mathbb{Z}$ και $\mathbb{F}_q[T]$, όπου $\mathbb{F}_q$ είναι το πεπερασμένο σώμα με q στοιχεία, πολλά θέματα της Θεωρίας Αριθμών, μεταφέρονται φυσιολογικά στην Θεωρία των Πεπερασμένων Σωμάτων. Μεταξύ αυτών είναι και το θεώρημα του Dirichlet.

Θεώρημα του Dirichlet για πολυώνυμα. *Αν* $a, m \in \mathbb{F}_q[T]$ *είναι πρώτα μεταξύ τους, υπάρχουν ανάγωγα πολυώνυμα στην κλάση του* $a \pmod m$.

Το μεγαλύτερο μέρος της εργασίας θα αφιερωθεί στην απόδειξη μιας ισχυρότερης (ποσοτικής) μορφής αυτού του θεωρήματος.

Δεύτερος στόχος της εργασίας είναι η εξέταση του παρακάτω ερωτήματος, της οποίας η απάντηση θα βασιστεί στο θεώρημα του Dirichlet.

Ερώτημα. *Αν* $a, m \in \mathbb{F}_q[T]$ *πρώτα μεταξύ τους, πόσα ανάγωγα πολυώνυμα της μορφής* $T^n + a_k T^k + a_{k-1} T^{k-1} + \cdots + a_1 T + a_0$ *υπάρχουν στην κλάση του* $a \pmod m$ *σε σχέση με το* k*;*

Ανάγωγα πολυώνυμα της παραπάνω μορφής με αρκούντως μικρό k χρειάζονται στον αλγόριθμο του Coppersmith για τον υπολογισμό Διακριτού Λογαρίθμου, ένα κρίσιμης σημασίας πρόβλημα για την Κρυπτογραφία. Συγκεκριμένη ποσοτική απάντηση θα δοθεί στην τελευταία ενότητα.

Η εργασία αυτή βασίστηκε στα κεφάλαια 1,2 και 4 του βιβλίου Number Theory in Funcion Fields του M. Rosen (Graduate Texts in Mathematics, Springer-Verlag, New York 2002).

Ευχαριστίες. Ευχαριστώ τους καθηγητές μου κ.κ. Ι. Αντωνιάδη, Θ. Γαρεφαλάκη και Μ. Παπαδημητράκη, που συμμετείχαν στην εξεταστική επιτροπή και με τις παρατηρήσεις τους βοήθησαν στη βελτίωση της εργασίας αυτής. Ιδιαιτέρως ευχαριστώ τον κ. Θ. Γαρεφαλάκη, υπό την επίβλεψη και την καθοδήγηση του οποίου εκπονήθηκε αυτή η εργασία. Η συνεργασία μαζί του υπήρξε μοναδική διδακτική εμπειρία και με επηρρέασε καθοριστικά στον δρόμο που θα ακολουθήσω από δω και πέρα.

Γιώργος Τζανάκης
Ιούλιος 2008

1 Πεπερασμένα σώματα-Συνοπτική εισαγωγή

Θα χρειαστεί να κάνουμε μια μικρή εισαγωγή στην Θεωρία των Πεπερασμένων Σωμάτων, με ορισμούς και προτάσεις που θα μας χρειαστούν για το υπόλοιπο της εργασίας.

Οι παρακάτω είναι γνωστές προτάσεις της άλγεβρας.

- Εαν p είναι πρώτος, ο δακτύλιος $\mathbb{Z}/p\mathbb{Z}$ είναι σώμα με p στοιχεία, το οποίο συμβολίζουμε $\mathbb{F}_p$.
- Το $\mathbb{F}_p[T] = \{a_nT^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0,\ a_i \in \mathbb{F}_p\}$ (ο δακτύλιος των πολυωνύμων πάνω από το $\mathbb{F}_p$) είναι ευκλείδια περιοχή.

Από τα παραπάνω, μπορούμε να ορίσουμε

$$\mathbb{F}_p[T]/f\mathbb{F}_p[T] = \{a + f\mathbb{F}_p[T],\ a \in \mathbb{F}_p[T]\}$$

όπου

$$a + f\mathbb{F}_p[T] = \{a + fh,\ h \in \mathbb{F}_p[T]\}\,.$$

Πρόταση 1.1. *Εαν το $f \in \mathbb{F}_p$ είναι ανάγωγο, τότε ο δακτύλιος $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$ είναι σώμα.*

Απόδειξη. Αρκεί να δείξουμε οτι κάθε μή μηδενικό στοιχείο του $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$ έχει αντίστροφο. Έστω $\bar{h} \in \mathbb{F}_p[T]/f\mathbb{F}_p[T]$ με $\bar{h} \neq \bar{0}$, δηλαδή $f \nmid h$. Αφού f ανάγωγο, είναι $(f, h) = 1$. Βρισκόμαστε σε ευκλείδια περιοχή, οπότε υπάρχουν $s, t \in \mathbb{F}_p[T]$ τέτοια ώστε $fs + th = 1 \Rightarrow th \equiv 1 \pmod f \Rightarrow \bar{t}\bar{h} = \bar{1}$. Άρα το $\bar{h}^-1$ υπάρχει και είναι το $\bar{t}$. □

Παρατήρηση 1.2. Έστω

$$H = \{a \in \mathbb{F}_p[T] \text{ με } a \equiv 0 \text{ ή } \deg a < \deg f\}\,.$$

Το H είναι ένα πλήρες σύστημα αντιπροσώπων του $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$, οπότε το $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$ έχει ακριβώς $p^{\deg f}$ στοιχεία. Από δω και πέρα, για πρακτικούς λόγους, δεν θα διαχωρίζουμε κλάσεις από αντιπροσώπους και θα χρησιμοποιούμε αποκλειστικά αντιπροσώπους από το H.

Για πρώτο p και φυσικό n, και ανάγωγο $f \in \mathbb{F}_p$ με $\deg f = n$, κατασκευάσαμε ενα πεπερασμένο σώμα με p^n στοιχεία. Το ερώτημα που φυσιολογικά τίθεται τώρα είναι εαν για κάθε πρώτο p και φυσικό n υπάρχει ανάγωγο $f \in \mathbb{F}_p$ με $\deg f = n$. Η απάντηση είναι θετική και προκύπτει από το θεώρημα (2.7) που θα δούμε αργότερα. Δηλαδή για κάθε πρώτο p και κάθε φυσικό n, υπάρχει σώμα με p^n στοιχεία.

Παρατήρηση 1.3. Υπενθυμίζουμε οτι χαρακτηριστική ενός σώματος $\mathbb{F}$ ονομάζεται ο μικρότερος φυσικός n ώστε $n \cdot 1 = 0$ και ορίζεται να είναι το 0 αν δεν υπάρχει τέτοιο n. Το $\mathbb{F}_p[T]/f\mathbb{F}_p[T]$ για f ανάγωγο, έχει χαρακτηριστική p. Ένα σώμα με μη μηδενική χαρακτηριστική, δεν μπορεί παρά να έχει χαρακτηριστική πρώτο αριθμό, αλλιώς θα είχε διαιρέτες του μηδενός.

Τώρα μένει να εξετάσουμε τι πληθάριθμο έχει το τυχαίο πεπερασμένο σώμα. Αυτό που έχουμε συμπεράνει είναι οτι υπάρχουν πεπερασμένα σώματα με πληθάριθμο κάθε δύναμη πρώτου. Με την επόμενη πρόταση της οποίας την απόδειξη θα παρουσιάσουμε πολύ συνοπτικά, θα δείξουμε οτι είναι μόνο αυτά.

Πρόταση 1.4. *Έστω πρώτος p και F σώμα με πεπερασμένο πλήθος στοιχείων, χαρακτηριστικής p. Τότε $|F| = p^n$ για κάποιον φυσικό n.*

Απόδειξη. Η απεικόνιση

$$\begin{array}{rccc} \theta: & \mathbb{F}_p & \longrightarrow & F \\ & a & \mapsto & a \cdot 1_F \end{array}$$

είναι μονομορφισμός, δηλαδή το F περιέχει μια ισομορφική εικόνα του $\mathbb{F}_p$. Το F είναι επέκταση του $\theta(\mathbb{F}_p)$, άρα είναι διανυσματικός χώρος πάνω από το $\theta(\mathbb{F}_p)$. Αφού το F είναι πεπερασμένο, θα έχει πεπερασμένη διάσταση (ως διανυσματικός χώρος) πάνω από το $\mathbb{F}_p$. Εαν $n = [F : \theta(\mathbb{F}_p)]$, το F έχει p^n όρους. □

Αποδεικνύεται οτι (σε σταθεροποιημένη αλγεβρική θήκη) τα σώματα με πληθάριθμο p^n είναι μοναδικά μέχρις ισομορφισμού. Από τα παραπάνω προκυπτει το επόμενο πόρισμα.

Πόρισμα 1.5. *Τα πεπερασμένα σώματα είναι ακριβώς αυτά με πληθάριθμο p^n, με p πρώτο και n φυσικό.*

Από δω και πέρα θα συμβολίζουμε με $\mathbb{F}_q = \mathbb{F}_{p^n}$ το πεπερασμένο σώμα με q στοιχεία και $\mathbb{A} = \mathbb{F}_q[T]$ τον δακτύλιο των πολυωνύμων πάνω από το $\mathbb{F}_q$.Εύκολα ελέγχει κανείς οτι ο $\mathbb{A}$ είναι ευκλείδια περιοχή.

Παρατηρούμε οτι στις αποδείξεις που χρησιμοποιήσαμε τον δακτύλιο $\mathbb{F}_p[T]$ μπορούμε να τον αντικαταστήσουμε με το $\mathbb{A}$ ξωρίς να αλλάξει κάτι άλλο, οπότε έχουμε οτι

- για $g \in \mathbb{A}$, το $\{r \in \mathbb{A},\ \deg(r) < \deg(g)\}$ είναι ένα πλήρες σύστημα αντιπροσώπων του δακτυλίου $\mathbb{A}/g\mathbb{A}$, συνεπώς $|\mathbb{A}/g\mathbb{A}| = q^{\deg g}$.
- ο $\mathbb{A}/g\mathbb{A}$ είναι σώμα αν και μόνο αν το g είναι ανάγωγο στο $\mathbb{A}$.

Ορισμός 1.6. (Συνάρτηση του Euler για πολυώνυμα) Έστω f ένα μη-μηδενικό πολυώνυμο του $\mathbb{A}$. Ορίζουμε $\Phi(f)$ να είναι ο αριθμός των στοιχείων της ομάδας $(\mathbb{A}/f\mathbb{A})^*$. Αφού το $\{r \in \mathbb{A},\ \deg(r) < \deg(g)\}$ είναι ένα πλήρες σύστημα αντιπροσώπων του $\mathbb{A}/f\mathbb{A}$ και r είναι μονάδα αν και μόνο αν είναι πρώτο ως προς το f, το $\Phi(f)$ δεν είναι παρά ο αριθμός των πρώτων ως προς το f πολυωνύμων, με βαθμό μικρότερο του $\deg(g)$.

Ορισμός 1.7. Έστω $g \in \mathbb{A}$. Ορίζουμε $|g| = q^{\deg(g)}$ αν $g \neq 0$ και $|g| = 0$ αν $g = 0$.

Εύκολα ελέγχει κανείς οτι η συνάρτηση $|\cdot| : \mathbb{A} \longrightarrow \mathbb{R}_{\geq 0}$ πληροί πράγματι τις απαραίτητες ιδιότητες για να είναι απόλυτη τιμή.

Ορίζοντας μια σειρά αρίθμισης στα (αριθμήσιμα το πλήθος) στοιχεία του $\mathbb{A}$, θα γράφουμε $\sum_g$, $\prod_g$ και θα εννούμε το άθροισμα/γινόμενο πάνω στα πολυώνυμα του $\mathbb{A}$¨, ενώ με $\sum_P$, $\prod_P$ θα εννούμε οτι η άθροιση και το γινόμενο γίνεται πάνω σε ανάγωγα.

2 Ο Τύπος του Euler για Πολλαπλασιαστικές Συναρτήσεις

Λέμε οτι ενα άπειρο γινόμενο της μορφής $\prod_{n\in\mathbb{N}}(1+a_n)$, $(a_n)_{n\in\mathbb{N}} \in \mathbb{C}$ συγκλίνει απόλυτως εαν συγκλίνει το γινόμενο $\prod_{n\in\mathbb{N}}(1+|a_n|)$. Ένα γνωστό Θεώρημα της Μιγαδικής Ανάλυσης μας λέει οτι το γινόμενο $\prod_{n\in\mathbb{N}}(1+a_n)$ συγκλίνει απολύτως εαν και μόνον αν συγκλίνει η σειρά $\sum_{n\in\mathbb{N}}|a_n|$. Από το γεγονός οτι τα στοιχεία του $\mathbb{A}$ είναι αριθμήσιμα το πλήθος, παίρνουμε το παρακάτω θεώρημα.

Θεώρημα 2.1. *Εστω $h : \mathbb{A} \longrightarrow \mathbb{C}$. Τότε, το γινόμενο $\prod_g(1+h(g))$ συγκλίνει απολύτως εαν και μόνον αν συγκλίνει η σειρά $\sum_g |h(g)|$*

Απο δω και πέρα θα ασχολούμαστε με συναρτήσεις που ανήκουν στην κατηγορία των *πολλαπλασιαστικών συναρτήσεων*.

Ορισμός 2.2. Μια συνάρτηση λ ορισμένη στα μονικά του $\mathbb{A}$ με πεδίο τιμών στο $\mathbb{C}$ λέγεται *πολλάπλασιαστική* εαν δεν ειναι η μηδενική και $\lambda(f_1f_2) = \lambda(f_1)\lambda(f_2)$ για κάθε f_1, f_2 με $\gcd(f_1, f_2) = 1$ και *πλήρως πολλαπλασιαστική* αν η παραπάνω σχέση ισχύει για κάθε ζεύγος f_1, f_2, ανεξάρτητα αν αυτά ειναι πρώτα μεταξύ τους ή οχι.

Παράδειγμα. Η συνάρτηση με τύπο $\lambda(g) = \frac{1}{|g|^s}$, $s \in \mathbb{C}$ ειναι πλήρως πολλαπλασιαστική.

Στην πορεία θα χρησιμοποιήσουμε το παρακάτω θεώρημα για τις πλήρως πολλαπλασιαστικές συναρτήσεις, το οποίου η απόδειξη είναι εύκολη.

Θεώρημα 2.3. *Αν η συνάρτηση λ είναι πολλαπλασιαστική και $\lambda(1) = 1$ τότε αυτή είναι πλήρως πολλαπλασιαστική αν και μόνο άν $\lambda(P^k) = \lambda(P)^k$ για κάθε ανάγωγο P και ακέραιο $k \geqslant 1$.*

Θα διατυπώσουμε τώρα το Θεώρημα που μας δίνει τον τύπο του Euler για πολλαπλασιαστικές συναρτήσεις.

Θεώρημα 2.4. *(Τύπος του Euler για πολλαπλασιαστικές συναρτήσεις) Εστω πολλαπλασιαστική συνάρτηση $f : \mathbb{A} \longrightarrow \mathbb{C}$ και εστω οτι η $\sum_g |f(g)|$ συγκλίνει. Τότε*

$$\sum_g f(g) = \prod_P (1 + f(P) + f(P^2) + \cdots).$$

Εαν επιπλέον η f είναι πλήρως πολλαπλασιαστική, τότε

$$\sum_g f(g) = \prod_P (1 - f(P))^{-1}.$$

Απόδειξη. Για σταθερό $g \in \mathbb{A}$ είναι

$$\left\{g^i, i = 1, 2, ...\right\} \subset \left\{g' : g' \in \mathbb{A} \text{ μονικό } \right\}.$$

Επειδή εξ υποθέσεως η σειρά $\sum_{g'} |f(g')|$ συγκλίνει, έπεται ότι και η $\sum_{i=1}^{\infty} f(g^i)$ συγκλίνει. Άρα, για καθε μονικό ανάγωγο $g \in \mathbb{A}$ έχει νόημα να ορίσουμε την συνάρτηση $h(g) = \sum_{i=1}^{\infty} f(g^i)$. Προφανώς

$$\bigcup_P \left\{P^i : i = 1, 2, 3, ...\right\} \subset \left\{g : g \in \mathbb{A} \text{ μονικό } \right\}.$$

Επειδή η σειρα $\sum_g f(g)$ είναι απολύτως συγκλίνουσα, έπεται ότι η σειρά $\sum_P \sum_{i=1}^{\infty} |f(P^i)|$ συγκλίνει, δηλαδή η $\sum_P |h(P)|$ συγκλίνει.

Εφαρμόζοντας λοιπόν το θεώρημα (2.1) προκύπτει οτι ισοδύναμα συγκλίνει απολύτως και το $\prod_P (1 + h(P))$. Για να δείξουμε την ζητούμενη ισότητα, πρέπει να παρατηρήσουμε τα εξής:

$$\prod_P (1 + f(P) + f(P^2) + \cdots) = \lim_{n \to \infty} \prod_{|P| \leq n} (1 + f(P) + f(P^2) + \cdots)$$

και

$$\prod_{|P| \leq n} (1 + f(P) + f(P^2) + \cdots) = \sum_{\substack{g \\ P|g \Rightarrow |P| \leq n}} f(g) \tag{1}$$

λόγω της πολλαπλασιαστικότητας της f και της μονοσήμαντης ανάλυσης του κάθε g σε πρώτους παράγοντες. Οπότε, παίρνοντας στην (1) το όριο καθώς n τείνει στο άπειρο, έχουμε

$$\prod_P (1 + f(P) + f(P^2) + \cdots) = \sum_g f(g)$$

και έχουμε αποδείξει το πρώτο σκέλος του Θεωρήματος.

Όταν τώρα η f είναι πλήρως πολλαπλασιαστική, τότε από το θεώρημα (2.3), ισχύει για κάθε μονικό ανάγωγο $P \in \mathbb{A}$ οτι

$$1 + f(P) + f(P^2) + \cdots = 1 + f(P) + f(P)^2 + \cdots$$

Επειδή η τελευταία σειρά συγκλίνει απολύτως, πρέπει να ισχύει $|f(P)| < 1$ και επομένως

$$1 + f(P) + f(P^2) + \cdots = (1 - f(P))^{-1}.$$

Άρα, για μια πλήρως πολλαπλασιαστική f έχουμε

$$\sum_g f(g) = \prod_P (1 - f(P))^{-1}$$

□

Εστω $s \in \mathbb{C}$. Τότε

$$\sum_g |g|^{-s} = \sum_{m=0}^{\infty} \sum_{\substack{g \\ \deg(g)=m}} |g|^{-s}.$$

Παρατηρώντας οτι υπάρχουν q^m τον αριθμό μονικά πολυώνυμα βαθμού m πάνω απο το $\mathbb{A}$, βλέπουμε οτι το τελευταίο άθροισμα ισούται με

$$\sum_{m=0}^{\infty} q^m q^{-sm} = \sum_{m=0}^{\infty} q^{m(1-s)}$$

Η τελευταία δυναμοσειρά συγκλίνει αν και μονο αν $\Re(s) > 1$, οπότε το ίδιο ισχύει και για την $\sum_g |g|^{-s}$. Η σειρά αυτή είναι το ανάλογο της συνάρτησης ζ του *Riemann* στους ακεραίους και παίζει εξίσου σπουδαίο ρόλο στα πεπερασμένα σώματα.

Ορισμός 2.5. *(Η Συνάρτηση ζ για Πολυώνυμα)*

Η συνάρτηση ζήτα του $\mathbb{A}$ συμβολίζεται $\zeta_{\mathbb{A}}$ και ορίζεται ως εξής:

$$\zeta_{\mathbb{A}}(s) = \sum_g \frac{1}{|g|^s} \quad s \in \mathbb{C},\ \Re(s) > 1.$$

Με βάση το Θεώρημα 2.4 και με δεδομένο οτι η $|g|^{-s}$ είναι πλήρως πολλαπλασιαστική, θα βγάλουμε εναν χρήσιμο τύπο (Τύπος του Euler) για την συνάρτηση $\zeta_{\mathbb{A}}$.

Πρόταση 2.6. *(Τύπος του Euler για την συνάρτηση ζ)*

$$\zeta_{\mathbb{A}}(s) = \prod_{P}(1 - \frac{1}{|P|^s})^{-1} \quad \Re(s) > 1$$

Απόδειξη. Εφαρμόζουμε το θεώρημα (2.4) για την πλήρως πολλαπλασιαστική $f : \mathbb{A} \longrightarrow \mathbb{C}$ με $f(g) = \frac{1}{|g|^s},\ \Re(s) > 1.$ □

Έχοντας εισάγει την συνάρτηση $\zeta_{\mathbb{A}}$, θα κλείσουμε αυτήν την ενότητα με ενα πολύ χρήσιμο συμπέρασμα. Δοθέντος ενός $n \in \mathbb{N}$, θα βρούμε τον αριθμό των μονικών αναγώγων πολυωνύμων βαθμού n πάνω απο το $\mathbb{A}$, χρησιμοποιόντας την παραπάνω πρόταση.

Ας συμβολίσουμε με a_d τον αριθμό των μονικών αναγώγων βαθμού d. Τότε απο την πρόταση (2.6) προκύπτει οτι

$$\zeta_{\mathbb{A}}(s) = \prod_{d=1}^{\infty}(1 - q^{-ds})^{-a_d}. \tag{2}$$

Παρατηρούμε οτι υπάρχουν ακριβώς q^n μονικά πολυώνυμα βαθμού n στο $\mathbb{A}$, επομένως

$$\sum_{\deg(f)\leq d} |f|^{-s} = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots + \frac{q^d}{q^{ds}},$$

συνεπώς για $\Re(s) > 1$

$$\zeta_{\mathbb{A}}(s) = \lim_{d\to\infty} \sum_{\deg(g)\leq d} |g|^{-s} = \lim_{d\to\infty}(1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots + \frac{q^d}{q^{ds}})$$

$$= \sum_{d=0}^{\infty} q^{d(1-s)} = \frac{1}{1 - q^{1-s}} \tag{3}$$

Στις (2) και (3), κάνουμε την αντικατάσταση $u = q^{-s}$ και παρατηρούμε οτι $|u| < \frac{1}{q}$ αν και μόνο αν $\Re(s) > 1$, οπότε

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty}(1 - u^d)^{-a_d}.$$

Λογαριθμίζουμε και τα δύο μέλη και παίρνουμε

$$\log(\frac{1}{1-qu}) = \sum_{d=1}^{\infty} -a_d \log(1-u^d).$$

Παραγωγίζουμε ως προς u και η ισότητα γίνεται

$$\frac{q}{1-qu} = \sum_{d=1}^{\infty} a_d \frac{du^{d-1}}{1-u^d}$$

και πολλαπλασιάζοντας με u.

$$\frac{qu}{1-qu} = \sum_{d=1}^{\infty} a_d \frac{du^d}{1-u^d} \tag{4}$$

Και τα δύο μέλη της παραπάνω ισότητας, μπορούν να εκφραστούν ως δυναμοσειρές του u. Συγκεκριμένα έχουμε

$$\frac{qu}{1-qu} = \sum_{n=0}^{\infty} (qu)^{n+1} = \sum_{n=1}^{\infty} q^n u^n \tag{5}$$

και

$$\frac{u^d}{1-u^d} = u^d \sum_{k=0}^{\infty} u^{dk} = \sum_{k=0}^{\infty} u^{d(k+1)} = \sum_{k=1}^{\infty} u^{dk}$$

οπότε

$$\sum_{d=1}^{\infty} a_d \frac{du^d}{1-u^d} = \sum_{d=1}^{\infty} da_d \sum_{k=1}^{\infty} u^{dk} = \sum_{d=1}^{\infty} \sum_{k=1}^{\infty} da_d u^{dk} = \sum_{n=1}^{\infty} (\sum_{d|n} da_d) u^n \tag{6}$$

Λαμβάνοντας υπ'οψιν τις (4),(5) και (6) , παίρνουμε την εξίσωση

$$\sum_{d|n} da_d = q^n.$$

Ετσι λοιπόν, απο τον τύπο αντιστροφής του Möbius προκύπτει οτι

$$a_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Το παρακάτω Θεώρημα, μας δείχνει πιο ξεκάθαρα την τάξη μεγέθους του a_n.

Θεώρημα 2.7. *Έστω a_n ο αριθμός των μονικών αναγώγων πολυωνύμων βαθμού n του $\mathbb{A}$. Τότε*

$$|a_n - \frac{q^n}{n}| \leqslant \frac{q^{\frac{n}{2}}}{\frac{n}{2}}.$$

Απόδειξη. Αφού $|\mu(d)| = 1$ ή 0, έχουμε

$$a_n = \frac{1}{n}\sum_{d|n} \mu(d) q^{\frac{n}{d}} \Rightarrow |a_n - \frac{q^n}{n}| = \frac{1}{n}|\sum_{\substack{d|n \\ d \geqslant 2}} \mu(d) q^{\frac{n}{d}}| \leqslant \frac{1}{n} \sum_{\substack{d|n \\ d \geqslant 2}} |\mu(d) q^{\frac{n}{d}}|$$

$$\leqslant \frac{1}{n} \sum_{\substack{d|n \\ d \geqslant 2}} q^{\frac{n}{d}} \leqslant \frac{1}{n} \sum_{i=1}^{[\frac{n}{2}]} q^i = \frac{1}{n} q \frac{q^{[\frac{n}{2}]} - 1}{q-1} \leqslant \frac{q^{\frac{n}{2}}}{\frac{n}{2}}.$$

□

3 Χαρακτήρες και Σειρές Dirichlet

Ενα απαραίτητο εργαλείο για τη συνέχεια είναι οι Χαρακτήρες και οι Σειρές Dirichlet, τα οποία θα εισάγουμε σε αυτήν την ενότητα.

Ορισμός 3.1. Έστω $m \in \mathbb{A}$ θετικού βαθμού. Ορίζουμε τον Χαρακτήρα Dirichlet modulo m να είναι μια συνάρτηση $\mathbb{A} \longrightarrow \mathbb{C}$ τέτοια ώστε

- $\chi(a + bm) = \chi(a)$ για κάθε $a, b \in \mathbb{A}$
- $\chi(a)\chi(b) = \chi(ab)$ για κάθε $a, b \in \mathbb{A}$
- $\chi(a) \neq 0 \Leftrightarrow (a, m) = 1$

Απο τον ορισμό του, ένας χαρακτήρας Dirichlet είναι μια πλήρως πολλαπλασιαστική συνάρτηση.

Έστω X_m το σύνολο των χαρακτήρων Dirichlet modulo m. Ορίζουμε τον πολλαπλασιασμό δύο στοιχείων χ, ψ του X_m να δίνεται από τον τύπο $\chi \cdot \psi(a) = \chi(a)\psi(a)$, πράξη που καθιστά το X_m ομάδα. Ουδέτερο στοιχείο της είναι ο τετριμμένος χαρακτήρας χ_0 με $\chi_0(a) = 1$ αν $(a, m) = 1$ και $\chi_0(a) = 0$ αλλιώς και το αντίστροφο του στοιχείου χ δίνεται απο το $\chi^{-1}(a) = \chi(a)^{-1}$.
Θα εισάγουμε τωρα την έννοια του χαρακτήρα μιας πεπερασμένης αβελιανής ομάδας.

Ορισμός 3.2. Έστω $\mathbb{G}$ πεπερασμένη αβελιανή ομάδα. Ένας ομομορφισμός $\chi : \mathbb{G} \longrightarrow \mathbb{C}^*$ λέγεται *χαρακτήρας* της $\mathbb{G}$.

Ορίζουμε τον πολλαπλασιασμό των χαρακτήρων μιας πεπερασμένης αβελιανής ομάδας $\mathbb{G}$ όπως τον πολλαπλασιάσμό των χαρακτήρων Dirichlet: Αν χ και ψ χαρακτήρες, τότε $\chi\psi$ ορίζουμε τον χαρακτήρα με $\chi\psi(g) = \chi(g)\psi(g)$. Το συνολο των χαρακτήρων της $\mathbb{G}$ με αυτόν τον πολλαπλασιασμό και ουδέτερο στοιχείο τον τετριμμένο χαρακτήρα, αποτελεί ομάδα, την οποία συμβολίζουμε $\widehat{\mathbb{G}}$.

Πρόταση 3.3. *Έστω $\mathbb{G}$ πεπερασμένη αβελιανή ομάδα. Τα παρακάτω είναι γνωστά απο τη Θεωρία Ομάδων.*

- *Υπάρχουν $|\mathbb{G}|$ το πλήθος χαρακτήρες της $\mathbb{G}$.*
- *Αν χ χαρακτήρας της $\mathbb{G}$ τότε $|\chi(a)| = 1$ για κάθε $a \in \mathbb{G}$.*
- *Αν χ και ψ χαρακτήρες της $\mathbb{G}$ τότε*

$$\sum_{g\in\mathbb{G}} \chi(g)\overline{\psi(g)} = |\mathbb{G}|\ \delta(\chi,\psi) \quad \text{και} \quad \sum_{\chi\in\widehat{\mathbb{G}}} \chi(g_1)\overline{\chi(g_2)} = |\mathbb{G}|\ \delta(g_1,g_2)$$

οπου $\delta(a,b) = 0$ αν $a \neq b$ και $\delta(a,b) = 1$, αλλιώς.

Θα δείξουμε οτι οι παραπάνω ιδιότητες ισχύουν και για τους χαρακτήρες Dirichlet . Ακόμα γενικότερα, θα δούμε οτι η ομάδα των χαρακτήρων Dirichlet modulo m ενος σώματος είναι ισόμορφη με την ομάδα των χαρακτήρων μιας πεπερασμένης αβελιανής ομάδας.

Η ομάδα $(\mathbb{A}/m\mathbb{A})^*$ των μονάδων του $\mathbb{A}/m\mathbb{A}$ είναι αβελιανή λόγω της αντιμεταθετικότητας των στοιχείων του $\mathbb{A}/m\mathbb{A}$ και πεπερασμένη καθώς αν $\mathbb{A} = \mathbb{F}_q[T]$, έχει ακριβώς $q^{\deg(m)} - 1$ στοιχεία.

Θεώρημα 3.4. *Η ομάδα X_m των χαρακτήρων Dirichlet modulo m είναι ισόμορφη με την $\widehat{(\mathbb{A}/m\mathbb{A})^*}$*

Απόδειξη. Ορίζουμε την απεικόνιση

$$\theta : X_m \longrightarrow \widehat{(\mathbb{A}/m\mathbb{A})^*}$$

$$\chi \longmapsto \widehat{\chi}$$

με $\hat{\chi}(\hat{a}) = \chi(a)$, αν $(a,m) = 1$.

Θα δείξουμε οτι η θ είναι ισομορφισμός. Η τιμή του $\hat{\chi}$ δεν εξαρτάται από την επιλογή του αντιπροσώπου a της κλάσεως $\hat{a}$, οπότε η απεκόνιση κατ'αρχάς είναι καλώς ορισμένη.

Είναι ομομορφισμός: Για $\chi, \psi \in X_m$ έχουμε $\theta(\chi\psi) = \widehat{\chi\psi} = \hat{\chi}\hat{\psi} = \theta(\chi)\theta(\psi)$.

Είναι $1-1$: Έστω $\theta(\chi) = 1$, δηλαδή $\hat{\chi}(\hat{a}) = 1$ για κάθε $(a, m) = 1$. Τότε από τον ορισμό της θ, $\chi(a) = 1$ για κάθε $(a, m) = 1$, δηλαδή ο χ είναι ο τετριμμένος χαρακτήρας και $\ker(\theta) = \{1\}$.

Είναι επί: Έστω $\psi \in (\widehat{\mathbb{A}/m\mathbb{A}})^*$. Θα δούμε ότι $\psi = \hat{\chi}$, για κάποιο $\chi \in X_m$. Ορίζω χ την απεικόνιση απο το $\mathbb{A}$ στο $\mathbb{C}$ με $\chi(a) = \psi(\hat{a})$ όταν $(a, m) = 1$ και $\chi(a) = 0$ αλλιώς. Η απεικόνιση αυτή είναι προφανώς χαρακτήρας και $\psi = \theta(\chi)$.

□

Πρόταση 3.5. *Υπάρχουν $\Phi(m)$ το πλήθος χαρακτήρες Dirichlet modulo m*

Απόδειξη. Απο το Θεώρημα (3.4) έχουμε $|(\widehat{\mathbb{A}/m\mathbb{A}})^*| = |X_m|$ και από το πρώτο μέρος της πρότασης (3.3), $|(\widehat{\mathbb{A}/m\mathbb{A}})^*| = |(\mathbb{A}/m\mathbb{A})^*| = \Phi(m)$. □

Επίσης θα χρησιμοποιήσουμε επανειλλημένως την ακόλουθη πρόταση.

Πρόταση 3.6. $|\chi(a)| = 1$ *αν* $(a, m) = 1$ *και* $|\chi(a)| = 0$ *αλλιώς.*

Απόδειξη. Η απόδειξη προκύπτει άμεσα λαμβάνοντας υπ'όψιν τον ισομορφισμό του θεωρήματος (3.4) και το δεύτερο σκέλος του θεωρήματος (3.3). □

Εαν $\chi \in X_m$, ορίζουμε τον συζυγή χαρακτήρα Dirichlet $\overline{\chi}$ να δίνεται από την σχέση $\overline{\chi}(a) = \overline{\chi(a)}$. Έχουμε την ακόλουθη σημαντική πρόταση.

Πρόταση 3.7. *Έστω χ και ψ δύο χαρακτήρες Dirichlet modulo m και $a, b \in \mathbb{A}$ πρώτα ως προς το m. Τότε*

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\,\delta(\chi, \psi)$
2. $\sum_\chi \chi(a)\overline{\chi(b)} = \Phi(m)\,\delta(a, b)$

   όπου $\delta(x, y) = 0$ εαν $x \neq y$ και $\delta(x, y) = 1$ αλλιώς.

Το πρώτο άθροισμα είναι πάνω απο κάθε $a \in \mathbb{A}/m\mathbb{A}$ και το δεύτερο πάνω απο όλους τους χαρακτήρες Dirichlet modulo m.

Απόδειξη. Η απόδειξη ποκύπτει άμεσα λαμβάνοντας υπ'όψιν τον ισομορφισμό του θεωρήματος (3.4),το θεώρημα (3.5) και το τρίτο σκέλος του θεωρήματος (3.3). □

Πόρισμα 3.8.

1. $\sum_a \chi(a) = 0$ *για κάθε* $\chi \in X_m$ *με* $\chi \neq \chi_0$

2. $\sum_\chi \chi(a) = 0$ *για κάθε* $a \in \mathbb{A}/m\mathbb{A}$ *με* $a \neq 1$

Το πρώτο άθροισμα είναι πάνω απο κάθε $a \in \mathbb{A}/m\mathbb{A}$ *και το δεύτερο πάνω απο όλους τους χαρακτήρες Dirichlet modulo* m.

Απόδειξη. Εφαρμόζουμε την πρόταση (3.7) για $\psi = \chi_0$, $\chi \neq \psi$ και $b = 1,\ a \neq 1$ αντιστοίχως. □

Έχοντας ορίσει τους χαρακτήρες Dirichlet είμαστε έτοιμοι να μιλήσουμε και για τις σειρές Dirichlet. Ξέρουμε οτι η συνάρτηση $\zeta_{\mathbb{A}}(s)$ που ορίσαμε στην πρώτη ενότητα συγκλίνει για $\Re(s) > 1$. Εφαρμόζοντας την Πρόταση (3.6) έχουμε

$$\sum_f \frac{|\chi(f)|}{|f|^s} \leq \sum_f \frac{1}{|f|^s} = \zeta_{\mathbb{A}}(s).$$

Συνεπώς και η σειρά $\sum_f \frac{|\chi(f)|}{|f|^s}$ συγκλίνει απολύτως για $\Re(s) > 1$.

Ορισμός 3.9. Εστω χ ένας χαρακτήρας Dirichlet modulo m. Η σειρά Dirichlet που αντιστοιχεί στον χ, είναι μια συνάρτηση με πεδίο ορισμού το $\mathbb{C}$, συμβολίζεται $L(s, \chi)$ και ορίζεται από την σειρά

$$L(s, \chi) = \sum_f \frac{\chi(f)}{|f|^s} \quad s \in \mathbb{C},\ \Re(s) > 1$$

Επίσης, όπως και για την συνάρτηση $\zeta_{\mathbb{A}}$, θα βγάλουμε τον αντίστοιχο τύπο του Euler για μια σειρά Dirichlet.

Πρόταση 3.10. *Για κάθε χαρακτήρα Dirichlet* $\chi \pmod m$ *ισχύει*

$$L(s, \chi) = \prod_P (1 - \frac{\chi(P)}{|P|^s})^{-1}$$

Απόδειξη. Η ισότητα προκύπτει αμέσως απο το Θεώρημα (2.4) και απο το γεγονός οτι ένας Χαρακτήρας Dirichlet modulo m είναι πλήρως πολλαπλασιαστική συνάρτηση. □

Οι σειρές Dirichlet για πολυώνυμα έχουν οριστεί σε αναλογία με τις σειρές Dirichlet για ακεραίους στην Θεωρία Αριθμών. Ωστόσο, έχουν μια εξαιρετικά βολική ιδιότητα που δεν έχουν οι τελευταίες. Συγκεκριμένα έχουμε την ακόλουθη πρόταση.

Πρόταση 3.11. *Εαν* χ *είναι ένας μή-τετριμμένος χαρακτήρας Dirichlet modulo* m*, τοτε η σειρά Dirichlet* $L(s, \chi)$ *είναι πολυώνυμο του* q^{-s} *βαθμού το πολύ* $\deg(m) - 1$ *με συντελεστές από το* $\mathbb{C}$.

Απόδειξη. Έχουμε

$$L(s,\chi) = \sum_f \frac{\chi(f)}{|f|^s} = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}$$

όπου

$$A(n,\chi) = \sum_{\deg(f)=n} \chi(f).$$

Το ζητούμενο θα προκύψει εαν δείξουμε ότι $A(n,\chi) = 0$ για όλα τα $n \geqslant \deg(m)$. Έστω λοιπόν $n \geqslant \deg(m)$. Εαν $\deg(f) = n$, μπορούμε να γράψουμε το f στην μορφή $f = hm + r$ όπου $1 \leq \deg(r) \leq \deg(m)$ ή $r = 0$ και h πολυώνυμο βαθμού $n - \deg(m) \geqslant 0$, του οποίου ο μεγιστοβάθμιος όρος έχει συντελεστή $\mathrm{sgn}(m)^{-1}$. Επίσης κάθε πολυώνυμο βαθμού $n \geqslant \deg(m)$ μπορεί να γραφτεί έτσι με μοναδικό τρόπο. Το h μπορεί να επιλεχθεί με $q^{n-\deg(m)}$ τρόπους. Έτσι,

$$A(n,\chi) = \sum_r \sum_h \chi(hm+r) = \sum_r \sum_h \chi(r) = q^{n-\deg(m)} \sum_h \chi(r) = 0$$

απο την πρόταση (3.8). □

Για πρακτικούς λόγους θα γράφουμε $L^*(u,\chi)$ και θα εννοούμε $L(s,\chi)$ όπου $u = q^{-s}$. Απο την παραπάνω πρόταση, προκύπτει οτι το $L^*(u,\chi)$ είναι πολυώνυμο του u.

4 Το Θεώρημα του Dirichlet στα πεπερασμένα σώματα

Το ερώτημα με το οποίο θα ασχοληθούμε σε αυτήν την ενότητα είναι το εξής: Δοθέντων στοιχείων a και m του $\mathbb{A}$ με $(a,m) = 1$ και φυσικού n, ζητάμε τον αριθμό των μονικών αναγώγων πολυωνύμων $P \in \mathbb{A}$ με $P \equiv a \pmod m$ και $\deg(P) = n$. Το αντίστοιχο ερώτημα για τους φυσικούς αριθμούς απάντησε ο Dirichlet. Εμείς θα δείξουμε το ανάλογο Θεώρημα του Dirichlet για πολυώνυμα σε μια πιο ισχυρή μορφή. Ενώ το Θεώρημα του Dirichlet μας δίνει μια ιδέα για την πυκνότητα αυτών των πολυωνύμων, εμείς θα κάνουμε μια συγκεκριμένη, πιο ακριβή εκτίμηση. Στις δύο πρώτες ενότητες αυτής της εργασίας παρουσιάσαμε ο,τι μας ήταν απαραίτητο για να ασχοληθούμε με αυτό το θεώρημα, ωστόσο πριν προχωρήσουμε στην απόδειξη θα πρέπει να δούμε ένα λήμμα και να κάνουμε μερικούς υπολογισμούς. Είναι επίσης απαραίτητο το Θεώρημα του A. Weil το οποίο θα χρησιμοποίησουμε χωρίς απόδειξη.

Λήμμα 4.1. *Έστω χ ενας μη-τετριμμένος χαρακτήρας Dirichlet modulo m, $\alpha \in \mathbb{C}$, $k \in \mathbb{N}$ και $u = q^{-s}$ με $|u|^k < |\alpha|^{-1}$. Τότε*

$$u\frac{d}{du}\log(1-\alpha u^k) = -k\sum_{i=1}^{\infty}\alpha^i u^{ki} \tag{7}$$

Απόδειξη. Έχουμε

$$u\frac{d}{du}\log(1-\alpha u^k) = u\frac{-\alpha k u^{k-1}}{1-\alpha u^k} = -\alpha k u^k \frac{1}{1-\alpha u^k} = -\alpha k u^k \sum_{i=0}^{\infty}\alpha^i u^{ik}$$

$$= -k\sum_{i=1}^{\infty}\alpha^i u^{ki}.$$

□

Λήμμα 4.2. *Έστω χ ενας μη-τετριμμένος χαρακτήρας Dirichlet modulo m, $a \in \mathbb{A}$ και $u = q^{-s}$. Τότε για κατάλληλο s*

$$u\frac{d}{du}\log(L^*(u,\chi)) = \sum_{n=0}^{\infty} c_n(\chi)u^n$$

με

$$c_n(\chi) = -\sum_{k=1}^{l-1}\alpha_k(\chi)^n = \sum_{\substack{k,\,P \\ k\deg(P)\,=\,n}} \deg(P)\chi(P)^k$$

όπου $\alpha_k(\chi)$ τα αντίστροφα των ριζών του πολυωνύμου $L^*(u,\chi)$.

Απόδειξη. Το $L^*(u,\chi)$ έχει σταθερό όρο

$$\sum_{\deg(f)=0}\chi(f) = \sum_{a\in\mathbb{F}_q^*} = \sum_{a=1}\chi(a) = 1$$

Οπότε μπορούμε να γράψουμε

$$L^*(u,\chi) = \prod_{i=1}^{l-1}(1-\alpha_i(\chi)u)$$

όπου $l \leq \deg(m)$. Για κατάλληλη επιλογή του u, από την (7) για $k = 1$, έχουμε

$$u\frac{d}{du}\log(L^*(u,\chi)) = u\frac{d}{du}\log\prod_{k=1}^{l-1}(1-\alpha_k(\chi)u) = \sum_{k=1}^{l-1}u\frac{d}{du}\log(1-\alpha_k(\chi)u)$$

$$= -\sum_{k=1}^{l-1}\sum_{n=1}^{\infty}\alpha_k(\chi)^n u^n = \sum_{n=1}^{\infty}(-\sum_{k=1}^{l-1}\alpha_k(\chi)^n)u^n$$

οπότε προκύπτει η πρώτη ισότητα που θέλαμε να δείξουμε:

$$c_n(\chi) = -\sum_{k=1}^{l-1}\alpha_k(\chi)^n.$$

Επίσης, απο την πρόταση (3.10) (τύπος του Euler) για τις σειρές Dirichlet έχουμε

$$L(s,\chi) = \prod_{P}(1-\chi(P)|P|^{-s})^{-1} = \prod_{P\nmid m}(1-\chi(P)|P|^{-s})^{-1}$$

$$= \prod_{d=1}^{\infty}\prod_{\substack{P\nmid m\\ deg(P)=d}}(1-\chi(P)q^{-ds})^{-1}$$

οπότε

$$L^*(u,\chi) = \prod_{d=1}^{\infty}\prod_{\substack{P\nmid m\\ deg(P)=d}}(1-\chi(P)u^{d})^{-1}$$

και

$$u\frac{d}{du}\log(L^*(u,\chi)) = u\frac{d}{du}\log(\prod_{d=1}^{\infty}\prod_{\substack{P\nmid m\\ deg(P)=d}}(1-\chi(P)u^{d})^{-1})$$

$$= \sum_{d=1}^{\infty}\sum_{\substack{P\nmid m\\ deg(P)=d}} -u\frac{d}{du}\log(1-\chi(P)u^d).$$

Για κατάλληλη επιλογή του u και λαμβάνοντας υπ'οψιν το λήμμα (7), το τελευταίο διπλό άθροισμα είναι ίσο με

$$\sum_{d=1}^{\infty}\sum_{\substack{P\nmid m\\ deg(P)=d}} d\sum_{k=1}^{\infty}\chi(P)^k u^{dk} = \sum_{d=1}^{\infty}(\sum_{d|n}\sum_{\substack{P\nmid m\\ deg(P)=d}} d\chi(P)^{\frac{n}{d}})u^n.$$

Οπότε

$$c_n(\chi) = \sum_{\substack{P\nmid m\\ deg(P)=d}}\sum_{d|n} d\chi(P)^{\frac{n}{d}} = \sum_{\substack{k,\,P\\ kdeg(P)\,=\,n}}\deg(P)\chi(P)^k$$

□

Άλλο ένα εργαλείο που θα χρειαστούμε είναι το ανάλογο της υπόθεσης του Riemann για σώματα συναρτήσεων πάνω απο ένα πεπερασμένο σώμα. Αυτό μας λέει οτι όλες οι ρίζες του πολυωνύμου $L(s,\chi)$ έχουν απόλυτη τιμή είτε 1 είτε $1/\sqrt{q}$, συνεπώς οι $\alpha_k(\chi)$ που ορίσαμε παραπάνω, έχουν απόλυτη τιμή 1 ή $\sqrt{q}$. Αυτό είναι συνέπεια του θεωρήματος του A. Weil το οποίο απέδειξε το 1948.

Πόρισμα 4.3. *Εαν χ χαρακτήρας Dirichlet modulo m και $\deg(m) = M$, τότε*

$$|c_n(\chi)| \leq (M-1)q^{\frac{n}{2}}$$

όπου c_n όπως παραπάνω.

Απόδειξη. Από το θεώρημα τού Weil έχουμε $|a_k(\chi)| \leq q^{\frac{1}{2}}$, οπότε

$$|c_n(\chi) = |-\sum_{k=1}^{l-1} a_k(\chi)^n| \leq \sum_{k=1}^{l-1} |a_k(\chi)^n| = \sum_{k=1}^{l-1} |a_k(\chi)|^n \leq \sum_{k=1}^{l-1} q^{\frac{n}{2}}$$

$$= (l-1)q^{\frac{n}{2}} \leq (M-1)q^{\frac{n}{2}}$$

□

Έχουμε συμβολίσει με a_n τον αριθμό των αναγώγων πολυωνύμων του $\mathbb{A}$ βαθμού n.

Λήμμα 4.4.

$$|\sum_{\deg(P)=n} \chi(P)| \leq \begin{cases} \frac{M+1}{n} q^{\frac{n}{2}} & \text{όταν } \chi \neq \chi_0 \\ a_n & \text{όταν } \chi = \chi_0 \end{cases}$$

Απόδειξη. Στην περίπτωση που $\chi = \chi_0$ έχουμε

$$|\sum_{\deg(P)=n} \chi_0(P)| \leq \sum_{\deg(P)=n} |\chi_0(P)| = \sum_{\deg(P)=n} 1 = a_n.$$

Έστω τωρα χ ενας μη-τετριμμένος χαρακτήρας Dirichlet. Τότε

$$c_n(\chi) = \sum_{\substack{k,\, P \\ k\deg(P)\,=\,n}} \deg(P)\chi(P)^k = n \sum_{\deg(P)=n} \chi(P) + \sum_{\substack{k\,\geq\,2,\, P \\ k\deg(P)\,=\,n}} \deg(P)\chi(P)^k$$

$$\Rightarrow \sum_{\deg(P)=n} \chi(P) = \frac{1}{n} c_n(\chi) + \frac{1}{n} \sum_{\substack{k\,\geq\,2,\, P \\ k\deg(P)\,=\,n}} \deg(P)\chi(P)^k$$

$$\Rightarrow |\sum_{\deg(P)=n} \chi(P)| \leq \frac{1}{n}|C_n(\chi)| + \frac{1}{n}|\sum_{\substack{k\geq 2,\, P \\ k\deg(P)=n}} \deg(P)\chi(P)^k| \qquad (8)$$

Το $|c_n(\chi)|$ έχει ήδη εκτιμηθεί απο το προηγούμενο πόρισμα. Μας μένει λοιπόν να φράξουμε το

$$|\sum_{\substack{k\geq 2,\, P \\ k\deg(P)=n}} \deg(P)\chi(P)^k|.$$

Παρατηρούμε οτι

$$\sum_{\substack{k\geq 2,\, P \\ k\deg(P)=n}} \deg(P)\chi(P)^k = \sum_{\substack{d|n \\ d\leq n/2}} d \sum_{\deg(P)=d} \chi(P)^{\frac{n}{d}}.$$

Για το εσωτερικό άθροισμα, απο το θεώρημα (2.7) έχουμε

$$|\sum_{\deg(P)=d} \chi(P)^{\frac{n}{d}}| \leq \sum_{\deg(P)=d} |\chi(P)|^{\frac{n}{d}} \leq \sum_{\deg(P)=d} 1 = a_d \leq \frac{q^d}{d} + \frac{q^{\frac{d}{2}}}{\frac{d}{2}}$$

έτσι

$$|\sum_{\substack{k\geq 2,\, P \\ k\deg(P)=n}} \deg(P)\chi(P)^k| = |\sum_{\substack{d|n \\ d\leq n/2}} d \sum_{\deg(P)=d} \chi(P)^{\frac{n}{d}}|$$

$$\leq \sum_{\substack{d|n \\ d\leq n/2}} d|\sum_{\deg(P)=d} \chi(P)^{\frac{n}{d}}| \leq \sum_{\substack{d|n \\ d\leq n/2}} da_d \leq \sum_{\substack{d|n \\ d\leq n/2}} d(\frac{q^d}{d} + \frac{q^{\frac{d}{2}}}{\frac{d}{2}})$$

$$= \sum_{\substack{d|n \\ d\leq n/2}} q^d + 2\sum_{\substack{d|n \\ d\leq n/2}} q^{\frac{d}{2}}$$

$$= 1 + q + q^2 + \cdots + q^{[\frac{n}{2}]} + 2(1 + q + q^2 + \cdots + q^{[n/4]})$$

$$\leq 1 + q + q^2 + \cdots + q^{\frac{n}{2}} + 2(1 + q + q^2 + \cdots + q^{n/4}) = \frac{q^{\frac{n}{2}} - 1}{q-1} + 2\frac{q^{\frac{n}{4}} - 1}{q-1}$$

$$\leq \frac{q^{\frac{n}{2}} + q^{\frac{n}{4}}}{q-1} \leq 2q^{\frac{n}{2}}$$

Τελικά

$$|\sum_{\substack{k\geq 2,\, P \\ k\deg(P)=n}} \deg(P)\chi(P)^k| \leq 2q^{\frac{n}{2}}. \qquad (9)$$

Οπότε, από το (8), το πόρισμα (4.3) και το (9) παίρνουμε

$$|\sum_{\deg(P)=n} \chi(P)| =\leq \frac{M-1}{n}q^{\frac{n}{2}} + \frac{2}{n}q^{\frac{n}{2}} = \frac{M+1}{n}q^{\frac{n}{2}}.$$

□

Θέτουμε $S_n(a,m) = \{P \in \mathbb{A},\ \deg(P) = n,\ P \equiv a \pmod m\}$. Δοθέντων των n, a, m θέλουμε να υπολογίσουμε το $\sharp S_n(a,m)$.

Θεώρημα 4.5.

$$|\sharp\ S_n(a,m) - \frac{1}{\Phi(m)}\frac{q^n}{n}| \leq \frac{M+1}{n} q^{\frac{n}{2}}$$

Απόδειξη. Από την πρόταση (3.7) έχουμε

$$\sum_{\chi} \chi(P)\overline{\chi(a)} = \Phi(m)\,\delta(P,a)$$

συνεπώς

$$\frac{1}{\Phi(m)} \sum_{\chi} \chi(P)\overline{\chi(a)} = \begin{cases} 1 & \text{αν } P \equiv a \pmod m \\ 0 & \text{αλλιώς} \end{cases}$$

Οπότε

$$\sharp S_n(a,m) = \sum_{\substack{P \\ deg(P)=n}} \left(\frac{1}{\Phi(m)} \sum_{\chi} \chi(P)\overline{\chi(a)} \right) = \frac{1}{\Phi(m)} \sum_{\substack{P \\ deg(P)=n}} \sum_{\chi} \chi(P)\overline{\chi(a)}$$

$$= \frac{1}{\Phi(m)} \sum_{\chi} \overline{\chi(a)} \sum_{\substack{P \\ deg(P)=n}} \chi(P) = \frac{1}{\Phi(m)}(a_n + \sum_{\chi \neq \chi_0} \overline{\chi(a)} \sum_{\substack{P \\ deg(P)=n}} \chi(P)).$$

Αφαιρόντας το $\frac{1}{\Phi(m)}\frac{q^n}{n}$ και από τα δύο μέλη της ισότητας, παίρνοντας απόλυτες τιμές και εφαρμόζοντας την τριγωνική ανισότητα, έχουμε

$$|\sharp\ S_n(a,m) - \frac{1}{\Phi(m)}\frac{q^n}{n}| \leq \frac{1}{\Phi(m)}|a_n - \frac{q^n}{n}| + \sum_{\chi \neq \chi_0} |\overline{\chi(a)}|| \sum_{\substack{P \\ deg(P)=n}} \chi(P)|$$

$$= \frac{1}{\Phi(m)}|a_n - \frac{q^n}{n}| + \sum_{\chi \neq \chi_0} | \sum_{\substack{P \\ deg(P)=n}} \chi(P)|$$

Από το θεώρημα (2.7) έχουμε $|a_n - \frac{q^n}{n}| \leqslant \frac{q^{\frac{n}{2}}}{\frac{n}{2}}$. ενώ από το Λήμμα (4.4) είναι $|\sum_P \chi(P)| \leq \frac{M+1}{n} q^{\frac{n}{2}}$ συνεπώς

$$|\sharp\ S_n(a,m) - \frac{1}{\Phi(m)}\frac{q^n}{n}| \leq \frac{1}{\Phi(m)}(2\frac{q^{\frac{n}{2}}}{n} + \sum_{\chi \neq \chi_0} | \sum_{\substack{P \\ deg(P)=n}} \chi(P)|)$$

$$\leq \frac{1}{\Phi(m)}(2\frac{q^{\frac{n}{2}}}{n} + \sum_{\chi \neq \chi_0} \frac{M-1}{n} q^{\frac{n}{2}}) = \frac{1}{\Phi(m)}(2\frac{q^{\frac{n}{2}}}{n} + \frac{M-1}{n} q^{\frac{n}{2}}(\Phi(m)-1))$$

$$\leq \frac{q^{\frac{n}{2}}}{\frac{n}{2}}(\frac{1}{\Phi(m)} + \frac{M-1}{2}) \leq \frac{q^{\frac{n}{2}}}{\frac{n}{2}}(1 + \frac{M-1}{2}) = \frac{q^{\frac{n}{2}}}{\frac{n}{2}} \frac{M+1}{2}.$$

□

5 Εφαρμογές του Θεωρήματος του Dirichlet

Το Θεώρημα του Dirichlet που αποδείξαμε στην προηγούμενη ενότητα, απαντά σε κάποια ερωτήματα που προκύπτουν απο πρακτικές εφαρμογές. Για παράδειγμα, όταν πρέπει να γίνουν υπολογισμοί πάνω σε πεπερασμένα σώματα συχνά πρέπει να επιλεξει κανείς κατάλληλα στοιχεία ώστε να βελτιώσει την ταχύτητα κάποιου αλγορίθμου. Πιο συγκεκριμένα στον αλγόριθμο παραγοντοποίησης του Coppersmith οι πράξεις που χρειάζονται μειώνονται σημαντικά εαν χρησιμοποιηθούν αρκούντως 'αραιά' ανάγωγα πολυωνυμα, δηλαδή πολυώνυμα με πολλούς μηδενικούς συντελεστές. Προκύπτουν λοιπόν ερωτήματα σχετικά με την ύπαρξη και το πλήθος τέτοιων πολυωνύμων. Θα δούμε οτι εαν συγκεκριμενοποιήσουμε τη θέση των μηδενικών όρων μπορούμε να χρησιμοποιήσουμε το θεώρημα του Dirichlet για την απάντηση τέτοιων ερωτημάτων.

Αρχικά θα πρέπει να ορίσουμε την έννοια του 'αραιού' πολυωνύμου ως εξής:

Ένα πολυώνυμο βαθμού n θα ονομάζεται $k-$αραιό εαν είναι της μορφής $f = T^n + g$ όπου το g έχει βαθμό $k < n$.

Το πόσο αραιό είναι ένα τέτοιο πολυώνυμο εξαρτάται από την τιμή του k. Ορίζουμε τώρα το σύνολο

$$D_n(k) = \{f \in \mathbb{A}, f \text{ ανάγωγο}, f = T^n + g \text{ για κάποιο } g \in \mathbb{A} \text{ με } \deg(g) \leq k\}$$

των k-αραιών πολυωνύμων βαθμού n. Το ερώτημά μας είναι λοιπόν, δεδομένου n, πόσο μικρό μπορεί να γίνει το k ωστε το πλήθος των στοιχείων του $D_n(k)$ να είναι μη μηδενικό. Ωστόσο δεν φαίνεται να υπάρχει κάποιος άμεσος τρόπος να συνδέσουμε το Θεώρημα του Dirichlet με το $D_n(k)$. Αυτό που θα κάνουμε είναι οτι θα δουλέψουμε πάνω σε ένα σύνολο που είναι κλάση

ισοδυναμίας modulo ενός στοιχείου του $\mathbb{A}$ και είναι ισοπληθικό με το $D_n(k)$, συγκεκριμένα του

$$S_n(1, T^{n-k}) = \{f \in \mathbb{A}, f \text{ μονικό ανάγωγο με } \deg f = n \text{ και } f \equiv 1 \bmod T^{n-k}\}.$$

Η αιτιολόγηση για το οτι τα δυο προαναφερθέντα σύνολα είναι ισοπληθικά, θα δωθεί ώς πρόταση, πόρισμα του παρακάτω λήμματος.

Λήμμα 5.1. *Έστω $f = c_nT^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0$. Το f είναι ανάγωγο εαν και μόνο αν είναι ανάγωγο το $f = c_0T^n + c_1T^{n-1} + \cdots + c_{n-1}T + c_n$.*

Απόδειξη. Πριν προχωρήσουμε, παρατηρούμε οτι $g(T) = T^n f(\frac{1}{T})$ Έστω τώρα οτι f είναι ανάγωγο αλλά το g δεν είναι. Θα καταλήξουμε σε άτοπο. Πράγματι, έστω θ μια ρίζα του f σε μια επέκταση του $\mathbb{F}_q$ (υπενθυμίζουμε οτι έχουμε ορίσει $\mathbb{A} = \mathbb{F}_q[T]$ όπου p είναι δύναμη πρώτου). Τότε εξ ορισμού $\mathbb{F}_q(\theta) = \mathbb{F}_{q^n}$. Επίσης από το γεγονός οτι $g(T) = T^n f(\frac{1}{T})$ προκύπτει οτι το στοιχείο $a = \frac{1}{\theta}$ είναι ρίζα του g. Έτσι, $a \in \mathbb{F}_q(a) = \mathbb{F}_q(\frac{1}{\theta}) = \mathbb{F}_q(\theta) = \mathbb{F}_{q^n}$ αφού το $\frac{1}{\theta}$ είναι ρίζα του f, δηλαδή ενός αναγώγου πάνω απο το $\mathbb{F}_q$πολυωνύμου. Η ισότητα $\mathbb{F}_q(\frac{1}{\theta}) = \mathbb{F}_q(\theta)$ αναλυτικότερα προκύπτει ως εξής: $\mathbb{F}_q(\frac{1}{\theta}) \subseteq \mathbb{F}_q(\theta)$, αφού $\frac{1}{\theta} \in \mathbb{F}_q(\theta)$ ως αντίστροφο του θ και $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_q(\frac{1}{\theta})$ αφού $\theta \in \mathbb{F}_q(\frac{1}{\theta})$ ως αντίστροφο του $\frac{1}{\theta}$. Τώρα, αφού a είναι ρίζα του g, υπάρχει ανάγωγο h πάνω από το F_q με $h|g$ και $h(a) = 0$. Εαν ήταν $\deg(h) < n$, τότε απο τα προηγούμενα θα είχαμε $\mathbb{F}_{q^n} = \mathbb{F}(a) = \mathbb{F}_{q^{\deg(h)}}$ πράγμα αδύνατο από την μοναδικότητα του $\mathbb{F}_{q^n}$. Συνεπώς, $\deg(h) = n$, δηλαδή το g είναι ανάγωγο σε αντίθεση με την υπόθεση. Τα $c_i, \quad i = 1, 2, ..., n$ είναι τυχαία, οπότε η άλλη κατεύθυνση της απόδειξης είναι η ίδια. □

Σύμφωνα με το Λήμμα (5.1), το $T^n + a_kT^k + a_{k-1}T^{k-1} + \cdots + a_1T + a_0$ είναι ανάγωγο αν και μόνο αν είναι ανάγωγο το $a_0 + T^n + a_1T^{n-1} + a_2T^{n-2} + \cdots + a_kT^{n-k} + 1$ το οποίο (αφού μιλάμε για πολλαπλασιασμό με σταθερά) είναι ανάγωγο αν και μόνο αν είναι ανάγωγο το $T^n + a_1a_0{}^{-1}T^{n-1} + a_2a_0{}^{-1}T^{n-2} + \cdots + a_ka_0{}^{-1}T^{n-k} + a_0{}^{-1}1$. Παρατηρόντας τώρα ότι πολυώνυμα όπως το τελευταίο είναι ακριβώς τα στοιχεία του $S_n(1, T^{n-k})$ και πολυώνυμα όπως το αρχικό είναι ακριβώς τα στοιχεία του $D_n(k)$, έχουμε την βασική ιδέα για να αποδείξουμε την ισοπληθικότητα των δύο συνόλων.

Πρόταση 5.2. *Τα $D_n(k)$, $S_n(1, T^{n-k})$ είναι ισοπληθικά.*

Απόδειξη. Γράφουμε το $S_n(1, T^{n-k})$ στην εξής μορφή:

$$S_n(1, T^{n-k}) = \{T^n + b_{n-1}T^{n-1} + b_{n-2}T^{n-2} + \cdots + b_kT^k + 1, \quad b_i \in \mathbb{F}_q\}.$$

Πράγματι, ένα τέτοιο πολυώνυμο είναι φανερό οτι ανήκει στην κλάση του $1 \mod T^{n-k}$. Εαν πάλι f είναι ένα ανάγωγο μονικό πολυώνυμο βαθμού n

που ανήκει στην κλάση του $1 \mod T^{n-k}$ τότε -απο τον ορισμό της κλάσης ισοδυναμίας- είναι της μορφής $f = 1 + hT^{n-k}$ όπου $h \in \mathbb{F}_q[T]$μονικό και $\deg(h) = k$ (αφού $\deg(f) = n$) συνεπώς το f έχει την ζητούμενη μορφή. Σ'αυτό το σημείο ας παρατηρήσουμε οτι το $D_n(k)$ μπορεί εναλλακτικά να γραφτεί

$$D_n(k) = \{f \in \mathbb{A} \text{ ανάγωγο και } f = T^n + a_k T^k + a_{k-1}T^{k-1} + \cdots + a_1 T + a_0, b_i \in \mathbb{F}_q\}.$$

Θεωρούμε την συνάρτηση

$$r : D_n(k) \longrightarrow S_n(1, T^{n-k})$$

$$T^n + a_k T^k + a_{k-1}T^{k-1} + \cdots + a_1 T + a_0 \longmapsto {a_0}^{-1}(a_0 T^n + a_1 T^{n-1} + \cdots + a_k T^{n-k} + 1)$$

Από το Λήμμα (5.1), για

$$c_i = \begin{cases} a_0, \text{ αν } i = 0 \\ 0, \text{ αν } k+1 \leq i \leq n-1 \end{cases}$$

από το γεγονός ότι ο πολλαπλασιασμός με τη σταθερά ${a_0}^{-1}$ δεν επηρρεάζει το ανάγωγο του πολυωνύμου και από τον ορισμό των $D_n(k)$ και $S_n(1, T^{n-k})$, διαπιστώνουμε οτι πράγματι $r(D_n(k)) \subseteq S_n(1, T^{n-k})$.

Η r είναι προφανώς καλώς ορισμένη. Τώρα

$$r(T^n + a_k T^k + \cdots + a_1 T + a_0) = 0 \Leftrightarrow {a_0}^{-1}(a_0 T^n + a_1 T^{n-1} + \cdots + a_k T^{n-k} + a_n) = 0$$

$$\Leftrightarrow a_i = 0 \text{ για όλα τα } 0 \leq i \leq n \Leftrightarrow \ker(r) = \{0\} \Leftrightarrow r \text{ είναι } 1-1.$$

Τέλος, αν $f \in S_n(1, T^{n-k})$ είναι της μορφής $f = T^n + b_{n-1}T^{n-1} + \cdots + b_{n-k}T^{n-k} + 1$ οπότε $f \in r(D_n(k))$ αφού $f = r(T^n + b_{n-k}T^k + b_{n-k-1}T^{k-1} + \cdots + b_{n-1}T + 1)$ οπότε η r είναι και *επι*. Συνεπώς τα $D_n(k)$ και $S_n(1, T^{n-k})$ είναι ισοπληθικά.

□

Για να βρούμε πόσο αραιά ανάγωγα πολυώνυμα μπορεί να υπάρχουν πάνω από ενα πεπερασμένο σώμα, ψάχνουμε το ελάχιστο k, ώστε το $D_n(k)$ να είναι μη-μηδενικό. Από την Πρόταση (5.2) όμως, μπορούμε ισοδύναμα να κάνουμε το ίδιο για το σύνολο $S_n(1, T^{n-k})$. Χρησιμοποιόντας το Θεώρημα (4.5) για το τελευταίο σύνολο, προκύπτει εύκολα ένα κάτω φράγμα για το k.

Πρόταση 5.3. *Έστω $\mathbb{A} = \mathbb{F}_q[T]$ και $n \in \mathbb{N}$. Για $k \geq \frac{n}{2} + \log_q n$, υπάρχει $k-$αραιό ανάγωγο πολυώυυμο βαθμού n στο $\mathbb{A}$.*

Απόδειξη. Από το Θεώρημα (4.5) έχουμε

$$\frac{1}{\Phi(T^{n-k})}\frac{q^n}{n} - \frac{\deg(T^{n-k})+1}{n}q^{\frac{n}{2}} = \frac{1}{\Phi(T^{n-k})}\frac{q^n}{n} - \frac{n-k+1}{n}q^{\frac{n}{2}} \leq \sharp S_n(1, T^{n-k})$$

Ψάχνουμε να ελαχιστοποιήσουμε όσο το δυνατόν γίνεται το k ώστε το αριστερό μέλος της ανισότητας να παραμείνει γνήσια θετικό. Έχουμε

$$\frac{1}{\Phi(T^{n-k})}\frac{q^n}{n} - \frac{n-k+1}{n}q^{\frac{n}{2}} > 0 \Leftrightarrow \frac{1}{\Phi(T^{n-k})}\frac{q^{\frac{n}{2}}}{\frac{n}{2}} > \frac{n-k+1}{n}$$

$$\Leftrightarrow \frac{2}{\Phi(T^{n-k})}q^{\frac{n}{2}} > n-k+1.$$

Είναι

$$\Phi(T^{n-k}) = |T^{n-k}|(1-\frac{1}{|T|}) = q^{n-k}(1-\frac{1}{q}) = q^{n-k-1}(q-1)$$

οπότε ισοδύναμα θέλουμε

$$\frac{q^{\frac{n}{2}}}{q^{n-k-1}(q-1)} > \frac{n-k+1}{2} \Leftrightarrow \frac{q^{\frac{n}{2}-n+k+1}}{q-1} > \frac{n-k+1}{2}$$

Όμως

$$\frac{q^{\frac{n}{2}-n+k+1}}{q-1} > \frac{q^{\frac{n}{2}-n+k+1}}{q} = q^{-\frac{n}{2}+k} \text{ και } n > \frac{n-k+1}{2}$$

οπότε αρκεί

$$q^{-\frac{n}{2}+k} \geq n \Leftrightarrow -\frac{n}{2}+k \geq \log_q n \Leftrightarrow k \geq \frac{n}{2} + \log_q n.$$

□

Το Θεώρημα του Dirichlet, όπως διατυπώθηκε στην προηγούμενη ενότητα, μας έδωσε ένα κάτω φράγμα για το ζητούμενο k σε σχέση με τα n και q. Ωστόσο, ο αλγόριθμος του Coppersmith, ο οποίος χρησιμοποιεί αραιά ανάγωγα πολυώνυμα, χρειάζεται πολύ μικρότερο k για να τρέξει. Από την άλλη, η πραγματικότητα φαίνεται να είναι ευνοϊκή, καθώς η εμπειρία έχει δείξει ότι, για κάθε q και n, βρίσκει κανείς k, όχι μόνο μικρότερο από το φράγμα που δώσαμε στην Πρόταση (5.3) αλλά μικρότερο και από το κάτω φράγμα που απαιτεί ο αλγόριθμος του Coppersmith. Όσον αφορά το θεωρητικό κομμάτι του προβλήματος, το φράγμα της Πρότασης (5.3) είναι, μέχρι στιγμής, το καλλίτερο και τυχόν βελτίωση θα αποτελέσει σημαντική πρόοδο στον κλάδο της Θεωρίας Πεπερασμένων Σωμάτων.