Αθροισματα Gauss και Jacobi και Εφαρμογες

Κατερίνα Κούτα

Πτυχιακή Εργασία

Παρουσιάσθηκε στις 15-11-2004

Επιβλέπων Καθηγητής Ν.Γ. Τζανάκης

Τμήμα Μαθηματικών - Πανεπιστήμιο Κρήτης

Φθινοπωρινό εξάμηνο 2004

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Η πτυχιακή αυτή εργασία μου απευθύνεται σε όσους ενδιαφέρονται για τη Μαθηματική Επιστήμη, ιδιαίτερα σε εκείνους που εκτιμούν την ομορφιά της Αριθμοθεωρίας. Ως βάση της χρησιμοποιήθηκε το βιβλίο *A Classical Introduction to Modern Number Theory* των Kenneth Ireland και Michael Rosen, GTM 84, Springer - Verlag, New York 1982.

Συνοπτική περιγραφή των περιεχομένων της εργασίας.

Κεφάλαιο 2. Στην παράγραφο 2.1 αποδεικνύεται το *συμπλήρωμα του νόμου τετραγωνικής αντιστροφής*, το οποίο αφορά στον υπολογισμό του τετραγωνικού χαρακτήρα του 2. Η «κυκλοτομική» απόδειξη, που παρουσιάζουμε εδώ, δεν είναι αυτή που συνήθως συναντά κανείς σε βιβλία στοιχειώδους Αριθμοθεωρίας. Ωστόσο, είναι εξαιρετικά γόνιμη, καθώς εισάγει εργαλεία χρήσιμα και ενδιαφέροντα καθ' εαυτά.

Στην παράγραφο 2.2 εισάγονται, μέσω του συμβόλου Legendre, τα *τετραγωνικά αθροίσματα Gauss*, με χρήση των οποίων, δίνεται η απόδειξη του *νόμου τετραγωνικής αντιστροφής*.

Στην παράγραφο 2.3 παρουσιάζουμε ορισμένες προτάσεις, στοχεύοντας στην απόδειξη ενός σημαντικού θεωρήματος του Gauss (θεώρημα 2.3.4), το οποίο υπολογίζει το τετραγωνικό άθροισμα του Gauss g_1. Επίσης, η πρόταση 2.3.3 μου έκανε ιδιαίτερη εντύπωση, καθώς δίνει μία κομψή έκφραση του αθροίσματος Gauss ως γινομένου. Η απόδειξη αυτής της απλής, κατά τη μορφή, σχέσης, παρουσίασε για μένα μια απρόσμενη δυσκολία.

Κεφάλαιο 3. Στην παράγραφο 3.1 ορίζουμε τους πολλαπλασιαστικούς χαρακτήρες του σώματος $\mathbb{F}_p$ και εξετάζουμε βασικές ιδιότητές τους, οι οποίες τους καθιστούν ισχυρά εργαλεία. Συγκεκριμένα, δείχνουμε ότι το σύνολο των πολλα-

πλασιατικών χαρακτήρων στο $\mathbb{F}_p^*$ είναι κυκλική ομάδα τάξεως $p-1$ και αποδεικνύουμε (θεώρημα 3.1.9) ότι το πλήθος των λύσεων της εξίσωσης $x^n = a$ στο $\mathbb{F}_p^*$ ισούται με το άθροισμα των εικόνων του a μέσω των χαρακτήρων, των οποίων η τάξη διαιρεί το n.

Στην παράγραφο 3.2, ορίζονται τα *αθροίσματα Gauss*, ειδική περίπτωση των οποίων είναι τα τετραγωνικά αθροίσματα Gauss, τα οποία χρησιμοποιήσαμε στο κεφάλαιο 2 και υπολογίζουμε το μέτρο τους.

Στοχεύοντας στην εκτίμηση του πλήθους των λύσεων της εξίσωσης $x^n+y^n = 1$ στο $\mathbb{F}_p$, σταθεροποιούμε αρχικά το $n = 2$ και, στη συνέχεια, $n = 3$, δίνοντας μία πρώτη ιδέα των υπολογιστικών βημάτων που απαιτούνται. Διαφαίνεται έτσι, με πολύ φυσικό τρόπο, η ανάγκη ορισμού και μελέτης των αθροισμάτων Jacobi. Έπειτα, στο θεώρημα 3.2.5 δείχνουμε μία εντυπωσιακή σύνδεση αθροισμάτων Gauss και Jacobi, πόρισμα της οποίας είναι ο υπολογισμός του μέτρου των αθροισμάτων Jacobi. Από αυτό το τελευταίο συνάγονται ενδιαφέροντα θεωρήματα για το πλήθος των λύσεων των εξισώσεων $x^2 + y^2 = 1$ και $x^3 + y^3 = 1$. Για την πρώτη προσδιορίζεται ακριβώς αυτό το πλήθος, ενώ για τη δεύτερη δίνεται μια καλή εκτίμησή του, απ' την οποία συμπεραίνουμε ότι υπάρχουν πάντα λύσεις και, μάλιστα, πολλές αν ο πρώτος p είναι αρκετά μεγάλος.

Στην παράγραφο 3.3 πραγματευόμαστε τη δυνατότητα αναπαράστασης πρώτων αριθμών από δυαδικές τετραγωνικές μορφές, αποδεικνύοντας, με τη βοήθεια των αθροισμάτων Jacobi, κλασικά θεωρήματα για πρώτους $p \equiv 1 \pmod 4$ και πρώτους $p \equiv 1 \pmod 3$. Βάσει αυτών, είμαστε πλέον σε θέση να προσδιορίσουμε με ακρίβεια το πλήθος των λύσεων της εξίσωσης $x^3 + y^3 = 1$. Ιδιαίτερα εντυπωσιακό είναι το θεώρημα 3.3.6, το οποίο συνδέει την αναπαράσταση του $4p$ από τη δυαδική τετραγωνική μορφή $x^2 + 3y^2$, με το πλήθος των λύσεων της εξίσωσης $x^3 + y^3 = 1$ στο $\mathbb{F}_p$.

Στην παράγραφο 3.4 ολοκληρώνουμε τη μελέτη μας αποδεικνύοτας το θεώρημα 3.4.1, το οποίο παρέχει εκτίμηση του πλήθους των λύσεων της εξίσωσης $x^n + y^n = 1$ (όταν το n διαιρεί το $p-1$), συνέπεια της οποίας είναι ότι, για μεγάλα p, η εν λόγω εξίσωση έχει πολλές μη τετριμμένες λύσεις.

Κεφάλαιο 4. Στόχος αυτού του κεφαλαίου είναι ο *νόμος κυβικής αντιστροφής* και ορισμένα άλλα συναφή, εξίσου σημαντικά, θεωρήματα. Η υλοποίηση αυτού του στόχου απαιτεί να εργασθούμε στην ακέραια περιοχή $D = \mathbb{Z}[\omega]$, όπου ω είναι πρωταρχική κυβική ρίζα της μονάδας, και επιτυγχάνεται με τη χρήση αθροισμάτων Gauss και Jacobi, τα οποία μελετήσαμε στο κεφάλαιο 3. Το γεγονός αυτό καταδεικνύει ότι αυτά τα αθροίσματα είναι πολύ ισχυρά εργαλεία για την Αριθμοθεωρία. Πιο συγκεκριμένα:

Στην παράγραφο 4.1, προσδιορίζουμε τις μονάδες και τα πρώτα στοιχεία της D. Παρατηρούμε ότι στη D η έννοια της ισοτιμίας $\bmod \gamma$ για $\gamma \in D$, είναι ιδιαί-

τερα χρήσιμη και δείχνουμε ότι για $\pi \in D$ πρώτο, ο δακτύλιος κλάσεων $\mathrm{mod}\pi$ είναι ισόμορφος με το πεπερασμένο σώμα με $N\pi$ το πλήθος στοιχεία και, βάσει αυτού, διατυπώνουμε το ανάλογο του «μικρού θεωρήματος του Fermat». Στη συνέχεια, για κάθε πρώτο π με $N\pi \neq 3$ και α στη D, ορίζουμε τον κυβικό χαρακτήρα του $\alpha \pmod{\pi}$ και παρουσιάζουμε χρήσιμες για τη μελέτη μας ιδιότητές του.

Στην παράγραφο 4.2, διατυπώνουμε το νόμο της κυβικής αντιστροφής. Στην απόδειξή του οδηγούμαστε μέσω μιας σειράς ενδιαμέσων προτάσεων, κάποιες από τις οποίες είναι ενδιαφέρουσες καθ' εαυτές.

Στην παράγραφο 4.3, διατυπώνουμε το λεγόμενο *συμπλήρωμα του νόμου κυβικής αντιστροφής*, το οποίο αφορά τον κυβικό χαρακτήρα του πρώτου $\lambda = 1-\omega$ (ο λ είναι ο μοναδικός πρώτος διαιρέτης του 3) και δίνουμε την απόδειξή του αφού, πρώτα, μελετήσουμε σχετικές προτάσεις - εργαλεία, τα οποία χρειάζονται στη συγκεκριμένη απόδειξη.

Ακολουθεί η παράγραφος 4.4, αντικείμενο της οποίας είναι ο προσδιορισμός των πρώτων p για τους οποίους το 2 είναι κυβικό υπόλοιπο $\mathrm{mod}\ p$.

Στην παράγραφο 4.5, ολοκληρώνουμε τη μελέτη μας παρουσιάζοντας τρία θεωρήματα, δύο εκ των οποίων αποτελούν τις γενικεύσεις του νόμου κυβικής αντιστροφής και του συμπληρώματός του για στοιχεία της D, όχι κατ' ανάγκη πρώτα. Το τρίτο θεώρημα (4.5.2) λέει ότι, αν ο πρώτος $p \equiv 1 \pmod{3}$ γραφεί ως $a^2 - ab + b^2$ με $a \equiv 2$ και $b \equiv 0 \pmod{3}$, τότε οι $2a - b$ και $b/3$ είναι κυβικά ισοϋπόλοιπα $\mathrm{mod}\ p$. Αυτό είναι ένα αξιοσημείωτο θεώρημα, διότι, παρά την απλή διατύπωσή του, δεν αποδεικνύεται με στοιχειώδη Αριθμοθεωρία.

Στο τέλος κάθε κεφαλαίου παρατίθενται ορισμένες βοηθητικές προτάσεις,που χρησιμεύουν στα τεχνικά μέρη αποδείξεων των βασικών προτάσεων του αντιστοίχου κεφαλαίου.

Κλείνοντας αυτή την εισαγωγή, θα ήθελα να απευθύνω ευχαριστίες στους καθηγητές, η διαδασκαλία των οποίων υπήρξε καθοριστική για τη δημιουργία της εργασίας αυτής. Ειδικότερα, τις κυρίες Αικατερίνη Παπαδάκη και Μαρία Κουτράκη, καθηγήτριες Αγγλικής στο Τμήμα Μαθηματικών (Τ.Μ.) του Πανεπιστημίου Κρήτης (Π.Κ.), διότι η διδασκαλία τους μου πρόσφερε την ικανότητα μελέτης και επεξεργασίας αγγλικών μαθηματικών κειμένων· τον κύριο Εμμανουήλ Κατσοπρινάκη, Αναπληρωτή Καθηγητή του Τ.Μ. του Π.Κ., διότι από εκείνον διδάχθηκα μια πρώτη εισαγωγή στη Θεωρία των Αριθμών και, κατά κύριο λόγο, τον κύριο Νικόλαο Τζανάκη, Καθηγητή του Τ.Μ. του Π.Κ., επιβλέποντα Καθηγητή της εργασίας αυτής, διότι εργάστηκε με ζήλο καθοδηγώντας και διδάσκοντάς με.

Ηράκλειο, Νοέμβρης 2004

Κατερίνα Μ. Κούτα.

Κεφάλαιο 2

Τετραγωνικά αθροίσματα Gauss

Νόμος της τετραγωνικής αντιστροφής

Σε αυτό το κεφάλαιο θα αποδείξουμε το κλασικό θεώρημα του *νόμου της τετραγωνικής αντιστροφής* και του λεγομένου συμπληρώματός του (υπολογισμός του τετραγωνικού χαρακτήρα του 2) με τη βοήθεια των *τετραγωνικών αθροισμάτων Gauss* . Η προσέγγιση αυτή έχει το πλεονέκτημα ότι μπορεί να γενικευθεί και στη θεωρία των κυβικών υπολοίπων $\bmod p$. Το p θα συμβολίζει, πάντα σ' αυτή την εργασία, ένα περιττό πρώτο.

2.1 Ο τετραγωνικός χαρακτήρας του 2

Θεώρημα 2.1.1.

$$\left(\frac{2}{p}\right) = (-1)^{\epsilon}, \quad \textit{όπου} \quad \epsilon = \frac{p^2-1}{8}\,.$$

Απόδειξη. Έστω ζ μία πρωταρχική όγδοη ρίζα της μονάδας, $\zeta = e^{\frac{2\pi i}{8}}$. Επομένως, $0 = \zeta^8 - 1 = (\zeta^4 - 1)(\zeta^4 + 1)$. Επειδή $\zeta^4 \neq 1$, έχουμε $\zeta^4 = -1$ και πολλαπλασιάζοντας τη σχέση επί ζ^{-2} παίρνουμε $\zeta^2 + \zeta^{-2} = 0$. [1]

Έστω $\tau = \zeta + \zeta^{-1}$. Παρατηρούμε ότι οι τ και ζ είναι αλγεβρικοί ακέραιοι, επομένως μπορούμε να δουλέψουμε με ισοτιμίες στον δακτύλιο των αλγεβρικών ακεραίων. Ο τετραγωνικός χαρακτήρας του 2 θα προκύψει από τη σχέση

$$\tau^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2.$$

[1] Η εξίσωση αυτή προκύπτει επίσης από την παρατήρηση ότι $\zeta^2 = e^{i\frac{\pi}{2}} = i$.

Παρατηρούμε ότι $\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$, άρα

$$\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p} \tag{2.1}$$

Χρησιμοποιούμε την πρόταση 2.4.3 (βλέπε παράρτημα) και έχουμε

$$\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p}. \tag{2.2}$$

Το ζ είναι όγδοη ρίζα της μονάδας, δηλαδή $\zeta^8 = 1$. Αφετέρου, ο p είναι πρώτος, άρα οι μόνες δυνατές τιμές του $\bmod 8$ είναι ± 1 και ± 3.

1. Εάν $p \equiv \pm 1 \pmod{8}$ τότε :

$$\left.\begin{array}{rcl} \zeta^p & = & \zeta^{\pm 1} \\ \zeta^{-p} & = & \zeta^{\mp 1} \end{array}\right\} \Rightarrow \zeta^p + \zeta^{-p} = \zeta + \zeta^{-1} = \tau$$

2. Εάν $p \equiv \pm 3 \pmod{8}$ τότε :

$$\left.\begin{array}{rcl} \zeta^p & = & \zeta^{\pm 3} \\ \zeta^{-p} & = & \zeta^{\mp 3} \end{array}\right\} \Rightarrow \zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3} = -\zeta^{-1} - \zeta = -\tau$$

Αυτά τα συμπεράσματα, σε συνδυασμό με την (2.2), μας δίνουν :

$$\tau^p \equiv \begin{cases} \tau \pmod{p}, & \text{για } p \equiv \pm 1 \pmod{8} \\ -\tau \pmod{p}, & \text{για } p \equiv \pm 3 \pmod{8} \end{cases}$$

και το δεξιό μέλος γράφεται ενοποιημένα ως $(-1)^{\varepsilon}\tau$, με το ε ορισμένο όπως στην εκφώνηση του θεωρήματος. Αυτά, σε συνδυασμό με την (2.1), μας δίνουν

$$(-1)^{\varepsilon}\tau \equiv \left(\frac{2}{p}\right)\tau \pmod{p}.$$

Είδαμε, όμως, ότι $\tau^2 = 2$, επομένως, εάν πολλαπλασιάσουμε τα δύο μέλη της ισοτιμίας με τ θα προκύψει ο παράγοντας 2 και στα δύο μέλη, οπότε, ύστερα από απλοποίηση έχουμε την αποδεικτέα σχέση.

□

2.2 Νόμος της τετραγωνικής αντιστροφής

Θα ορίσουμε τώρα τα *τετραγωνικά αθροίσματα Gauss*.

Ορισμός 2.2.1. *Έστω*

$$\chi(t) = \begin{cases} \left(\frac{t}{p}\right), & \text{εάν} (t,p) = 1 \\ 0, & \text{εάν } p \mid t \end{cases}$$

Ορίζουμε[2] *το τετραγωνικό άθροισμα* $g_a(\chi)$ *του Gauss ως εξής:*

$$g_a(\chi) = \sum_{t=0}^{p-1} \chi(t)\, \zeta^{at}.$$

Αντί για $g_1(\chi)$ *γράφουμε, απλούστερα,* $g(\chi)$.

Πρόταση 2.2.2.

$$g_a = \left(\frac{a}{p}\right) g\,.$$

Απόδειξη. Εάν $a \equiv 0 \pmod p$, τότε $\zeta^{at} = 1$ για κάθε t στο $\mathbb{F}_p$, οπότε είναι $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$, από το λήμμα 2.4.6. Αφετέρου, $\left(\frac{a}{p}\right) = 0$. Επομένως ισχύει το ζητούμενο.

Εάν $a \not\equiv 0 \pmod p$, τότε,

$$\begin{aligned} \left(\frac{a}{p}\right) g_a &= \left(\frac{a}{p}\right) \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at} = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{at=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \\ &= \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} = g, \end{aligned} \tag{2.3}$$

όπου χρησιμοποιήσαμε το γεγονός ότι, όταν το t διατρέχει ένα πλήρες σύστημα υπολοίπων $\mathrm{mod} p$, το ίδιο συμβαίνει και με το at.
Από την υπόθεση ότι $a \not\equiv 0 \pmod p$, έχουμε ότι $\left(\frac{a}{p}\right)^2 = 1$, επομένως, από την (2.3), πολλαπλασιάζοντας επί $\left(\frac{a}{p}\right)$, έχουμε το ζητούμενο.

□

Πρόταση 2.2.3. $g(\chi)^2 = (-1)^{\frac{p-1}{2}} p$.

Απόδειξη. Για απλούστευση του συμβολισμού θα γράφουμε g_a αντί $g_a(\chi)$.

Εάν $a \not\equiv 0 \pmod p$, τότε, από την πρόταση 2.2.2, έχουμε, $g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-a^2}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2$. Άρα,

$$\sum_{a=1}^{p-1} g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1) g^2 \tag{2.4}$$

[2]Πρόκειται για ένα πρώτο ορισμό, τον οποίο θα γενικεύσουμε στο κεφάλαιο 3.1· βλ. ορισμό 3.2.1.

Παρατηρούμε ότι

$$g_a g_{-a} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \zeta^{a(x-y)}$$

διότι $g_a g_{-a} = \left(\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{ax}\right) \left(\sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \zeta^{-ay}\right)$. Άρα,

$$\begin{aligned}
\sum_{a=1}^{p-1} g_a g_{-a} &= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \delta(x,y)\, p \qquad \text{(βλ. λήμμα 2.4.5)} \\
&= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{xy}{p}\right) \delta(x,y)\, p \\
&= p \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \left(\frac{xy}{p}\right) \delta(x,y) \\
&= p\,(p-1) \qquad (2.5)
\end{aligned}$$

όπου $\delta(x,y) = \begin{cases} 1, & x \equiv y \pmod p \\ 0, & x \not\equiv y \pmod p \end{cases}$.

Από τις (2.4) και (2.5) έχουμε

$$\left(\frac{-1}{p}\right)(p-1)g^2 = p\,(p-1),$$

απ' όπου έπεται, προφανώς, η αποδεικτέα σχέση.

□

Θεώρημα 2.2.4. - Νόμος της τετραγωνικής αντιστροφής. *Έστω q ένας περιττός πρώτος διάφορος του p. Τότε*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu},\ \mu = \frac{1}{2}(p-1)(q-1).$$

Απόδειξη. Δουλεύουμε με ισοτιμίες $\bmod q$ στον δακτύλιο των αλγεβρικών ακεραίων.

Έστω $p^* = (-1)^{\frac{(p-1)}{2}} p$. Από την πρόταση 2.2.3 έχουμε $g^2 = p^*$, άρα

$$g^q = g^{q-1} g = (g^2)^{\frac{(q-1)}{2}} g = {p^*}^{\frac{q-1}{2}} g \equiv \left(\frac{p^*}{q}\right) g \pmod q.$$

Χρησιμοποιώντας την πρόταση 2.4.3 βλέπουμε ότι :

$$g^q = (\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t)^q \equiv \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)^q \zeta^{qt} \equiv g_q \pmod q.$$

Έπεται (βλ. πρόταση 2.2.2) ότι

$$g^q \equiv g_q \equiv \left(\frac{q}{p}\right) g \pmod{q}$$

και άρα

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod{q}.$$

Πολλαπλασιάζοντας και τις δύο πλευρές της ισοτιμίας με g και χρησιμοποιώντας την πρόταση 2.2.3 καταλήγουμε στην

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \pmod{q}.$$

Διαγράφοντας το p^* από τα δύο μέλη και παρατηρώντας ότι

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right),$$

καταλήγουμε στην αποδεικτέα σχέση.

□

2.3 Υπολογισμός του τετραγωνικού αθροίσματος Gauss

Σκοπός όσων θα ακολουθήσουν παρακάτω είναι ο υπολογισμός του τετραγωνικού αθροίσματος Gauss $g(\chi)$. Πρόκειται για ένα σημαντικό θεώρημα του Gauss, το οποίο θα αποδείξουμε παρακάτω (θεώρημα 2.3.4). Αρχικά αποδεικνύουμε κάποιες προτάσεις.

Πρόταση 2.3.1. *Έστω πρώτος $p > 2$ και $\zeta = e^{i\frac{2\pi}{p}}$ p-οστή πρωταρχική ρίζα της μονάδας. Τότε*

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{\frac{p-1}{2}} p$$

Απόδειξη. Έχουμε $x^p - 1 = (x-1)\prod_{j=1}^{p-1}(x - \zeta^j)$. Διαιρούμε με $x - 1$:

$$1 + x + x^2 + \cdots + x^{p-1} = \prod_{j=1}^{p-1}(x - \zeta^j)$$

Η αντικατάσταση $x \leftarrow 1$ δίνει $p = \prod_r (1 - \zeta^r)$, όπου το r διατρέχει οποιοδήποτε πλήρες σύστημα αντιπροσώπων των μη μηδενικών κλάσεων $\bmod p$. Οι ακέραιοι

$\pm(4k-2),\ k=1,2,\cdots,\frac{p-1}{2}$ αποτελούν ένα τέτοιο σύστημα υπολοίπων (εύκολο), επομένως,

$$\begin{aligned}
p =& \prod_{k=1}^{\frac{p-1}{2}}(1-\zeta^{4k-2})\prod_{k=1}^{\frac{p-1}{2}}(1-\zeta^{-(4k-2)})\\
=& \prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}\zeta^{-(2k-1)}-\zeta^{2(2k-1)})\prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}\zeta^{-(2k-1)}-\zeta^{-2(2k-1)})\\
=& \prod_{k=1}^{\frac{p-1}{2}}\zeta^{2k-1}(\zeta^{-(2k-1)}-\zeta^{2k-1})\prod_{k=1}^{\frac{p-1}{2}}\zeta^{-(2k-1)}(\zeta^{2k-1}-\zeta^{-(2k-1)})\\
=& \prod_{k=1}^{\frac{p-1}{2}}\zeta^{2k-1}\zeta^{-(2k-1)}(\zeta^{-(2k-1)}-\zeta^{2k-1})\prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}-\zeta^{-(2k-1)})\\
=& \prod_{k=1}^{\frac{p-1}{2}}(\zeta^{-(2k-1)}-\zeta^{2k-1})\prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}-\zeta^{-(2k-1)})\\
=& (-1)^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}-\zeta^{-(2k-1)})^2.
\end{aligned}$$

□

Πρόταση 2.3.2.

$$\prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}-\zeta^{-(2k-1)}) = \begin{cases}\sqrt{p}, & \text{εάν } p\equiv 1 \pmod 4\\ i\sqrt{p}, & \text{εάν } p\equiv 3 \pmod 4\end{cases}$$

Απόδειξη.

$$\begin{aligned}
&\prod_{k=1}^{\frac{p-1}{2}}(\zeta^{2k-1}-\zeta^{-(2k-1)}) = \prod_{k=1}^{\frac{p-1}{2}}(e^{i\frac{(4k-2)\pi}{p}}-e^{-i\frac{(4k-2)\pi}{p}}) =\\
&= \prod_{k=1}^{\frac{p-1}{2}}[\cos\frac{(4k-2)\pi}{p}+i\sin\frac{(4k-2)\pi}{p}-(\cos\frac{(4k-2)\pi}{p}-i\sin\frac{(4k-2)\pi}{p})] =\\
&= \prod_{k=1}^{\frac{p-1}{2}}(2\,i\,\sin\frac{(4k-2)\pi}{p}) = i^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}2\,\sin\frac{(4k-2)\pi}{p}, \qquad (2.6)
\end{aligned}$$

Βρίσκουμε τις τιμές του k ($k=1,\cdots,\frac{p-1}{2}$) για τις οποίες $\sin\frac{(4k-2)\pi}{p}<0$,

$$\begin{aligned}
\sin\frac{(4k-2)\pi}{p}<0 \ \Rightarrow\ & \pi<\frac{4k-2}{p}\,\pi<2\,\pi\Rightarrow p<4k-2<2p\Rightarrow\\
\Rightarrow\ & \frac{p+2}{4}<k<\frac{p+1}{2}\Rightarrow\frac{p+2}{4}<k\le\frac{p-1}{2}
\end{aligned}$$

Η ποσότητα $\sin(\frac{4k-2}{p}\pi)$ είναι θετική για$k = 1, 2, \cdots, [\frac{p+2}{4}]$ και αρνητική για $k = [\frac{p+2}{4}] + 1, \cdots, \frac{p-1}{2}$, δηλαδή για $\frac{p-1}{2} - ([\frac{p+2}{4}] + 1) + 1 = \frac{p-1}{2} - [\frac{p+2}{4}]$ το πλήθος. Επομένως, η (2.6) γράφεται:

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = 2\, i^{\frac{p-1}{2}} \prod_{k=1}^{[\frac{p+2}{4}]} \sin\frac{(4k-2)\pi}{p} \prod_{k=[\frac{p+2}{4}]+1}^{\frac{p-1}{2}} \sin\frac{(4k-2)\pi}{p} =$$

$$= 2\, i^{\frac{p-1}{2}}\, (-1)^{\frac{p-1}{2}-[\frac{p+2}{4}]} \prod_{k=1}^{[\frac{p+2}{4}]} \sin\frac{(4k-2)\pi}{p} \prod_{k=[\frac{p+2}{4}]+1}^{\frac{p-1}{2}} |\sin\frac{(4k-2)\pi}{p}| =$$

$$= 2\, i^{\frac{p-1}{2}}\, (-1)^{\frac{p-1}{2}-[\frac{p+2}{4}]} \underbrace{\prod_{k=1}^{\frac{p-1}{2}} |\sin\frac{(4k-2)\pi}{p}|}_{>0} \tag{2.7}$$

Διακρίνουμε δύο περιπτώσεις:

1. $p = 4\lambda + 1,\ \lambda \in \mathbb{Z}$. Τότε, $\frac{p-1}{2} = \frac{4\lambda+1-1}{2} = 2\lambda$ και

$$\frac{p-1}{2} - [\frac{p+2}{4}] = 2\lambda - [\frac{4\lambda+3}{4}] = 2\lambda - \lambda = \lambda.$$

Οπότε

$$i^{\frac{p-1}{2}}\, (-1)^{\frac{p-1}{2}-[\frac{p+2}{4}]} = i^{2\,\lambda}(-1)^{\lambda}(-1)^{\lambda}(-1)^{\lambda} = (-1)^{2\,\lambda} = 1 \tag{2.8}$$

2. $p = 4\lambda + 3,\ \lambda \in \mathbb{Z}$. Τότε, $\frac{p-1}{2} = \frac{4\lambda+3-1}{2} = \frac{4\lambda+2}{2} = 2\,\lambda + 1$ και

$$\frac{p-1}{2} - [\frac{p+2}{4}] = 2\lambda + 1 - [\frac{4\lambda+3+2}{4}] = 2\,\lambda + 1 - [\frac{4\lambda+5}{4}] = 2\,\lambda + 1 - (\lambda+1) = \lambda.$$

Οπότε,

$$i^{\frac{p-1}{2}}\, (-1)^{\frac{p-1}{2}-[\frac{p+2}{4}]} = i^{2\,\lambda+1}(-1)^{\lambda} = i^{2\,\lambda} i (-1)^{\lambda} = (-1)^{\lambda} i (-1)^{\lambda} = (-1)^{2\,\lambda}\, i = i. \tag{2.9}$$

Από την πρόταση 2.3.1 γνωρίζουμε ότι

$$[\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)})\,]^2 = (-1)^{\frac{p-1}{2}}\, p$$

Εάν $p \equiv 1 \pmod 4$, από τις (2.7) και (2.8) έχουμε

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = 1 \prod_{k=1}^{\frac{p-1}{2}} |\ \sin\frac{(4k-2)\pi}{p}\ | > 0$$

Επομένως, όταν $p \equiv 1 \pmod 4$,

$$[\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)})\,]^2 = p \;\Rightarrow\; \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = \sqrt{p}$$

Εάν $p \equiv 3 \pmod 4$, από τις (2.7) και (2.9) παίρνουμε

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = i \prod_{k=1}^{\frac{p-1}{2}} |\, \sin\frac{(4k-2)\pi}{p}\,| = i\,\mu, \mu > 0$$

Επομένως, όταν $p \equiv 3 \pmod 4$,

$$i^2\mu^2 = [\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)})\,]^2 = i^2 p$$

και επειδή $\mu > 0$,

$$\prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = i\,\sqrt{p}.$$

□

Πρόταση 2.3.3.

$$g(\chi) = \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}).$$

Απόδειξη. Ο συνδυασμός των προτάσεων 2.3.1 και 2.2.3 δίνει

$$g(\chi) = \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)})\;\varepsilon = \pm 1$$

Θα δείξουμε ότι $\varepsilon = 1$. Θεωρούμε το πολυώνυμο

$$f(x) = \sum_{j=1}^{p-1} \chi(j)\, x^j - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (x^{2k-1} - x^{p-(2k-1)})$$

Τότε, $f(\zeta) = g(\chi) - g(\chi) = 0$, όπου ζ είναι η $p-$ οστή ρίζα της μονάδας, $\zeta = e^{i\frac{2\pi}{p}}$ και $f(1) = 0$ (διότι $\sum_{j=1}^{p-1} \chi(j) = 0$).
Το ζ είναι ρίζα του $f(x)$, άρα το ελάχιστο πολυώνυμο του ζ, το $1 + x + \cdots + x^{p-1}$ (βλ. πρόταση 2.4.2) διαιρεί το $f(x)$. Αντίστοιχα, το 1 είναι ρίζα του $f(x)$, άρα το ελάχιστο πολυώνυμο του 1, το $x - 1$ διαιρεί το $f(x)$. Τα πολυώνυμα $x - 1$ και $1 + x + \cdots + x^{p-1}$ είναι πρώτα μεταξύ τους, επομένως, το γινόμενό τους $x^p - 1$

διαιρεί το $f(x)$. Συνεπώς, υπάρχει $h(x) \in \mathbb{Z}[x]$, τέτοιο ώστε $f(x) = (x^p - 1)h(x)$. Θέτουμε $x = e^z$, οπότε

$$f(e^z) = \sum_{j=1}^{p-1} \chi(j)\, e^{zj} - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (e^{z(2k-1)} - e^{-z(p-(2k-1))}) = (e^{zp} - 1)h(e^z), \quad (2.10)$$

όπου $\sum_{j=1}^{p-1} \chi(j)\, e^{zj} = \sum_{j=1}^{p-1} \chi(j) \sum_{k=0}^{\infty} \frac{j^k}{k!}\, z^k$ και ο k-παράγοντας του γινομένου $\prod_{k=1}^{\frac{p-1}{2}} (e^{z(2k-1)} - e^{-z(p-(2k-1))})$ προκύπτει ως εξής :

$$\begin{aligned} e^{(2k-1)z} &= 1 + \frac{2k-1}{1!}\, z + \frac{(2k-1)^2}{2!}\, z^2 + \frac{(2k-1)^3}{3!}\, z^3 + \cdots \\ e^{[p-(2k-1)]z} &= 1 + \frac{p-(2k-1)}{1!}\, z + \frac{[p-(2k-1)]^2}{2!}\, z^2 + \frac{[p-(2k-1)]^3}{3!}\, z^3 + \cdots \end{aligned}$$

Αφαιρούμε κατά μέλη τις παραπάνω ισότητεσ:

$$e^{(2k-1)z} - e^{[p-(2k-1)]z} = (4k - 2 - p)\, z + \{\text{μεγαλύτερες δυνάμεις του } z\}$$

Παρατηρούμε ότι κάθε παράγοντας είναι βαθμού ≥ 1 ως προς z. Επειδή το γινόμενο έχει $\frac{p-1}{2}$ παράγοντες, έπεται ότι ο συντελεστής του $z^{\frac{p-1}{2}}$ στο γινόμενο ισούται με $\prod_{k=1}^{\frac{p-1}{2}} (4k - 2 - p)$. Οπότε ο συντελεστής του $z^{\frac{p-1}{2}}$ στο αριστερό μέλος της (2.10) είναι:

$$\frac{\sum_{j=1}^{p-1} \chi(j)\, j^{\frac{p-1}{2}}}{(\frac{p-1}{2})!} - \varepsilon \prod_{k=1}^{\frac{p-1}{2}} (4k - 2 - p)$$

Στο δεξιό μέλος της (2.10) πληρούνται οι προϋποθέσεις της πρότασης 2.4.1. Πράγματι, έστω $h(x) = \gamma_0 + \gamma_1\, x + \cdots + \gamma_m x^m, m \in N,\ \gamma_i \in \mathbb{Z}, i = 0, 1, \cdots, m$. Τότε

$$\begin{aligned} h(e^z) = \gamma_0 + \gamma_1 e^z + \cdots + \gamma_m e^{zm} &= \sum_{t=0}^{m} \gamma_t (1 + \frac{tz}{1!} + \frac{t^2 z^2}{2!} + \cdots + \frac{t^k z^k}{k!} + \cdots) \\ &= \sum_{k=0}^{\infty} \frac{1^k \gamma_1 + 2^k \gamma_2 + \cdots + m^k \gamma_m}{k!} z^k \end{aligned}$$

Άρα το $h(e^z)$ μπορεί να γραφτεί στη μορφή $h(e^z) = \sum_{k=0}^{\infty} \frac{\Gamma_k}{k!} z^k$. Επίσης, το $e^{zp} - 1$ γράφεται

$$e^{zp} - 1 = \sum_{k=0}^{\infty} \frac{p^k}{k!} z^k - 1 = \frac{p}{1!}\, z + \frac{p^2}{2!}\, z^2 + \frac{p^3}{3!}\, z^3 + \cdots = \sum_{k=0}^{\infty} \frac{\nu_k}{k!}\, z^k$$

όπου $\nu_0 = 0$ και $\nu_i = p^i$ για $i = 1, 2, \cdots$.
Επομένως, σε κάθε περίπτωση $p \mid \nu_i$ και $\nu_i \in \mathbb{Z}$, δηλαδή $p \mid \nu_i$ για $i = 0, 1, \ldots, p-1$. Από την πρόταση 2.4.1 έχουμε ότι ο συντελεστής του $z^{\frac{p-1}{2}}$ στο δεξί μέλος της (2.10) μπορεί να γραφτεί ως $p\frac{A}{B}, A \in \mathbb{Z}, B \in \mathbb{Z}^*, p \not| B$. Εξισώνουμε τους συντελεστές του $z^{\frac{p-1}{2}}$ από τα δύο μέλη της (2.10), πολλαπλασιάζουμε με $B(\frac{p-1}{2})!$ και παίρνουμε

$$B\sum_{j=1}^{p-1}\chi(j)\, j^{\frac{p-1}{2}} - B(\frac{p-1}{2})!\varepsilon\prod_{k=1}^{\frac{p-1}{2}}(4k-2-p) = A\,p\,(\frac{p-1}{2})!$$

Άρα,

$$B\sum_{j=1}^{p-1}\chi(j)\, j^{\frac{p-1}{2}} \equiv \varepsilon B(\frac{p-1}{2})!\prod_{k=1}^{\frac{p-1}{2}}(4k-2) \pmod p$$

Μπορούμε να διαγράψουμε το B από τα δύο μέλη της ισοδυναμίας διότι $p \not| B$, οπότε έχουμε διαδοχικά:

$$\begin{aligned}
\sum_{j=1}^{p-1}\chi(j)\, j^{\frac{p-1}{2}} &\equiv \varepsilon(1\cdot 2\cdot 3\cdots\frac{p-1}{2})2^{\frac{p-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}(2k-1) \pmod p\\
&\equiv \varepsilon(2\cdot 4\cdot 6\cdots(p-1))\prod_{k=1}^{\frac{p-1}{2}}(2k-1) \pmod p\\
&\equiv \varepsilon\,(2\cdot 4\cdot 6\cdots(p-1))(1\cdot 3\cdot 5\cdots(p-2)) \pmod p\\
&\equiv \varepsilon(p-1)! \pmod p
\end{aligned}$$

Με χρήση του θεωρήματος του Wilson καταλήγουμε στη σχέση

$$\sum_{j=1}^{p-1}\chi(j)\, j^{\frac{p-1}{2}} \equiv -\varepsilon \pmod p \tag{2.11}$$

Όμως, από τη στοιχειώδη Θεωρία Αριθμών είναι γνωστό ότι, $\chi(j) \equiv j^{\frac{p-1}{2}} \pmod p$, άρα

$$\sum_{j=1}^{p-1}\chi(j)\, j^{\frac{p-1}{2}} \equiv \sum_{j=1}^{p-1}\chi(j)^2 \equiv \sum_{j=1}^{p-1}1 \;\equiv\; p-1 \equiv -1 \pmod p.$$

Από την τελευταία και την (2.11) έπεται ότι $\varepsilon \equiv 1 \pmod p$. Όμως $\varepsilon = \pm 1$, επομένως $\varepsilon = 1$.

□

Είμαστε τώρα σε θέση να αποδείξουμε το σημαντικό

Θεώρημα 2.3.4. *(**Gauss**) Για p περιττό πρώτο και $g(\chi)$ όπως στον ορισμό 2.2.1 ισχύει*

$$g(\chi) = \begin{cases} \sqrt{p}\,, & \text{αν} p \equiv 1 \pmod 4 \\ i\sqrt{p}\,, & \text{αν} p \equiv 3 \pmod 4 \end{cases}$$

Απόδειξη.

$$\begin{aligned} g(\chi) &= \prod_{k=1}^{\frac{p-1}{2}} (\zeta^{2k-1} - \zeta^{-(2k-1)}) \quad \text{(από πρόταση 2.3.3)} \\ &= \begin{cases} \sqrt{p}, & \text{εάν} p \equiv 1 \pmod 4 \\ i\sqrt{p}, & \text{εάν} p \equiv 3 \pmod 4 \end{cases} \quad \text{(από πρόταση 2.3.2)} \end{aligned}$$

□

2.4 Παράρτημα - Βοηθητικές προτάσεις

Πρόταση 2.4.1. *Έστω $f(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!}\, x^n$ και $g(x) = \sum_{n=0}^{\infty} \frac{b_n}{n!}\, x^n$ με $a_n, b_n \in \mathbb{Z}$. Εάν p πρώτος τέτοιος ώστε $p \mid \alpha_i$ για $i = 0, \cdots, p-1$, τότε κάθε συντελεστής c_t του γινομένου $f(x)\, g(x) = \sum_{n=0}^{\infty} \frac{c_n}{n!}\, x^n$ για $t = 0, \cdots, p-1$ μπορεί να γραφτεί ως $p\, \frac{A}{B}$, όπου $p \not| B$.*

Απόδειξη. Στο πολυώνυμο $f(x)g(x)$ έστω c_t ο συντελεστής του x^t. Είναι $c_0 = a_0 b_0$. Από υπόθεση $p \mid \alpha_i\,, i = 0, 1, \cdots, p-1$, οπότε θέτουμε $a_i = p\,\mu_i,\ \mu_i \in \mathbb{Z}$. Άρα, $c_0 = p\,\mu_0\,b_0$, ενώ για $t = 1, \ldots, p-1$,

$$c_t = \sum_{k=0}^{t} \frac{a_k}{k!}\, \frac{b_{t-k}}{(t-k)!} = \sum_{k=0}^{t} \frac{p\,\mu_k}{k!}\, \frac{b_{t-k}}{(t-k)!} = p \sum_{k=0}^{t} \frac{\mu_k\, b_{t-k}}{k!\,(t-k)!}.$$

Επειδή $0 \le k \le t$ και $1 \le t \le p-1$, έπεται ότι $p \not| k!$ και $p \not| (t-k)!$. Άρα κάθε συντελεστής $c_t\,,\ t = 1, \cdots, p-1$ γράφεται στη μορφή $c_t = p\, \frac{A_t}{B_t}$, όπου $B_t = \prod_{k=0}^{t} k!\,(t-k)!$. Οπότε, από την παραπάνω παρατήρηση, $p \not| B_t$.

□

Πρόταση 2.4.2. *Έστω πρώτος p και $\zeta \neq 1$, p-οστή ρίζα της μονάδας. Το ελάχιστο πολυώνυμο της ζ είναι το $g(x) = \sum_{k=0}^{p-1} x^k$.*

Απόδειξη. Η σχέση $g(x) = \frac{x^p-1}{x-1}$ δείχνει ότι $g(\zeta) = 0$. Αρκεί να δείξουμε ότι το $g(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$. Ισοδύναμα, αρκεί να δείξουμε ότι το $f(x) = g(x+1)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ [3]. Πράγματι,

$$\begin{aligned} f(x) &= g(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x + 1 - 1}{x} \\ &= x^{p-1} + px^{p-2} + \cdots + p \end{aligned}$$

Από το κριτήριο Eisenstein για τον πρώτο p, το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

□

Πρόταση 2.4.3. *Εάν $\omega_1, \omega_2 \in \Omega$ και ο $p \in Z$ είναι πρώτος, τότε*

$$(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \pmod{p}.$$

Απόδειξη. $(\omega_1 + \omega_2)^p = \sum_{k=0}^{p} \binom{p}{k} \omega_1^k \omega_2^{p-k}$ και ο συντελεστής $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ είναι πολλαπλάσιο του p για $1 \leq k \leq p-1$, διότι $p \,|\, p!$ και ο p δε διαιρεί το $k!(p-k)!$ αφού αυτή η έκφραση είναι γινόμενο ακεραίων μικρότερων και επομένως σχετικά πρώτων προς τον p.
Το αποτέλεσμα έπεται από το παραπάνω συμπέρασμα και από το γεγονός ότι ο Ω είναι δακτύλιος.

□

Λήμμα 2.4.4.

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p, & \textit{εάν} \quad a \equiv 0 \pmod{p} \\ 0, & \textit{αλλιώς.} \end{cases}$$

Απόδειξη. Εάν $a \equiv 0 \pmod{p}$, τότε $\zeta^a = 1$ και επομένως

$$\sum_{t=0}^{p-1} \zeta^{at} = p.$$

Εάν $a \not\equiv 0 \pmod{p}$, τότε $\zeta^a \neq 1$ και επομένως

$$\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0.$$

□

[3] διότι τότε, εάν το $g(x)$ έχει μία μη - τετριμμένη ανάλυση στο $\mathbb{Z}[x]$, έστω $g(x) = h(x)q(x)$, θα είναι $g(x+1) = h(x+1)q(x+1)$, δηλαδή $f(x) = h(x+1)q(x+1)$, το οποίο μας δίνει μία μη τετριμμένη ανάλυση του $f(x)$ στο $\mathbb{Z}[x]$, άρα και στο $\mathbb{Q}[x]$. Αντίφαση, γιατί το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Πόρισμα 2.4.5.

$$p^{-1}\sum_{t=0}^{p-1}\zeta^{t(x-y)} = \delta(x,y) = \begin{cases} 1, & \textit{εάν} \quad x \equiv y \pmod{p}, \\ 0, & \textit{εάν} \quad x \not\equiv y \pmod{p} \end{cases}$$

Απόδειξη. Προκύπτει αμέσως από το Λήμμα 2.4.4 εάν θέσουμε $t = x - y$.

□

Λήμμα 2.4.6.

$$\sum_{t=0}^{p-1}\left(\frac{t}{p}\right) = 0,$$

όπου $\left(\frac{t}{p}\right)$ *είναι το σύμβολο Legendre.*

Απόδειξη. Εξ ορισμού $\left(\frac{0}{p}\right) = 0$. Από τους υπόλοιπους $p-1$ όρους του αθροίσματος, μισοί είναι ίσοι με $+1$ και μισοί είναι ίσοι με -1, διότι γνωρίζουμε ότι υπάρχουν τόσα τετραγωνικά ισοϋπόλοιπα όσα είναι τα τετραγωνικά ανισοϋπόλοιπα $\pmod{p}$.

□

Κεφάλαιο 3

Αθροίσματα Gauss και Jacobi

Στο κεφάλαιο αυτό θα μελετήσουμε κάποιες εξισώσεις στο F_p (p πρώτος) και θα αποδείξουμε κάποια κλασικά θεωρήματα αναπαράστασης του p από ειδικές δυαδικές τετραγωνικές μορφές. Βασικά εργαλεία για τη μελέτη μας θα είναι οι *πολλαπλασιαστικοί χαρακτήρες* τα *γενικευμένα αθροίσματα Gauss* και τα *αθροίσματα Jacobi*.

3.1 Πολλαπλασιαστικοί χαρακτήρες

Ορισμός 3.1.1. *Ένας ομομορφισμός ομάδων $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ λέγεται πολλαπλασιαστικός χαρακτήρας του (σώματος) $\mathbb{F}_p$. Σ' αυτή την εργασία, συχνά, θα παραλείπομε το επίθετο «πολλαπλασιαστικός». Ένας πολλαπλασιστικός χαρακτήρας είναι, δηλαδή, μία απεικόνιση $\chi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ με την ιδιότητα*

$$\chi(ab) = \chi(a)\chi(b), \forall a, b \in \mathbb{F}_p^*.$$

Παραδείγματα:

1. Το σύμβολο Legendre , $\left(\frac{a}{p}\right)$ εάν θεωρηθεί συνάρτηση της κλάσης $a \bmod p$.
2. Ο *τετριμμένος χαρακτήρας*, που ορίζεται από τη σχέση $\varepsilon(a) = 1, \forall a \in \mathbb{F}_p^*$.

Συχνά είναι χρήσιμο να επεκτείνουμε το πεδίο ορισμού του χαρακτήρα σε όλο το $\mathbb{F}_p$. Εάν $\chi \neq \varepsilon$, αυτό γίνεται εάν θέσουμε $\chi(0) = 0$. Για τον χαρακτήρα ε ορίζουμε $\varepsilon(0) = 1$.

Πρόταση 3.1.2. *Έστω χ χαρακτήρας του $\mathbb{F}_p$ και $a \in \mathbb{F}_p^*$. Τότε:*

1. $\chi(1) = 1$.
2. $\chi(a)$ *είναι* $(p-1)$*-οστή ρίζα της μονάδας.*
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Απόδειξη. **1.** Είναι $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$. Αλλά $\chi(1) \neq 0$, διότι $\chi(1) \in \mathbb{C}^*$, άρα $\chi(1) = 1$.
2. Από υπόθεση, είναι $1 = a^{p-1}$, άρα $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.
3. Είναι $1 = \chi(1) = \chi(a \cdot a^{-1}) = \chi(a)\chi(a^{-1})$, απ' όπου $\chi(a)^{-1} = \chi(a^{-1})$.
Ακόμη, $\chi(a^{-1}) = \overline{\chi(a)}$ διότι από το (2) έχουμε διαδοχικά:
$\chi(a)^{p-1} = 1 \Rightarrow |\chi(a)^{p-1}| = 1 \Rightarrow |\chi(a)|^{p-1} = 1 \Rightarrow |\chi(a)| = 1 \Rightarrow |\chi(a)|^2 = 1$
$\Rightarrow \chi(a)\overline{\chi(a)} = 1 \Rightarrow \chi(a)^{-1} = \overline{\chi(a)}$.

□

Πρόταση 3.1.3. *Αν ο* χ *είναι πολλαολασιαστικός χαρακτήρας του* $\mathbb{F}_p$*, τότε*

$$\sum_{t \in \mathbb{F}_p} \chi(t) = \begin{cases} 0 & \text{αν } \chi \neq \varepsilon \\ p\,, & \text{αν } \chi = \varepsilon \end{cases}$$

Απόδειξη. Εάν $\chi \neq \varepsilon$, τότε υπάρχει $a \in \mathbb{F}_p^*$, τέτοιο ώστε $\chi(a) \neq 1$. Έστω $T = \sum_{t \in F_p} \chi(t)$. Παρατηρούμε ότι $\{at : t \in \mathbb{F}_p^*\} = \mathbb{F}_p^*$, άρα

$$\chi(a)T = \sum_{t \in F_p} \chi(t)\chi(a) = \sum_{t \in F_p} \chi(at) = T,$$

απ¨ όπου $(\chi(a) - 1)T = 0$. Αλλά ο συντελεστής του T είναι μη μηδενικός, άρα $T = 0$.

Εάν $\chi = \varepsilon$, τότε $\sum_{t \in \mathbb{F}_p} \chi(t) = \sum_{t \in \mathbb{F}_p} 1 = p$.
τελος

Πρόταση 3.1.4. *Αν* χ, λ *είναι πολλαπλασιαστικοί χαρακτήρες του* $\mathbb{F}_p^*$*, τότε και οι απεικονίσεις* $\chi \cdot \lambda$ *και* χ^{-1} *είναι πολλαπλασιαστικοί χαρακτήρες του* $\mathbb{F}_p^*$.

Απόδειξη. Έστω $a, b \in \mathbb{F}_p^*$. Τότε,

$$\begin{aligned} \chi\lambda(ab) &\overset{ορσ}{=} \chi(ab)\lambda(ab) = \chi(a)\chi(b)\lambda(a)\lambda(b) = (\chi(a)\lambda(a))(\chi(b)\lambda(b)) \\ &= \chi\lambda(a)\chi\lambda(b) \end{aligned}$$

Επίσης,

$$\chi^{-1}(ab) = \chi(ab)^{-1} = (\chi(a)\chi(b))^{-1} = \chi(a)^{-1}\chi(b)^{-1} = \chi^{-1}(a)\chi^{-1}(b)$$

□

Πρόταση 3.1.5. *Το σύνολο των πολλαπλασιαστικών χαρακτήρων του $\mathbb{F}_p^*$, εφοδιασμένο με την πράξη του πολλαπλασιασμού συναρτήσεων, είναι κυκλική ομάδα τάξεως $p-1$. Το ουδέτερο στοιχείο αυτής της ομάδας είναι ο τετριμμένος χαρακτήρας ε.*

Εάν $a \in \mathbb{F}_p^*$ και $a \neq 1$, τότε υπάρχει χαρακτήρας χ, τέτοιος ώστε $\chi(a) \neq 1$.

Απόδειξη. Το ότι οι πολλαπλασιαστικοί χαρακτήρες, με πράξη τον πολλαπαλσιασμό συναρτήσεων, αποτελούν ομάδα, είναι άμεση συνέπεια της πρότασης 3.1.3. Προφανώς, ο ε είναι ουδέτερο στοιχείο γι¨ αυτή την πράξη.

Θα δείξουμε τώρα ότι αυτή η ομάδα είναι κυκλική, τάξεως $p-1$. Γνωρίζουμε ότι η $\left(\mathbb{F}_p^*, \cdot\right)$ είναι πολλαπλασιαστική ομάδα και έστω g ένας γεννήτοράς της.
Πρώτη παρατήρηση: Κάθε χαρακτήρας χ προσδιορίζεται πλήρως από την τιμή $\chi(g)$. Πράγματι, αφού κάθε $a \in \mathbb{F}_p^*$ είναι της μορφής $a = g^l$ με $0 \leq l \leq p-2$, έπεται ότι

$$\chi(a) = \chi(g^l) = \chi(g)^l.$$

Δεύτερη παρατήρηση: $\chi(g)$ είναι $(p-1)$-οστή ρίζα της μονάδας (πρόταση 3.1.2) και υπάρχουν ακριβώς $p-1$ τέτοιες ρίζες, άρα η ομάδα των χαρακτήρων έχει τάξη το πολύ $p-1$.

Έστω, τώρα, $\zeta \in \mathbb{C}$ μία πρωταρχική $(p-1)$-οστή ρίζα της μονάδας. Θα ορίσουμε ένα χαρακτήρα $\lambda : \mathbb{F}_p^* \to \mathbb{C}^*$. Προσωρινά, τα γράμματα k, ℓ ας συμβολίζουν ακεραίους πρώτους προς τον p και οι αντίστοιχες κλάσεις τους $\bmod p$ (δηλαδή, τα αντίστοιχα στοιχεία του $\mathbb{F}_p^*$) ας συμβολίζονται $[k], [\ell]$. Ορίζουμε

$$\lambda(g^{[k]}) = \zeta^k.$$

Η λ είναι καλά ορισμένη, δηλαδή, θα δείξουμε ότι όταν $[k] = [\ell]$ τότε $\lambda\left(g^{[k]}\right) = g([\ell])$. Πράγματι,

$$[k] = [\ell] \Rightarrow k = \ell + np \Rightarrow \zeta^k = \zeta^\ell(\zeta^p)^n = \zeta^\ell \Rightarrow \lambda(g^{[k]}) = \lambda(g^{[\ell]}).$$

Έχοντας αποδείξει ότι η λ είναι καλά ορισμένη, επανερχόμαστε στον απλούστερο συμβολισμό $k, \ell, \ldots$ για τα στοιχεία του $\mathbb{F}_p^*$.

Η συνάρτηση λ είναι χαρακτήρας διότι

$$\lambda(g^k)\lambda(g^\ell) = \zeta^k\zeta^\ell = \zeta^{k+\ell} = \lambda\left(g^{k+\ell}\right).$$

Τώρα θ' αποδείξουμε ότι η τάξη του χαρακτήρα λ είναι $p-1$. Έστω, λοιπόν, $n > 0$ η τάξη του λ στην ομάδα των χαρακτήρων. Τότε ο n είναι διαιρέτης της τάξης της ομάδας, η οποία είδαμε ότι είναι, το πολύ, $p-1$. Άρα $n \leq p-1$. Αφετέρου, $\lambda^n = \varepsilon$, άρα

$$1 = \varepsilon(g) = \lambda^n(g) = (\lambda(g))^n = \lambda(g^n) = \zeta^n$$

και επειδή η ζ είναι πρωταρχική $(p-1)$-οστή ρίζα της μονάδας, έπεται ότι $n = p-1$. Αφού, όμως, η ομάδα των χαρακτήρων έχει τάξη το πολύ $p-1$, και το στοιχείο της λ έχει τάξη $p-1$, έπεται ότι η τάξη αυτής της ομάδας είναι, ακριβώς, $p-1$ και το λ είναι γεννήτοράς της.

Τέλος, εάν $a \in \mathbb{F}_p^*$ και $a \neq 1$, τότε $a = g^\ell$, όπου $1 \leq \ell < p-1$. Συνεπώς,

$$\lambda(a) = \lambda(g^\ell) = \zeta^\ell \neq 1.$$

□

Πόρισμα 3.1.6. *Έστω* $\mathbf{X}$ *η ομάδα των χαρακτήρων. Για κάθε* $a \in \mathbb{F}_p^*$, $a \neq 1$ *ισχύει* $\sum_{\chi \in \mathbf{X}} \chi(a) = 0$.

Απόδειξη. Έστω $S = \sum_{\chi \in \mathbf{X}} \chi(a)$. Από την πρόταση 3.1.5 έχουμε ότι υπάρχει χαρακτήρας λ, τέτοιος ώστε $\lambda(a) \neq 1$. Τότε

$$\lambda(a)S = \lambda(a) \sum_{\chi \in \mathbf{X}} \chi(a) = \sum_{\chi \in \mathbf{X}} \lambda(a)\chi(a) = \sum_{\chi \in \mathbf{X}} \lambda\chi(a) \overset{\P}{=} S.^1$$

Άρα, $(1-\lambda(a))S = 0$ και, επειδή $\lambda(a) \neq 1$, έπεται ότι $S = 0$.

□

Μέσω των χαρακτήρων μπορούμε τώρα να εκφράσουμε το πλήθος των λύσεων της εξίσωσης $x^n = a$, όπου $a \in \mathbb{F}_p^*$ και $n|p-1$. Θέτουμε $d = (p-1, n)$ και από την πρόταση 3.5.3 συμπεραίνουμε ότι η εξίσωση αυτή έχει λύση εάνν $a^{\frac{p-1}{d}} = 1$.

Ορισμός 3.1.7. *Για* $n|p-1$ *και* $a \in \mathbb{F}_p$ *συμβολίζουμε με* $N_p(x^n = a)$ *το πλήθος των λύσεων της εξίσωσης* $x^n = a$.

Πρόταση 3.1.8. *Εάν* $a \in \mathbb{F}_p^*$ *και* $n|p-1$ *και η εξίσωση* $x^n = a$ *δεν επιλύεται στο* $\mathbb{F}_p$, *τότε υπάρχει χαρακτήρας* χ *τέτοιος ώστε* $\chi^n = \varepsilon$ *και* $\chi(a) \neq 1$.

Απόδειξη. Έστω g, ζ, λ όπως στην πρόταση 3.1.5. Θέτουμε $\chi = \lambda^{\frac{p-1}{n}}$, οπότε $\chi^n = \lambda^{p-1} = \varepsilon$, διότι η τάξη της ομάδας των χαρακτήρων είναι $p-1$ (πρόταση 3.1.5). Επίσης,

$$\chi(g) = \lambda^{\frac{p-1}{n}}(g) = \lambda(g)^{\frac{p-1}{n}} = e^{\frac{2\pi i}{n}}.$$

Έστω $a = g^\ell$ για κάποιο ℓ. Αφού η $x^n = a$ δεν είναι επιλύσιμη, έπεται ότι $n \not| \ell$.
($n|\ell \Leftrightarrow \exists k \in \mathbb{Z} : \ell = nk \Leftrightarrow a = g^\ell = g^{nk} = (g^k)^n$, αντίφαση.)
Συνεπώς, $\chi(a) = \chi(g^\ell) = \chi(g)^\ell = \zeta^\ell = e^{2\pi i \frac{\ell}{n}} \neq 1$.

□

[1] Η ισότητα (¶) ισχύει διότι $(\mathbf{X}, \cdot)$ είναι ομάδα, άρα, εφόσον ο χ διατρέχει όλο το $\mathbf{X}$, το ίδιο συμβαίνει και με τον $\lambda\chi$.

Θεώρημα 3.1.9.

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$$

όπου το άθροισμα είναι πάνω από όλους τους χαρακτήρες των οποίων η τάξη διαιρεί το n.

Απόδειξη. Από τις προτάσεις 3.1.5 και 3.5.2 του παραρτήματος συμπεραίνουμε ότι υπάρχουν ακριβώς n χαρακτήρες των οποίων η τάξη διαιρεί το n. Διακρίνουμε δύο περιπτώσεις:

Έστω $a = 0$. Η εξίσωση $x^n = 0$ έχει ακριβώς μία λύση, τη $x = 0$. Επίσης, $\sum_{\chi^n=\varepsilon} \chi(0) = 1$ διότι $\chi(0) = 0$ όταν $\chi \neq \varepsilon$ και $\varepsilon(0) = 1$. Άρα, στην περίπτωση που $a = 0$, η πρόταση ισχύει.

Έστω ότι $a \neq 0$, διακρίνουμε δύο υποπεριπτώσεις.

1 . Αν η $x^n = a$ επιλύεται, τότε υπάρχει b τέτοιο ώστε $b^n = a$.
Εάν $\chi^n = \varepsilon$ τότε $\chi(a) = \chi(b^n) = \chi^n(b) = \varepsilon(b) = 1$. Επομένως

$$\sum_{\chi^n=\varepsilon} \chi(a) = \sum_{\chi^n=\varepsilon} 1 = n.$$

Όμως, από την πρόταση 3.5.3, $N_p(x^n = a) = (p-1, n) = n$, άρα η πρόταση ισχύει.

2 . Αν η $x^n = a$ δεν επιλύεται, τότε έχουμε να δείξουμε ότι

$$\sum_{\chi^n=\varepsilon} \chi(a) = 0$$

Έστω $T = \sum_{\chi^n=\varepsilon} \chi(a)$. Από την πρόταση 3.1.8, υπάρχει χαρακτήρας ϱ ώστε $\varrho(a) \neq 1$ και $\varrho^n = \varepsilon$, άρα

$$\varrho(a)T = \sum_{\chi^n=\varepsilon} \varrho(a)\chi(a) \overset{\dagger}{=} \sum_{(\varrho\chi)^n=\varepsilon} \varrho\chi(a) = T.^2$$

Συνεπώς, $(1 - \varrho(a))T = 0$ και επειδή $\varrho(a) \neq 1$, έπεται ότι $T = 0$.

□

Το θεώρημα 3.1.9 επαληθεύεται τετριμμένα για p περιττό και $n = 2$. Πράγματι, τότε υπάρχουν δύο χαρακτήρες τάξεως 2: Ο τετριμμένος και ο οριζόμενος μέσω του συμβόλου Legendre (βλ. ορισμό 2.2.1). Το θεώρημα λέει, σ' αυτή την περίπτωση, ότι $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$. Εξ ορισμού, $\left(\frac{a}{p}\right) = 1$, εάνν η $x^2 = a$ επιλύεται. Άρα, $N(x^2 = a) = 1 + 1 = 2$, όταν η εξίσωση είναι επιλύσιμη και $N_p(x^2 = a) = 1 - 1 = 0$ όταν δεν είναι επιλύσιμη.

[2] Η ισότητα (†) ισχύει διότι, καθώς το χ διατρέχει την υποομάδα των χαρακτήρων, των οποίων η τάξη διαιρεί το n, το ίδιο συμβαίνει και με το $\varrho\chi$.

3.2 Αθροίσματα Gauss και Jacobi

Για να εκτιμήσουμε το πλήθος των λύσεων της εξίσωσης $x^n + y^n = 1$ στο $\mathbb{F}_p$ πολύ χρήσιμο εργαλείο θα είναι τα αθροίσματα Jacobi. Η εκτίμηση της απόλυτης τιμής αυτών των αθροισμάτων, την οποία θα χρειαστούμε, θα βασιστεί στην εκτίμηση της απόλυτης τιμής των *αθροισμάτων Gauss*, τα οποία αποτελούν γενίκευση των τετραγωνικών αθροισμάτων Gauss.

Ορισμός 3.2.1. *Έστω χ χαρακτήρας από το $\mathbb{F}_p$ και $a \in \mathbb{F}_p$. Θέτουμε $g_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t)\zeta^{at}$, όπου $\zeta = e^{\frac{2\pi i}{p}}$. Το $g_a(\chi)$ λέγεται άθροισμα Gauss πάνω από το $\mathbb{F}_p$ που ανήκει στον χαρακτήρα χ. Αντί για $g_1(\chi)$, θα γράφουμε, απλούστερα, $g(\chi)$.*

Πρόταση 3.2.2.

1. $\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$.
2. $g_a(\chi) = \begin{cases} \chi(a^{-1})g(\chi)\,, & \text{αν } a \neq 0 \text{ και } \chi \neq \varepsilon \\ 0\,, & \text{αν } (a \neq 0 \text{ και } \chi = \varepsilon) \text{ είτε } (a = 0 \text{ και } \chi \neq \varepsilon) \\ p\,, & \text{αν } a = 0 \text{ και } \chi = \varepsilon \end{cases}$

Απόδειξη. **1.** Είναι $\overline{g(\chi)} = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\zeta^{-t} = \chi(-1)\sum_{t\in F_p} \overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi})$, όπου, για τον υπολογισμό του $\overline{\chi(t)}$ χρησιμοποιήσαμε την πρόταση 3.1.2(3).
2.

(i). Εάν $a \neq 0$ και $\chi \neq \varepsilon$, τότε

$$\chi(a)g_a(\chi) = \chi(a)\sum_{t\in\mathbb{F}_p} \chi(t)\zeta^{at} = \sum_{t\in\mathbb{F}_p} \chi(at)\zeta^{at} = \sum_{\mu\in\mathbb{F}_p} \chi(\mu)\zeta^{\mu} = g(\chi)\ .$$

Άρα $g_a(\chi) = \chi(a)^{-1}g(\chi) = \chi(a^{-1})g(\chi)$.

(ii). Εάν $a \neq 0$ και $\chi = \varepsilon$, τότε

$$g_a(\varepsilon) = \sum_{t\in\mathbb{F}_p} \varepsilon(t)\zeta^{at} = \sum_{t\in\mathbb{F}_p} \zeta^{at} = 0$$

Η τελευταία ισότητα ισχύει από το λήμμα 2.4.4 .

(iii). Εάν $a = 0$ και $\chi \neq \varepsilon$, τότε

$$g_0(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t) = 0$$

Η τελευταία ισότητα ισχύει από την πρόταση 3.1.3.

(iv). Εάν $a = 0$ και $\chi = \varepsilon$, τότε

$$g_0(\varepsilon) = \sum_{t\in\mathbb{F}_p} \varepsilon(t) = \sum_{t\in\mathbb{F}_p} 1 = p$$

□

Θεώρημα 3.2.3. *Εάν $\chi \neq \varepsilon$, τότε $|g(\chi)| = \sqrt{p}$.*

Απόδειξη. Υπολογίζουμε το $\sum_{a\in\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)}$ με δύο τρόπους και εξισώνουμε τα δύο αποτελέσματα. Στους παρακάτω υπολογισμούς κάνουμε χρήση της πρότασης 3.1.2.

Για $a \neq 0$, από την πρόταση 3.2.2, έχουμε, $g_a(\chi) = \chi(a^{-1})g(\chi)$ και $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = (\chi(a^{-1}))^{-1}\overline{g(\chi)} = \chi(a)\,\overline{g(\chi)}$. Άρα,

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = \chi(a^{-1}\cdot a)g(\chi)\overline{g(\chi)} = g(\chi)\overline{g(\chi)} = |g(\chi)|^2.$$

Επομένως, έχουμε

$$\sum_{a\in\,\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} \overset{*}{=} \sum_{a\in\,\mathbb{F}_p^*} g_a(\chi)\overline{g_a(\chi)} = \sum_{a\in\,\mathbb{F}_p^*} |g(\chi)|^2 = |g(\chi)|^2 \sum_{a\in\,\mathbb{F}_p^*} 1 = (p-1)|g(\chi)|^2.$$

Η ισότητα (*) ισχύει διότι όταν $\chi \neq \varepsilon$, τότε $g_0(\chi) = 0$ (πρόταση 3.2.2).
Επίσης,

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in\,\mathbb{F}_p}\sum_{y\in\,\mathbb{F}_p} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}$$

Επομένως, είναι

$$\sum_{a\in\,\mathbb{F}_p} g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in\,\mathbb{F}_p}\sum_{y\in\,\mathbb{F}_p} \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p$$

όπου $\delta(x,y) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}$ (βλ. πόρισμα 2.4.5). Άρα, $(p-1)|g(\chi)|^2 = (p-1)p$, απ' όπου προκύπτει αμέσως η αποδεικτέα.

□

Όταν χ είναι ο χαρακτήρας που προκύπτει από το σύμβολο του Legendre, από την παραπάνω σχέση, με χρήση της πρότασης 3.2.2, προκύπτει ακριβώς η πρόταση 2.2.3:

$$g(\chi)^2 = (-1)^{\frac{p-1}{2}}p.$$

Θεωρούμε τώρα την εξίσωση $x^2 + y^2 = 1$ πάνω από το σώμα $\mathbb{F}_p$. Το $\mathbb{F}_p$ είναι πεπερασμένο, επομένως η εξίσωση έχει πεπερασμένες το πλήθος λύσεις. Έστω ότι αυτό το πλήθος είναι $N_p(x^2 + y^2 = 1)$. Θα προσδιορίσουμε την τιμή του. Παρατηρούμε ότι

$$N_p(x^2 + y^2 = 1) = \sum_{a,b\in\mathbb{F}_p\,:\,a+b=1} N_p(x^2 = a)N_p(y^2 = b).$$

όπου $N_p(x^2=1) = 1 + \left(\frac{a}{p}\right)$ (βλ. Θεώρημα 3.1.9) . Επομένως

$$\begin{aligned} N_p(x^2+y^2=1) &= \sum_{a,b\in\mathbb{F}_p\,:\,a+b=1} \left(\left(\frac{a}{p}\right)+1\right)\left(\left(\frac{b}{p}\right)+1\right) \\ &= \sum_{a,b\in\mathbb{F}_p\,:\,a+b=1} \left(1+\left(\frac{a}{p}\right)+\left(\frac{b}{p}\right)+\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right) \\ &= p+\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)+\sum_{b\in\mathbb{F}_p}\left(\frac{b}{p}\right)+\sum_{a,b\in\mathbb{F}_p:a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \\ &= p+\sum_{a,b\in\mathbb{F}_p:a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \end{aligned}$$

διότι από το λήμμα (2.4.6) ισχύει $\sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right) = \sum_{b\in\mathbb{F}_p}\left(\frac{b}{p}\right) = 0$.

Θα δούμε ότι

$$\sum_{a,b\in\mathbb{F}_p\,:a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -(-1)^{\frac{p-1}{2}}.$$

Άρα

$$N_p(x^2+y^2=1) = \begin{cases} = p-1, & \text{εάν } p\equiv 1 \pmod 4 \\ = p+1, & \text{εάν } p\equiv 3 \pmod 4. \end{cases}$$

□

Επιχειρούμε τώρα να εκτιμήσουμε το $N_p(x^3+y^3=1)$:

$$N_p(x^3+y^3=1) = \sum_{a,b\in\mathbb{F}_p\,:\,a+b=1} N_p(x^3=a)N_p(y^3=b)$$

Εάν $p \equiv 2 \pmod 3$, τότε $(3, p-1) = 1$. Άρα, από την πρόταση 3.5.3 (βλ. Παραρτημα 3.5) $N_p(x^3=a) = 1, \forall a \in F_p$. Έπεται ότι

$$N_p(x^3+y^3=1) = p\ .$$

Εάν $p \equiv 1 \pmod 3$ και θεωρήσουμε χαρακτήρα $\chi, \chi \neq \varepsilon$ τάξεως 3, τότε $\chi^2 \neq \varepsilon$ και ο χ^2 είναι, επίσης, τάξεως 3. Άρα, οι $\varepsilon, \chi, \chi^2$ είναι όλοι οι χαρακτήρες τάξεως 3 (κυβικοί χαρακτήρες). Από το θεώρημα 3.1.9 έχουμε

$$N_p(x^3=a) = \sum_{\chi^3=\varepsilon}\chi(a) = 1+\chi(a)+\chi^2(a)\ ,$$

άρα,

$$\begin{aligned} N_p(x^3+y^3=1) &= \sum_{a+b=1} \big(1+\chi(a)+\chi^2(a)\big)\big(1+\chi(b)+\chi^2(b)\big) \\ &= \sum_{a+b=1} (1+\chi(a)+\chi^2(a)+\chi(b)+\chi(a)\chi(b)+\chi^2(a)\chi(b) \\ &\qquad +\chi^2(b)+\chi(a)\chi^2(b)+\chi^2(a)\chi^2(b)) \\ &= \sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{a+b=1} \chi^i(a)\chi^j(b) \end{aligned}$$

□

Από τα παραπάνω βλέπουμε ότι, για να ολοκληρώσουμε τη μελέτη των $N_p(x^2+y^2=1)$ και $N_p(x^3+y^3=1)$ χρειάζεται να μελετήσουμε αθροίσματα όπως αυτά τα τελευταία, που εμφανίζονται στην παραπάνω σχέση. Πρόκειται για τα λεγόμενα αθροίσματα Jacobi.

Ορισμός 3.2.4. *Έστω χ, λ χαρακτήρες του $\mathbb{F}_p$. Θέτουμε*

$$J(\chi,\lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

Το $J(\chi,\lambda)$ λέγεται άθροισμα Jacobi.

Το ακόλουθο θεώρημα δείχνει μία εντυπωσιακή σύνδεση αθροισμάτων Jacobi και Gauss.

Θεώρημα 3.2.5. *Στα παρακάτω χ και λ είναι μη τετριμμένοι χαρακτήρες. Ισχύουν τα εξής:*

1. $J(\varepsilon,\varepsilon) = p$.
2. $J(\varepsilon,\chi) = 0$.
3. $J(\chi,\chi^{-1}) = -\chi(-1)$.
4. *Εάν $\chi\cdot\lambda \neq \varepsilon$, τότε* $J(\chi,\lambda) = \dfrac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Απόδειξη.

1. $J(\varepsilon,\varepsilon) = \sum_{a+b=1}\varepsilon(a)\varepsilon(b) = \sum_{a+b=1} 1 = \sum_{a\in\mathbb{F}_p} 1 = p$.

2. $J(\varepsilon,\chi) = \sum_{a+b=1}\varepsilon(a)\chi(b) = \sum_{b\in\mathbb{F}_p}\chi(b) = 0$.
Η τελευταία ισότητα ισχύει από την πρόταση 3.1.3.

3. Έχουμε διαδοχικά:

$$\begin{aligned} J(\chi,\chi^{-1}) &= \sum_{a+b=1}\chi(a)\chi^{-1}(b) \\ &= \chi(1)\chi^{-1}(0)+\sum_{a+b=1,b\neq 0}\chi(a)\chi(b)^{-1} \\ &= 0+\sum_{a+b=1,b\neq 0}\chi(a)\chi(b^{-1}) \\ &= \sum_{a+b=1,b\neq 0}\chi\left(\frac{a}{b}\right) \\ &= \sum_{a\neq 1}\chi\left(\frac{a}{1-a}\right) \end{aligned} \tag{3.1}$$

Για $a\in\mathbb{F}_p$, $a\neq 1$, έστω $c=\frac{a}{1-a}$. Τότε $c\in\mathbb{F}_p$ και $c\neq -1$. Πράγματι, αάν $c=-1$, τότε $\frac{a}{1-a}=-1$, δηλαδή, $a=a-1$, αδύνατο. Έτσι, η (3.1) γράφεται τώρα

$$J(\chi,\chi^{-1})=\sum_{c\in\mathbb{F}_p,c\neq -1}\chi(c)=0-\chi(-1)=-\chi(-1).$$

4. Έχουμε

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_{x=0}^{p-1}\chi(x)\zeta^x\right)\left(\sum_{y=0}^{p-1}\lambda(y)\zeta^y\right) \\ &= \sum_{x,y=0}^{p-1}\chi(x)\lambda(y)\zeta^{x+y} \\ &= \sum_{t=0}^{2p-2}\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)\zeta^t \\ &= \sum_{t=0}^{p-1}\left(\sum_{x+y\equiv t \pmod p}\chi(x)\lambda(y)\right)\zeta^t \end{aligned}$$

Εάν $t=0$, τότε

$$\begin{aligned} \sum_{x+y=0}\chi(x)\lambda(y) &= \sum_{x=0}^{p-1}\chi(x)\lambda(-x)=\lambda(-1)\sum_{x=0}^{p-1}\chi(x)\lambda(x) \\ &= \lambda(-1)\sum_{x=0}^{p-1}\chi\lambda(x)=\lambda(-1)\cdot 0=0 \end{aligned}$$

Εάν $t \neq 0$, τότε ορίζουμε τα x', y' από τις σχέσεις $x = tx', y = ty'$, οπότε, η αντικατάσταση στην $x + y = t$, δίνει $x' + y' = 1$ και

$$\begin{aligned}\sum_{x+y=t} \chi(x)\lambda(y) &= \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi(t)\lambda(t) \sum_{x'+y'=1} \chi(x')\lambda(y') \\ &= \chi\lambda(t)J(\chi,\lambda)\end{aligned}$$

Επομένως,

$$\begin{aligned}g(\chi)g(\lambda) &= \sum_{t\in\mathbb{F}_p^*} \chi\lambda(t)J(\chi,\lambda)\zeta^t + 0\cdot\zeta^0 = \sum_{t\in\mathbb{F}_p} \chi\lambda(t)J(\chi,\lambda)\zeta^t \\ &= J(\chi,\lambda)\sum_{t\in\mathbb{F}_p} \chi\lambda(t)\zeta^t = J(\chi,\lambda)g(\chi\lambda).\end{aligned}$$

Έχουμε από υπόθεση ότι $\chi\lambda \neq \varepsilon$, άρα από την πρόταση 3.2.2, είναι $g(\chi,\lambda) \neq 0$. Άρα,

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

□

Πόρισμα 3.2.6. *Εάν χ, λ και $\chi\lambda$ δεν είναι ίσα με ε, τότε*

$$|J(\chi,\lambda)| = \sqrt{p}$$

Απόδειξη. Από το (4) του θεωρήματος 3.2.5 έπεται ότι

$$|J(\chi,\lambda)| = |\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}| = \frac{|g(\chi)||g(\lambda)|}{|g(\chi\lambda)|} \overset{*}{=} \frac{\sqrt{p}\sqrt{p}}{\sqrt{p}} = \sqrt{p}$$

Στην ισότητα (*) χρησιμοποιούμε το γεγονός ότι $\chi, \lambda, \chi\lambda \neq \varepsilon$ και εφαρμόζουμε το θεώρημα 3.2.3

□

Επιστρέφουμε στην ανάλυση των $N_p(x^2 + y^2 = 1)$ και $N_p(x^3 + y^3 = 1)$.

Στην περίπτωση του $N_p(x^2 + y^2 = 1)$ χρειάζεται να εκτιμήσουμε το άθροισμα $\sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Το (3) του θεωρήματος 3.2.5 δίνει το αποτέλεσμα $-\left(\frac{-1}{p}\right) = -(-1)^{\frac{p-1}{2}}$.

Στην περίπτωση του $N_p(x^3 + y^3 = 1)$ είχαμε να υπολογίσουμε τα αθροίσματα $\sum_{a+b=1} \chi^i(a)\chi^j(b)$, όπου χ είναι κυβικός χαρακτήρας και $i, j = 0, 1, 2$. Η εφαρμογή του θεωρήματος 3.2.5 δίνει

$$\begin{aligned}N_p(x^3 + y^3 = 1) &= p + 0 + 0 + 0 + J(\chi,\chi) - \chi^2(-1) + 0 - \chi(-1) + J(\chi^2,\chi^2) \\ &= p - \chi^2(-1) - \chi(-1) + J(\chi,\chi) + J(\chi^2,\chi^2)\end{aligned}$$

Έχουμε $\chi(-1) = \chi\left((-1)^3\right) = \chi^3(-1) = \varepsilon(-1) = 1$. Επιπλέον, $\chi^3 = \varepsilon$ άρα $\chi^2 = \chi^{-1} = \overline{\chi}$. Άρα, από τη σχέση

$$J(\chi,\chi) + J(\chi^2,\chi^2) = J(\chi,\chi) + J(\overline{\chi},\overline{\chi}) = J(\chi,\chi) + \overline{J(\chi,\chi)} = 2\Re J(\chi,\chi)$$

έχουμε

$$N_p(x^3+y^3=1) = p - 2 + 2\Re J(\chi,\chi)\,. \tag{3.2}$$

Γνωρίζουμε ότι

$$|J(\chi,\lambda)| = \sqrt{p}\,,$$

άρα,

$$|N_p(x^3+y^3=1) - p + 2| = 2|\Re J(\chi,\chi)| \leq 2\sqrt{p}, \tag{3.3}$$

όπου χρησιμοποιήσαμε την ιδιότητα $|\Re z| \leq |z|$ και το θεώρημα 3.2.5.

Εάν N_p είναι το πλήθος των λύσεων της $x^3+y^3=1$ στο $\mathbb{F}_p$, τότε η παραπάνω σχέση μας οδηγεί στο συμπέρασμα ότι το N_p είναι της τάξεως του p, με ένα σφάλμα της τάξεως του $2\sqrt{p}$. Αυτό δείχνει ότι, για αρκετά μεγάλους πρώτους p, η παραπάνω εξίσωση έχει πολλές λύσεις.

Εάν $p \equiv 1 \pmod 3$, πάντα υπάρχουν τουλάχιστον έξι λύσεις, καθώς οι $x^3 = 1$ και $y^3 = 1$ έχουν τρεις λύσεις η κάθε μία. Για $p = 7, 13$ αυτές είναι οι μόνες λύσεις. Για $p = 19$ υπάρχουν και άλλες λύσεις. Για παράδειγμα, $3^3 + 10^3 \equiv 1 \pmod{19}$. Αυτές οι «μη-τετριμμένες» λύσεις υπάρχουν για κάθε πρώτο $p \geq 19$, αφού τότε, από τον τύπο (3.3), $N_p \geq p - 2 - 2\sqrt{p} > 8$.

3.3 Θεωρήματα αναπαράστασης πρώτων.

Σ' αυτό το κεφάλαιο αποδεικνύουμε τα δύο όμορφα κλασικά θεωρήματα 3.3.1 και 3.3.6. Αναφέρονται σε αναπαραστάσεις πρώτων από δυαδικές τετραγωνικές μορφές και τα αποδεικνύουμε με τη βοήθεια της θεωρίας των αθροισμάτων Jacobi, που μέχρι τώρα αναπτύξαμε.

Θεώρημα 3.3.1.

1. *Κάθε πρώτος $p \equiv 1 \pmod 4$ γράφεται με τη μορφή $a^2 + b^2 = p$ για κατάλληλους ακεραίους a, b.*

2. *Κάθε πρώτος $p \equiv 1 \pmod 3$ γράφεται με τη μορφή $a^2 - ab + b^2 = p$ για κατάλληλους ακεραίους a, b.*

Απόδειξη.

1. Εάν $p \equiv 1 \pmod 4$, τότε υπάρχει χαρακτήρας χ τάξης 4[3]. Οι τιμές του

[3]η ύπαρξη έπεται από την πρόταση 3.5.1 (βλ. παράρτημα 3.5) και από το γεγονός ότι η όμαδα των χαρακτήρων στο $\mathbb{F}_p$ είναι κυκλική τάξεως $p-1$ (βλ. πρόταση 3.1.5).

χ ανήκουν στο σύνολο $\{1,-1,i,-i\}$. Επομένως, το $J(\chi,\chi)=\sum_{s+t=1}\chi(s)\chi(t)$ είναι στοιχείο του $\mathbb{Z}[\omega]$, που σημαίνει ότι $J(\chi,\chi)=a+bi$ για κατάλληλους ακεραίους a,b, οπότε, $p=J(\chi,\chi)|^2=a^2+b^2$.

2. Εάν $p\equiv 1 \pmod 3$, τότε, κατ' αναλογία με την προηγούμενη περίπτωση, υπάρχει χαρακτήρας χ τάξης 3. Οι τιμές του χ ανήκουν στο σύνολο $\{1,\omega,\omega^2\}$, όπου ω είναι η πρωταρχική κυβική ρίζα της μονάδας. Επομένως, $J(\chi,\chi)=\sum_{s+t=1}\chi(s)\chi(t)\in\mathbb{Z}[\omega]$, που σημαίνει ότι $J(\chi,\chi)=a+b\omega$ για κατάλληλους ακεραίους a,b, οπότε, από το πόρισμα 3.2.6, $p=|J(\chi,\chi)|^2=a^2-ab+b^2$. □

Το γεγονός ότι οι πρώτοι της μορφής $p\equiv 1 \pmod 4$ γράφονται ως άθροισμα δύο τετραγώνων ανακαλύφθηκε από τον Fermat. Δεν είναι δύσκολο να αποδειχτεί ότι, υπό τους περιορισμούς $a,b>0$, a περιττός, b άρτιος, η αναπαράσταση $p=a^2+b^2$ είναι μοναδική.

Αντίθετα, για τους πρώτους $p\equiv 1 \pmod 3$, η αναπαράσταση $p=a^2-ab+b^2$ δεν είναι μοναδική, όπως φαίνεται από τις σχέσεις

$$a^2-ab+b^2=(b-a)^2-(b-a)b+b^2=a^2-(a-b)a+(a-b)^2\ .$$

Ωστόσο, μπορούμε να θέσουμε τους περιορισμούς ώστε η αναπαράσταση να είναι μοναδική, ως εξής: Εάν $p=a^2-ab+b^2$, τότε $4p=(2a-b)^2+3b^2=(2b-a)^2+3a^2=(a+b)^2+3(a-b)^2$. Ισχυριζόμαστε ότι το 3 διαιρεί κάποιο από τα $a,b,a-b$. Γιατί, σε αντίθετη περίπτωση, είτε $a\equiv 1 \pmod 3$ & $b\equiv 2 \pmod 3$, είτε $a\equiv 2 \pmod 3$ & $b\equiv 1 \pmod 3$. Αλλά τότε, και στις δύο περιπτώσεις, διαπιστώνεται αμέσως ότι $p=a^2-ab+b^2\equiv 0 \pmod 3$, άτοπο.

Πρόταση 3.3.2. *Έστω ακέραιος $n\geq 3$, πρώτος $p\equiv 1 \pmod n$ και χ χαρακτήρας του $\mathbb{F}_p$ τάξης n. Τότε*

$$g(\chi)^n=p\chi(-1)J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})\ .$$

Απόδειξη. Εφαρμόζοντας το (4) του θεωρήματος 3.2.5για $\lambda=\chi,\chi^2,\ldots,\chi^{n-2}$, παίρνουμε διαδοχικά:

$$\begin{aligned} J(\chi,\chi) &= \frac{g(\chi)^2}{g(\chi^2)}\\ J(\chi,\chi^2) &= \frac{g(\chi)g(\chi^2)}{g(\chi^3)}\\ \vdots &\qquad \vdots\\ J(\chi,\chi^{n-2}) &= \frac{g(\chi)g(\chi^{n-2})}{g(\chi^{n-1})} \end{aligned}$$

Πολλαπλασιάζοντας κατά μέλη, παίρνουμε

$$g(\chi)^{n-1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{n-2})g(\chi^{n-1}).$$

Εφαρμόζοντας διαδοχικά τις προτάσεις 3.1.2(3) (απ' όπου $\chi^{n-1} = \chi^{-1} = \overline{\chi}$), 3.1.3(1) και το θεώρημα 3.2.5 έχουμε

$$g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = g(\chi)\chi(-1)\overline{g(\chi)} = \chi(-1)|g(\chi)|^2 = \chi(-1)p.$$

Το ζητούμενο έπεται αμέσως.

□

Πόρισμα 3.3.3. *Εάν ο χ είναι κυβικός χαρακτήρας, τότε $g(\chi)^3 = pJ(\chi,\chi)$.*

Απόδειξη. Έχουμε $\chi(-1) = \chi((-1)^3) = \chi^3(-1) = \varepsilon(-1) = 1$. Συνδυάζοντας αυτό με την πρόταση 3.3.2, έχουμε $g(\chi)^3 = pJ(\chi,\chi)$.

□

Πρόταση 3.3.4. *Έστω $p \equiv 1 \pmod 3$ και χ κυβικός χαρακτήρας. Θέτουμε $J(\chi,\chi) = a + b\omega$. Τότε $b \equiv 0 \pmod 3$ και $a \equiv -1 \pmod 3$.*

Απόδειξη. Δουλεύουμε με ισοτιμίες στον δακτύλιο των αλγεβρικών ακεραίων. Το ζ είναι μία πρωταρχική p-οστή ρίζα της μονάδας.

$$g(\chi)^3 = (\sum_{t\in\mathbb{F}_p}\chi(t)\zeta^t)^3 \equiv \sum_{t\in\mathbb{F}_p}\chi(t)^3\zeta^{3t} \pmod 3 .$$

Από υπόθεση $\chi^3 = \varepsilon$, άρα $\chi^3(t) = 1$ για κάθε $t \neq 0$ και $\chi^3(0) = 0$. Συνεπώς,

$$g(\chi)^3 = \sum_{t\in\mathbb{F}_p}\chi(t)^3\zeta^{3t} = \sum_{t\in\mathbb{F}_p^*}\zeta^{3t} \overset{\zeta^3\neq 1}{=} \sum_{t\in\mathbb{F}_p}\zeta^{3t} - \zeta^0 = 0 - 1 = -1$$

Άρα,

$$-1 \equiv g(\chi)^3 = pJ(\chi,\chi) \equiv 1\cdot(a+b\omega) = a + b\omega \pmod 3 .$$

Δουλεύοντας με το $\overline{\chi}$ αντί του χ, και επειδή, αφού $\chi(-1) = 1$, είναι $\overline{g(\chi)} = g(\overline{\chi})$, έχουμε ότι

$$-1 \equiv g(\overline{\chi})^3 \overset{*}{=} pJ(\overline{\chi},\overline{\chi}) = p\overline{J(\chi,\chi)} \equiv 1\cdot(a+b\overline{\omega}) = a + b\overline{\omega} \pmod 3 ,$$

όπου για την ισότητα **(*)** χρησιμοποιήσαμε το πόρισμα 3.3.3. Άρα,

$$0 = g(\chi) - g(\overline{\chi}) \equiv (a+b\omega) - (a+b\overline{\omega}) = b(\omega - \overline{\omega}) = b\sqrt{-3} \pmod 3 .$$

Συνεπώς, $-3b^2 \equiv 0 \pmod 9$, άρα $3|b$. Τώρα, οι σχέσεις $3|b$ και $a + b\omega \equiv -1 \pmod 3$ συνεπάγονται την $a \equiv -1 \pmod 3$.

□

Πρόταση 3.3.5. *Εάν $p \equiv 1 \pmod 3$, τότε υπάρχουν $A, B \in \mathbb{Z}$ τέτοια ώστε $4p = A^2 + 27B^2$ και $A \equiv 1 \pmod 3$. Σε αυτή την αναπαράσταση του p το A είναι μονοσήμαντα ορισμένο.*

Απόδειξη. Η ύπαρξη των A, B εξασφαλίζεται από την πρόταση 3.3.4. Πράγματι, αν θέσουμε $A = 2a - b$ και $B = \frac{b}{3}$, τότε $A \equiv 1 \pmod 3$ και $4p = A^2 + 27B^2$.
Έστω A_1, B_1 και A_2, B_2 τέτοια ώστε

$$4p = A_1^2 + 27B_1^2 \qquad \text{και} \qquad 4p = A_2^2 + 27B_2^2 \tag{3.4}$$

και $A_1 \equiv A_2 \equiv 1 \pmod 3$.

Εστω ότι A_i άρτιος και B_i περιττός ($i = 1$ ή 2), δηλαδή υπάρχουν $k, m \in \mathbb{Z}$ ώστε $A_i = 2k$ και $B_i = 2m+1$. Τότε $4p = A_i^2 + 27B_i^2 = 4(k^2 + 27m^2 + 27m + 6) + 3$, δηλαδή $4 \not| 4p$, το οποίο είναι άτοπο. Όμοια, έστω ότι A_i περιττός και B_i άρτιος, δηλαδή υπάρχουν $k, m \in \mathbb{Z}$ ώστε $A_i = 2k+1$ και $B_i = 2m$. Τότε $4p = A_i^2 + 27B_i^2 = 4(k^2 + k + 27m^2 +) + 1$, δηλαδή $4 \not| 4p$, το οποίο είναι άτοπο. Άρα, οι A_i, B_i είναι ομότυποι για κάθε i. Επομένως, $A_2B_1 \pm A_1B_2$ είναι άρτιοι, δηλαδή διαιρούνται από το 2.

Ισχυριζόμαστε ότι ένας από τους $A_2B_1 \pm A_1B_2$ διαιρείται δια p. Πράγματι, εάν $A_i = 2a_i - b_i$ και $B_i = b_i/3$, όπου $p = a_i^2 - a_ib_i + b_i^2$ και $a_i \equiv -1 \pmod 3$, έχουμε

$$\begin{aligned} A_2B_1 + A_1B_2 &= (2a_2 - b_2)b_1/3 + (2a_1 - b_1)b_2/3 = 2\frac{a_2b_1}{3} + 2\frac{a_1b_2}{3} - 2\frac{b_1b_2}{3}, \\ A_2B_1 - A_1B_2 &= (2a_2 - b_2)b_1/3 - (2a_1 - b_1)b_2/3 = 2\frac{a_2b_1}{3} - 2\frac{a_1b_2}{3} \end{aligned}$$

απ' όπου

$$\begin{aligned} (A_2B_1 + A_1B_2)(A_2B_1 - A_1B_2) &= \left(2\frac{a_2b_1}{3} + 2\frac{a_1b_2}{3} - 2\frac{b_1b_2}{3}\right)\left(2\frac{a_2b_1}{3} - 2\frac{a_1b_2}{3}\right) = \\ = \frac{4}{9}\left(a_2^2b_1^2 - a_2b_1^2b_2 + a_1b_1b_2^2 - a_1^2b_2^2\right) &= \frac{4}{9}\left(b_1^2(a_2^2 - a_2b_2) - b_2^2(a_1^2 - a_1b_1)\right) = \\ = \frac{4}{9}\left(b_1^2(p - b_2^2) - b_2^2(p - b_1^2)\right) &= \frac{4}{9}\left(b_1^2p - b_1^2b_2^2 - b_2^2p + b_2^2b_1^2\right) = \\ = \frac{4}{9}\left(b_1^2p - b_2^2p\right) &= \frac{4}{9}p(b_1^2 - b_2^2) \end{aligned}$$

Άρα, $9\,(A_2B_1 + A_1B_2)\,(A_2B_1 - A_1B_2) = 4p\,(b_1^2 - b_2^2)$,
δηλαδή $p \,|\, 9\,(A_2B_1 + A_1B_2)\,(A_2B_1 - A_1B_2)$.
Όμως, από υπόθεση, $p \equiv 1 \pmod 3$, άρα $p \,|\, (A_2B_1 + A_1B_2)$ ή $p \,|\, (A_2B_1 - A_1B_2)$.

Επομένως, ένας από τους $A_2B_1 \pm A_1B_2$ είναι διαιρετός δια $2p$, έστω ότι είναι $A_2B_1 + \varepsilon A_1B_2$ όπου $\varepsilon = \pm 1$. Οπότε, εάν $|A_2B_1 + \varepsilon A_1B_2|$ δεν είναι 0, είναι $\geq 2p$. Έχουμε ότι

$$|A_2B_1 + \varepsilon A_1B_2| \leq |A_2|\,|B_1| + |A_1|\,|B_2| \tag{3.5}$$

Για κάθε i, $i = 1, 2$, από τις σχέσεις (3.4) έχουμε

$$\begin{aligned} A_i^2 &= 4p - 27B_i^2 < 4p \text{ και} \\ B_i^2 &= \frac{1}{27}(4p - A_i^2) < \frac{1}{27}4p < \frac{1}{25}4p \end{aligned}$$

Συνεπώς, είναι

$$|A_i| < 2\sqrt{p} \qquad \text{και} \qquad |B_i| < \frac{2}{5}\sqrt{p}.$$

Άρα, η (3.5) γίνεται

$$|A_2B_1 + \varepsilon A_1B_2| < (2\sqrt{p})\left(\frac{2}{5}\sqrt{p}\right) + (2\sqrt{p})\left(\frac{2}{5}\sqrt{p}\right) = \frac{4}{5}\,2p < 2p\,.$$

Οπότε, $|A_2B_1+\varepsilon A_1B_2| = 0$, άρα $A_2B_1+\varepsilon A_1B_2 = 0$. Τότε $A_1b_2 = \pm A_2B_1$, δηλαδή

$$\frac{A_1}{B_1} = \pm\frac{A_2}{B_2} \tag{3.6}$$

Παρατηρούμε ότι εάν A_i, B_i είναι περιττοί, τότε $(A_i, B_i) = 1$. Έστω ότι $(A_i, B_i) > 1$. Τότε υπάρχει πρώτος $q(> 2)$ ώστε $q|A_i$ και $q|B_i$, δηλαδή $A_i = cq$, $c \in \mathbb{Z}$ και $B_i = dq$, $d \in \mathbb{Z}$. Οπότε $4p = (c^2 + 27d^2)q^2$, που σημαίνει ότι $q^2|4p$, άρα $q|p$, το οποίο είναι άτοπο.
Αντίστοιχα, παρατηρούμε ότι εάν A_i, B_i είναι άρτιοι, τότε $(A_i, B_i) = 2$. Έστω ότι $(A_i, B_i) > 2$, δηλαδή $(A_i, B_i) = 4k$, $k \in \mathbb{N}$. Τότε $A_i = 4kc$, $c \in \mathbb{Z}$ και $B_i = 4kd$, $d \in \mathbb{Z}$. Οπότε $4p = (16k^2c^2 + 2716k^2d^2)q^2$, που σημαίνει ότι $16|4p$, άρα, αφού ο p είναι περιττός πρώτος, $16|4$, το οποίο είναι άτοπο.

Εάν A_1, B_1 και A_2, B_2 είναι περιττοί, τότε $(A_1, B_1) = 1$ και $(A_2, B_2) = 1$. Συνεπώς, από την (3.6) έπεται ότι $|A_1| = |A_2|$ και $|B_1| = |B_2|$. Επειδή $A_1 \equiv A_2 \pmod 3$, έχουμε ότι $A_1 = A_2$, το οποίο είναι το αποδεικτέο.

Εάν A_1, B_1 και A_2, B_2 είναι άρτιοι, τότε $(A_1, B_1) = 2$ και $(A_2, B_2) = 2$, δηλαδή $A_1 = 2A_1'$, $B_1 = 2B_1'$ για κάποια $A_1', B_1' \in \mathbb{Z}$ με $(A_1', B_1') = 1$ και $A_2 = 2A_2'$, $B_2 = 2B_2'$ για κάποια $A_2', B_2' \in \mathbb{Z}$ με $(A_2, B_2) = 1$. Συνεπώς, από την (3.6) έπεται ότι $\frac{A_1'}{B_1'} = \pm\frac{A_2'}{B_2'}$ και επειδή $(A_1', B_1') = 1$, $(A_2', B_2') = 1$, έχουμε ότι $|A_1'| = |A_2'|$ και $|B_1'| = |B_2'|$, δηλαδή $|A_1| = 2|A_1'| = 2|A_2'| = |A_2|$ και $|B_1| = 2|B_1'| = 2|B_2'| = |B_2|$. Επειδή $A_1 \equiv A_2 \pmod 3$, έπεται ότι $A_1 = A_2$, το οποίο είναι το αποδεικτέο.

Τέλος, εξετάζουμε την περίπτωση όπου το ένα ζεύγος (A_i, B_i) είναι περιττοί και το δεύτερο είναι άρτιοι. Έστω ότι A_1, B_1 είναι περιττοί και A_2, B_2 είναι άρτιοι, τότε $(A_1, B_1) = 1$ και $(A_2, B_2) = 2$. Από την τελευταία σχέση έπεται ότι υπάρχουν $A_2', B_2' \in \mathbb{Z}$ ώστε $A_2 = 2A_2'$ και $B_2 = 2B_2'$, με $(A_2', B_2') = 1$. Επομένως, η (3.6) δίνει $\frac{A_1}{B_1} = \pm\frac{A_2'}{B_2'}$ και επειδή $(A_1, B_1) = 1$, $(A_2', B_2') = 1$, έχουμε ότι $|A_1| = |A_2'|$ και $|B_1| = |B_2'|$. Άρα έχουμε $|2A_1| = |A_2|$ και $|2B_1| = |B_2|$, απ' όπου $A_2^2 = 4A_1^2$ και $B_2^2 = 4B_1^2$. Οπότε

$$4p = A_2^2 + 27B_2^2 = 4A_1^2 + 27 \cdot 4B_1^2 = 4(A_1^2 + 27B_1^2) = 16p$$

το οποίο είναι αδύνατο. Άρα, η περίπτωση αυτή αποκλείεται.

□

Θεώρημα 3.3.6. *Έστω ότι* $p \equiv 1 \pmod 3$ *και ακέραιοι* A, B *τέτοιοι ώστε* $A \equiv 1 \pmod 3$ *και* $4p = A^2 + 27B^2$*, η ύπαρξη των οποίων εξ ίσου εξασφαλίζεται από το θεώρημα 3.3.1 ή την πρόταση 3.3.5. Τότε* $N_p(x^3 + y^3 = 1) = p - 2 + A$.

Απόδειξη. Έχουμε δείξει ότι

$$N_p(x^3 + y^3 = 1) = p - 2 + 2\Re J(\chi, \chi),$$

όπου $J(\chi, \chi) = a + b\omega$, δηλαδή $\Re J(\chi, \chi) = \frac{2a-b}{2}$, άρα $2\Re J(\chi, \chi) = 2a - b = A \equiv 1 \pmod 3$.

□

3.4 Η εξίσωση $x^n + y^n = 1$ στο F_p

Υποθέτουμε ότι $p \equiv 1 \pmod n$ και εξετάζουμε το πλήθος των λύσεων της εξίσωσης $x^n + y^n = 1$ πάνω από το σώμα F_p. Έχουμε

$$N_p(x^n + y^n = 1) = \sum_{a+b=1} N_p(x^n = a) N_p(y^n = b)$$

Έστω χ ένας χαρακτήρας τάξης n. Από την πρόταση (3.1.9) είναι

$$N_p(x^n = a) = \sum_{\lambda^n = \varepsilon} \lambda(a) = \sum_{i=0}^{n-1} \chi^i(a)$$

Συνδυάζοντας τα παραπάνω έχουμε διαδοχικά

$$\begin{aligned} N_p(x^n + y^n = 1) &= \sum_{a+b=1} \sum_{i=0}^{n-1} \chi^i(a) \sum_{j=0}^{n-1} \chi^j(b) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \left(\sum_{a+b=1} \chi^i(a)\chi^j(b) \right) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} J(\chi^i, \chi^j) \\ &= J(\chi^0, \chi^0) + \sum_{i+j=n} J(\chi^i, \chi^j) + \sum_{j=1}^{n-1} J(\chi^0, \chi^j) \qquad (3.7) \\ &\quad + \sum_{i=1}^{n-1} J(\chi^i, \chi^0) + \sum_{\substack{1 \le i, j \le n-1 \\ i+j \ne n}} J(\chi^i, \chi^j)\ . \qquad (3.8) \end{aligned}$$

Παρακάτω χρησιμοποιούμε το θεώρημα 3.2.5 για να εκτιμήσουμε τα αθροίσματα στις (3.7) και (3.8). Εννοείται ότι $i, j \in \{1, \ldots, n-1\}$.

1 . Είναι $J(\chi^0, \chi^0) = J(\varepsilon, \varepsilon) = p$.

2 . Όταν $i + j = n$, τότε $\chi^j = \chi^{n-i}$ και αφού η τάξη του χ είναι n, έχουμε $\chi^{-i} = \chi^j$. Άρα, $J(\chi^i, \chi^j) = J(\chi^i, \chi^{-i})$, οπότε το δεύτερο άθροισμα στη (3.7) είναι ίσο με

$$-\sum_{i=1}^{n-1} \chi^i(-1) = \varepsilon(-1) - \sum_{i=0}^{n-1} \chi^i(-1) = 1 - N_p(x^n = -1) \ .$$

Αλλά από την πρόταση 3.5.3, η εξίσωση $x^n = -1$, $x \in \mathbb{F}_p^*$, ή δεν έχει λύση, ή το πλήθος των λύσεών της είναι ίσο με $(p-1, n) = n$. Άρα, το δεύτερο άθροισμα στη (3.7) ισούται με $1 - n\delta_n(-1)$, όπου

$$\delta_n(-1) = \begin{cases} 1, \text{ όταν -1 είναι } n\text{-οστή δύναμη} \\ 0, \text{ αλλιώς.} \end{cases}$$

3. Τέλος, όταν $i = 0$ και $j \neq 0$ ή $i \neq 0$ και $j = 0$, τότε $J(\chi^i, \chi^j) = 0$.

Επομένως,

$$N_p(x^n + y^n = 1) = p + 1 - \delta_n(-1)n + \sum_{1 \leq i,j \leq n-1, i+j \neq n} J(\chi^i, \chi^j),$$

όπου το τελευταίο άθροισμα έχει $(n-1)(n-1) - (n-1) \cdot 1 = (n-1)(n-2)$ το πλήθος όρους και όλοι έχουν απόλυτη τιμή $\sqrt{p}$. Άρα, αποδείξαμε το

Θεώρημα 3.4.1.

$$|N(x^n + y^n = 1) + \delta_n(-1)n - (p+1)| \leq (n-1)(n-2)\sqrt{p}.$$

Για μεγάλα p η παραπάνω εκτίμηση δείχνει την ύπαρξη πολλών μη-τετριμμένων λύσεων.

3.5 Παράρτημα - Βοηθητικές προτάσεις

Πρόταση 3.5.1. *Έστω G κυκλική ομάδα τάξεως m. Τότε, για κάθε θετικό διαιρέτη d του m, υπάρχει μία ακριβώς υποομάδα της G τάξεως d. Ειδικότερα, στην G υπάρχουν στοιχεία τάξεως d.*

Απόδειξη. Εάν g είναι γεννήτορας της G, δηλαδή $G =< g >$ και $a \in G$, τότε $a = g^k$, όπου $0 \leq k < m$. Έστω $d \in \mathbb{N}$ με $d|m$. Τότε, $g^{\frac{m}{d}} \in G$. Προφανώς, η τάξη του $g^{\frac{m}{d}}$ είναι ίση με d. Κάθε στοιχείο της G παράγει μία κυκλική υποομάδα της G (γνωστό από στοιχειώδη Θεωρία Ομάδων). Θεωρούμε την $H_d = \langle g^{\frac{m}{d}} \rangle =$

$\{1, g^{\frac{m}{d}}, g^{2\frac{m}{d}}, \cdots, g^{(d-1)\frac{m}{d}}\}$, υποομάδα της G με d το πλήθος στοιχεία. Τα στοιχεία της μορφής $g^{k\frac{m}{d}}$, όπου $(k,d)=1$, είναι $\phi(d)$ το πλήθος και έχουν τάξη d (από Θεωρία πεπερασμένων Ομάδων). Γνωρίζουμε όμως ότι το πλήθος των στοιχείων τάξης d στην G είναι ακριβώς $\phi(d)$. Συνεπώς, η H_d περιέχει όλα τα στοιχεία τάξης ίσης με d.

Έστω ότι υπάρχει $H < G$, $|H| = d$ και $H \neq H_d$. Τότε, υπάρχει $b \in G$ ώστε $H = \langle b \rangle$ και $b \notin H_d$. Δηλαδή, υπάρχει στοιχείο b της G, τάξης d, που δεν ανήκει στην H_d. Τότε όμως η G θα έχει $\phi(d)+1$ στοιχεία τάξης d. Άτοπο.

□

Πρόταση 3.5.2. *Έστω $(G,\cdot)$ κυκλική ομάδα τάξεως m, g ένας γεννήτοράς της και $n \in \mathbb{N}$. Τα στοιχεία της G, των οποίων η τάξη διαιρεί το n είναι τα g^k με $k = \ell\frac{m}{(m,n)}$, όπου $\ell = 0,1,\ldots,(n,m)-1$. Ειδικότερα, το πλήθος αυτών των στοιχείων είναι (n,m).*

Απόδειξη. Έστω $d=(m,n)$. Ο d είναι διαιρέτης του m, οπότε από την πρόταση 3.5.1, έχουμε ότι υπάρχει μοναδική υποομάδα H_d, με d το πλήθος στοιχεία, τα $g^{\ell\frac{m}{d}}$ όπου $\ell = 0, 1 \cdots, d-1$.

□

Πρόταση 3.5.3. *Έστω $(G,\cdot)$ κυκλική ομάδα τάξεως m, $a \in G$ και $n \in \mathbb{N}$. Τότε, η εξίσωση $x^n = a$ είναι επιλύσιμη στην G, ανν $a^{\frac{m}{(n,m)}} = 1$. Επιπλέον, αν αυτή η εξίσωση είναι επιλύσιμη, τότε έχει ακριβώς (m,n) το πλήθος διαφορετικές λύσεις.*

Απόδειξη. Εάν g γεννήτορας της G , δηλαδή $G =< g >$ και $a \in G$, τότε $a = g^k$, όπου $0 \leq k < m$. Έστω $d=(m,n)$.

Έστω ότι η $x^n = a$ έχει λύση και $x = g^\ell, 0 \leq \ell < m$ μία λύση της. Τότε $g^{\ell n} = a = g^k$, απ' όπου έπεται ότι $\ell n \equiv k \pmod m$. Οπότε $d|(k,m)$ και Θέτουμε $(k,m) = d\mu$, όπου $\mu \in \mathbb{N}$. Η τάξη του $a = g^k$ είναι ίση με $\frac{m}{(k,m)} = \frac{m}{d\mu}$.Άρα, $a^{\frac{m}{d\mu}} = 1$. Υψώνουμε στη μ και παίρνουμε $a^{\frac{m}{d}} = 1$.

Αντίστροφα, έστω ότι $a^{\frac{m}{d}} = 1$. Θέλοντας να δείξουμε ότι η εξίσωση $x^n = a$ έχει λύση, αναζητούμε λύσεις της μορφής $x = g^y$, με $0 \leq y < m$.

$$x^n = a \Leftrightarrow (g^y)^n = g^k \Leftrightarrow g^{yn} = g^k \Leftrightarrow ny \equiv k \pmod m$$

Η τελευταία ισοτιμία έχει λύση εάνν $(m,n)|k$, δηλαδή εάνν $d|k$ και τότε έχει ακριβώς $(m,n) = d$ το πλήθος λύσεις. Επειδή $a^{\frac{m}{d}} = 1$ και η τάξη του a είναι ίση με $\frac{m}{(m,k)}$, συμπεραίνουμε ότι $\frac{m}{(m,k)} | \frac{m}{d}$. Δηλαδή υπάρχει $\lambda \in \mathbb{N}$ τέτοιο ώστε $\frac{m}{d} = \lambda\frac{m}{(m,k)}$. Έπεται ότι $(m,k) = \lambda d$. Δηλαδή $d|(m,k)$, απ' όπου $d|k$, που είναι το ζητούμενο.

□

Κεφάλαιο 4

Κυβική αντιστροφή

4.1 Ο δακτύλιος $\mathbb{Z}[\omega]$

Θεωρούμε την πρωταρχική κυβική ρίζα της μονάδας $\omega = \frac{-1+\sqrt{-3}}{2}$. Τα στοιχεία του $\mathbb{Z}[\omega]$ είναι μιγαδικοί αριθμοί της μορφής $a+b\omega$, $a, b \in \mathbb{Z}$. Εάν $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, ορίζουμε τη *στάθμη* (*norm*) $\mathrm{N}\alpha$ του α μέσω του τύπου

$$\mathrm{N}\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$$

και παρατηρούμε ότι, για $\alpha \neq 0$, είναι $\mathrm{N}\alpha > 0$.

Θέτουμε $D = \mathbb{Z}[\omega]$. Το D είναι περιοχή μονοσήμαντης ανάλυσης[1]. Το πρώτο μέλημά μας είναι να ανακαλύψουμε τις μονάδες και τα πρώτα στοιχεία της D.

Πρόταση 4.1.1. *Το στοιχείο $\alpha \in D$ είναι μονάδα εάνν $\mathrm{N}\alpha = 1$. Οι μονάδες της D είναι $1, -1, \omega, -\omega, \omega^2, -\omega^2$.*

Απόδειξη. Εάν $\mathrm{N}\alpha = 1$ τότε $\alpha\overline{\alpha} = 1$. Άρα το α είναι μονάδα του δακτυλίου D διότι $\overline{\alpha} \in D$.

Αντίστροφα, εάν α είναι μονάδα, τότε υπάρχει ένα β τέτοιο ώστε $\alpha\beta = 1$. Άρα $N\alpha\mathrm{N}\beta = 1$. Οι $\mathrm{N}\alpha, \mathrm{N}\beta$ είναι θετικοί, άρα $\mathrm{N}\alpha = 1$. Συνεπώς, εάν θέσουμε $\alpha = a+b\omega$ μονάδα, τότε $1 = a^2-ab+b^2$ ή $4 = (2a-b)^2+3b^2$. Υπάρχουν δύο δυνατότητες: $2a - b = \pm 1$, $b = \pm 1$ ή $2a - b = \pm 2$, $b = 0$. Λύνοντας τα προκύπτοντα έξι ζεύγη εξισώσεων έχουμε τις εξής δυνατότητες για το α: $1, -1, \omega, -\omega, -1-\omega, 1+\omega$. Επειδή $\omega^2 + \omega + 1 = 0$, τα τελευταία δύο στοιχεία είναι τα ω^2 και $-\omega^2$.

□

[1] Η D είναι Ευκλείδεια Περιοχή, με ευκλείδεια απεικόνιση τη στάθμη N, άρα είναι Περιοχή Κυρίων Ιδεωδών και κατά συνέπεια είναι Περιοχή Μονοσήμαντης Ανάλυσης.

Για να βρούμε τους πρώτους της D είναι σημαντικό να συνειδητοποιήσουμε ότι οι πρώτοι του $\mathbb{Z}$ δεν παραμένουν απαραιτήτως πρώτοι στην D, π.χ. $7 = (3-\omega)(3+\omega)$.
Γι' αυτό το λόγο, οι πρώτοι του $\mathbb{Z}$ αναφέρονται ως *ρητοί πρώτοι* και οι πρώτοι της D απλώς αναφέρονται ως *πρώτοι*.

Πρόταση 4.1.2. *Εάν $\pi \in D$ είναι πρώτος της D, τότε υπάρχει ρητός πρώτος p τέτοιος ώστε $\mathrm{N}\pi = p$ ή p^2. Στην πρώτη περίπτωση ο π δεν είναι συνεταιρικός κάποιου ρητού πρώτου, στη δεύτερη περίπτωση ο π είναι συνεταιρικός του p.*

Απόδειξη. Έχουμε $\mathrm{N}\pi = n > 1$ ή $\pi\overline{\pi}$. Ο n είναι γινόμενο ρητών πρώτων. Άρα $\pi | p$ για κάποιο ρητό πρώτο p. Εάν $p = \pi\gamma$, $\gamma \in D$, τότε $\mathrm{N}\pi\mathrm{N}\gamma = \mathrm{N}p = p^2$. Άρα **είτε** $\mathrm{N}\pi = p^2$ και $\mathrm{N}\gamma = 1$ **ή** $\mathrm{N}\pi = p$. Στην πρώτη περίπτωση το γ είναι μονάδα και το π είναι συνεταιρικό του p. Στη δεύτερη περίπτωση, εάν $\pi = uq$, όπου u είναι μονάδα της D και q ρητός πρώτος, τότε $p = \mathrm{N}\pi = \mathrm{N}u\mathrm{N}q = q^2$, αδύνατο.

□

Πρόταση 4.1.3. *Εάν $\pi \in D$ είναι τέτοιος ώστε $\mathrm{N}\pi = p$ ρητός πρώτος, τότε ο π είναι πρώτος της D.*

Απόδειξη. Εάν ο π δεν ήταν πρώτος της D, θα αναλυόταν σε γινόμενο $\pi = \varrho\gamma$ με $\mathrm{N}\varrho, \mathrm{N}\gamma > 1$, οπότε $p = \mathrm{N}\pi = \mathrm{N}\varrho\mathrm{N}\gamma$. Αυτό είναι άτοπο διότι ο p είναι πρώτος στο $\mathbb{Z}$.

□

Η επόμενη πρόταση κατηγοριοποιεί τους πρώτους της D.

Πρόταση 4.1.4. *Κάθε ρητός πρώτος $p \equiv 1 \pmod 3$ αναλύεται στην D ως $p = \pi\overline{\pi}$, όπου ο π είναι πρώτος της D.*
Κάθε ρητός πρώτος $p \equiv 2 \pmod 3$ παραμένει πρώτος στη D.
Τέλος, $3 = -\omega^2(1-\omega)^2$ και ο $1-\omega$ είναι πρώτος στη D.

Απόδειξη. Υποθέτουμε ότι ο $p \neq 3$ δεν είναι πρώτος στη D. Τότε $p = \pi\gamma$, όπου $\mathrm{N}\pi > 1, \mathrm{N}\gamma > 1$. Επομένως $p^2 = \mathrm{N}\pi\mathrm{N}\gamma$, άρα, $\mathrm{N}\pi = \mathrm{N}\gamma = p$. Θέτοντας $\pi = a+b\omega$, έχουμε $p = a^2 - ab + b^2$, όποτε, $4p = (2a-b)^2 + 3b^2$.
Δηλαδή $p \equiv (2a-b)^2 \pmod 3$. Επειδή $3 \nmid p$, έπεται ότι $(2a-b) \not\equiv 0 \pmod 3$, άρα $p \equiv 1 \pmod 3$, γιατί το 1 είναι το μόνο μη μηδενικό τετράγωνο $\bmod 3$.

Άρα, εάν ο ρητός πρώτος p δεν είναι πρώτος της D, τότε, αναγκαστικά, είναι $p \equiv 1 \pmod 3$. Άμεση συνέπεια αυτού είναι ότι, εάν $p \equiv 2 \pmod 3$, τότε ο p είναι πρώτος της D.

Έστω τώρα ότι $p \equiv 1 \pmod 3$. Θα δείξουμε ότι ο p δεν είναι πρώτος στην D. Από το νόμο τετραγωνικής αντιστροφής έχουμε:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}} = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1^{\frac{3-1}{2}} = 1$$

Επομένως, υπάρχει $a \in \mathbb{Z}$ τέτοιο ώστε $a^2 \equiv -3 \pmod{p}$. Δηλαδή $a^2+3 = pb$, για κάποιο $b \in \mathbb{Z}$. Άρα ο p διαιρεί το

$$a^2+3 = (a-\sqrt{-3})(a+\sqrt{-3}) = (a-1-2\omega)(a+1+2\omega)$$

Εάν ο p ήταν πρώτος στην D θα έπρεπε να διαιρεί έναν από τους παράγοντες του a^2+3. Αυτό δεν μπορεί να συμβεί. Πράγματι, τότε υπάρχει $m+n\omega \in D$ τέτοιο ώστε $a+1+2\omega = p(m+n\omega)$. Από την τελευταία σχέση έπεται, ειδικότερα, ότι $2 = pn$. Άτοπο αφού $p, n \in \mathbb{Z}$ και $p > 2$. Εντελώς ανάλογα αποδεικνύουμε ότι ο p δεν διαιρεί το $a-1-2\omega$.

Τέλος, όσον αφορά στο 3, επειδή $\mathrm{N}(1-\omega) = 3$, η πρόταση 4.1.3 συνεπάγεται ότι ο $1-\omega$ είναι πρώτος.

□

Στη συνέχεια δίνουμε την έννοια του *πρώτιστου πρώτου* ώστε να μην υπάρξει σύγχυση από το γεγονός ότι κάθε μη μηδενικό στοιχείο της D έχει έξι συνεταιρικά στοιχεία.

Ορισμός 4.1.5. *Εάν π είναι πρώτος στη D, τότε λέμε ότι ο π είναι πρώτιστος (primary) εάν $\pi \equiv 2 \pmod{3}$. Εάν θέσουμε $\pi = a+b\omega$, ο ορισμός είναι ισοδύναμος με $a \equiv 2 \pmod{3}$ και $b \equiv 0 \pmod{3}$. Ειδικότερα, κάθε ρητός πρώτος $q > 0, q \equiv 2 \pmod{3}$, είναι πρώτιστος πρώτος της D.*

> **Σύμβαση συμβολισμού**: Στο εξής, το γράμμα q θα συμβολίζει ένα θετικό ρητό πρώτο $\equiv 2 \pmod{3}$, ενώ το π θα συμβολίζει πρώτο της D, του οποίου η στάθμη $\mathrm{N}\pi = p$, με p ρητό πρώτο $\equiv 1 \pmod{3}$. Περιστασιακά, το π θα αναφέρεται ως τυχών πρώτος της D. Το περιεχόμενο θα κάνει τη χρήση σαφή. Με λ θα συμβολίζουμε τον πρώτο $1-\omega$.

Όπως στον δακτύλιο $\mathbb{Z}$, έτσι και στον δακτύλιο D, η έννοια της ισοτιμίας είναι ιδιαίτερα χρήσιμη. Εάν $\alpha, \beta, \gamma \in D$ και $\gamma \neq 0$ δεν είναι μονάδα, λέμε ότι $\alpha \equiv \beta \pmod{\gamma}$ εάν το γ διαιρεί το $\alpha-\beta$. Οι κλάσεις ισοτιμιών $\bmod \gamma$ ορίζουν δακτύλιο $D/\gamma D$, που λέγεται *δακτύλιος κλάσεων* $\bmod \gamma$.

Πρόταση 4.1.6. *Έστω $\pi \in D$ πρώτος. Τότε $D/\pi D$ είναι πεπερασμένο σώμα με $\mathrm{N}\pi$ στοιχεία.*

Απόδειξη. Πρώτα δείχνουμε ότι το $K = D/\pi D$ είναι σώμα. Έστω $\alpha(\pi D)$ μη μηδενικό στοιχείο του K. Αυτό σημαίνει ότι $\alpha \not\equiv 0 \pmod{\pi}$, άρα τα α, π είναι πρώτα μεταξύ τους. Επειδή η D είναι περιοχή κυρίων ιδεωδών, έπεται ότι υπάρχουν $\beta, \gamma \in D$ τέτοια ώστε $\beta\alpha + \gamma\pi = 1$. Άρα, $\beta\alpha \equiv 1 \pmod{\pi}$, δηλαδή, $\beta(\pi D) \cdot \alpha(\pi D) = 1(\pi D)$. Άρα, κάθε μη μηδενικό στοιχείο του K έχει αντίστροφο,οπότε ο δακτύλιος K είναι σώμα.

Για να δείξουμε ότι το $D/\pi D$ έχει $\mathrm{N}\pi$ στοιχεία θεωρούμε ξεχωριστά τις τρεις περιπτώσεις πρώτων της D:

1. Έστω $\pi = q$ ρητός πρώτος, $\equiv 2 \pmod 3$. Ισχυριζόμαστε ότι το $S = \{a+b\omega | 0 \leq a, b < q\}$ είναι πλήρες σύστημα υπολοίπων $\mathrm{mod}\,\pi$. Αυτό θα δείξει ότι το σώμα D/qD έχει $q^2 = \mathrm{N}\pi$ στοιχεία. Έστω $\mu = m + n\omega \in D$. Τότε $m = qs + a$ και $n = qt + b$, με $s, t, a, b \in \mathbb{Z}$ και $0 \leq a, b < q$. Προφανώς, $\mu \equiv a + b\omega \pmod q$ και $a + b\omega \in S$.
Θα δείξουμε ότι όλα τα στοιχεία του S είναι διαφορετικά. Πράγματι, ας υποθέσουμε ότι $a + b\omega \equiv a' + b'\omega \pmod q$, όπου $0 \leq a, a', b, b' < q$. Τότε $a - a' + (b - b')\omega = q(c + d\omega)$ για κάποια $c, d \in \mathbb{Z}$. Αυτό συνεπάγεται τις σχέσεις $q|(a - a')$ και $q|(b - b')$, οι οποίες είναι δυνατό να ισχύουν εάν και μόνο εάν $a = a'$ και $b = b'$, αφού $0 \leq a, a', b, b' < q$.

2. Έστω τώρα $p \equiv 1 \pmod 3$ ρητός πρώτος και $\pi\overline{\pi} = \mathrm{N}\pi = p$. Θα δείξουμε ότι το $P = \{0, 1, ..., p-1\}$ είναι ένα πλήρες σύστημα αντιπροσώπων κλάσεων. Αυτό, ειδικότερα, θα έχει ως συνέπεια ότι το σώμα $K = D/\pi D$ έχει $p = \mathrm{N}\pi$ το πλήθος στοιχεία. Θέτουμε $\pi = a + b\omega$. Αφού $p = a^2 - ab + b^2$, έπεται ότι $p \not| b$.
Έστω τώρα τυχόν $\mu = m + n\omega$. Υπάρχει $c \in \mathbb{Z}$ τέτοιο ώστε $cb \equiv n \pmod p$. Τότε $\mu - c\pi = m + n\omega - ca - cb\omega \equiv m - ca \pmod p$, άρα, $\mu \equiv m - ca \pmod \pi$ και $m - ca \in P$. Πρέπει να δείξουμε, επίσης, ότι τα στοιχεία του P είναι διαφορετικά $\mathrm{mod}\pi$. Πράγματι, διότι τα στοιχεία του P είναι διαφορετικά $\mathrm{mod}\, p$, οπότε η πρόταση 4.6.3 μας λέει ότι είναι διαφορετικά $\mathrm{mod}\pi$.

3. Εάν $\pi = 1 - \omega = \lambda$, θα δείξουμε ότι $\{-1, 0, 1\}$ είναι ένα πλήρες σύστημα αντιπροσώπων κλάσεων. Αυτό, ειδικότερα, θα έχει ως συνέπεια ότι το σώμα $K = D/\lambda D$ έχει $3 = \mathrm{N}\lambda$ στοιχεία.
Έστω τυχόν $\mu = a + b\omega$. Αρκεί να εξετάσουμε τα $m + n\omega$ για $m, n \in \{-1, 0, 1\}$, αφού, εάν δύο στοιχεία είναι ισοδύναμα $\mathrm{mod}3$, τότε είναι ισοδύναμα και $\mathrm{mod}\lambda$. Προφανώς $1 - \omega \equiv 0 \pmod \lambda$. Άρα, $\omega \equiv 1 \pmod \lambda$, οπότε $\mu = m + n\omega \equiv m + n \pmod \lambda$. Αλλά ο ακέραιος $m + n$ είναι ισοδύναμος με $0, 1$ ή $-1 \bmod 3$, άρα ισοδύναμος με $0, 1$ ή $-1 \bmod \lambda$.
Τέλος, οι αριθμοί $-1, 0, 1$ είναι διαφορετικοί $\mathrm{mod}\lambda$. Πράγματι, διότι αυτοί είναι διαφορετικοί $\mathrm{mod}3$, οπότε εφαρμόζεται η πρόταση 4.6.3.

□

Έστω π πρώτος. Τότε, σύμφωνα με τα παραπάνω, η πολλαπλασιαστική ομάδα του $D/\pi D$ έχει τάξη $\mathrm{N}\pi - 1$ και έχουμε το ανάλογο του «Μικρού θεωρήματος του Fermat».

Πρόταση 4.1.7. *Εάν ο π είναι πρώτος και $\pi \not| \alpha$, τότε*

$$\alpha^{\mathrm{N}\pi - 1} \equiv 1 \pmod \pi.$$

Πρόταση 4.1.8. *Έστω π πρώτος τέτοιος ώστε $\mathrm{N}\pi \neq 3$ και $\pi \not| \alpha$. Τότε*

$$\alpha^{\frac{\mathrm{N}\pi - 1}{3}} \equiv \omega^m \pmod \pi \text{ για κάποιο } m \in \{0, 1, 2\}$$

Απόδειξη. Από την πρόταση 4.1.7 έχουμε $\pi|\alpha^{\mathrm{N}\pi-1}-1$. Άρα

$$\alpha^{\mathrm{N}\pi-1}-1=\left(\alpha^{(\mathrm{N}\pi-1)/3}-1\right)\left(\alpha^{(\mathrm{N}\pi-1)/3}-\omega\right)\left(\alpha^{(\mathrm{N}\pi-1)/3}-\omega^2\right)$$

Αφού ο π είναι πρώτος, θα διαιρεί τουλάχιστον έναν από τους τρεις παράγοντες στα δεξιά. Από τα προηγούμενα, όμως, μπορεί να διαιρεί το πολύ έναν παράγοντα, αφού εάν διαιρούσε δύο, θα διαιρούσε και τη διαφορά τους.

□

Λήμμα 4.1.9. *Έστω γ πρώτος της D, μη συνεταιρικός του $\lambda=1-\omega$. Εάν $\omega^\mu\equiv\omega^\nu\pmod{\gamma}$, τότε $\omega^\mu=\omega^\nu$.*

Απόδειξη. Αρκεί να αποδείξουμε ότι, εάν $\omega^\mu\equiv 1\pmod{\gamma}$, τότε $\omega^\mu=1$. Επειδή $\omega^3=1$, αρκεί να θεωρήσουμε τις τιμές $\mu=0,1,2$ και να αποκλείσουμε τις δύο τελευταίες.
Για $\mu=1$ έχουμε $\omega\equiv 1\pmod{\gamma}$. Ισοδύναμα $\gamma|(1-\omega)$. Αλλά $\gamma|(1-\omega)$ σημαίνει ότι ο γ είναι είναι συνεταιρικός του λ, που αντίκειται στην υπόθεση.
Για $\mu=2$ έχουμε διαδοχικα:

$$\begin{aligned}\omega^2 &\equiv 1 \pmod{\gamma}\Leftrightarrow(\omega-1)(\omega+1)\equiv 0 \pmod{\gamma}\Leftrightarrow\\ (-\lambda)(-\omega^2) &\equiv 0 \pmod{\gamma}\Leftrightarrow\gamma|\lambda\omega^2\end{aligned}$$

Και πάλι, η τελευταία σχέση μας λέει ότι ο γ είναι πρώτος διαιρέτης του πρώτου $\omega^2\lambda$, δηλαδή ο γ είναι συνεταιρικός του $\omega^2\lambda$, άρα και του λ, που αντιφάσκει στην υπόθεση.

□

Ορισμός 4.1.10. *Έστω $\pi\in D$ τυχών πρώτος με $\mathrm{N}\pi\neq 3$. Το κυβικό σύμβολο του α ως προς τον π, ή αλλιώς, ο κυβικός χαρακτήρας του $\alpha \bmod \pi$ συμβολίζεται $\left(\frac{\alpha}{\pi}\right)_3$ ή $\chi_\pi(\alpha)$ και ορίζεται ως εξής:*

1. *Εάν $\pi|\alpha$, τότε $\left(\frac{\alpha}{\pi}\right)_3=0$.*
2. *Εάν $\pi\not|\,\alpha$ και $\alpha^{(\mathrm{N}\pi-1)/3}\equiv\omega^m\pmod{\pi}$ (Πρόταση 4.1.8), τότε $\left(\frac{\alpha}{\pi}\right)_3=\omega^m$.*

Στον παραπάνω ορισμό, η χρήση της λέξης «χαρακτήρας» και του συμβόλου χ δικαιολογείται ως εξής: Έστω π μιγαδικός πρώτος τέτοιος ώστε $\mathrm{N}\pi=p\equiv 1\pmod 3$. Επειδή το $D/\pi D$ είναι πεπερασμένο σώμα χαρακτηριστικής p, θα περιέχει ένα ισόμορφο αντίγραφο του $\mathbb{F}_p$. Τα $D/\pi D$ και $\mathbb{F}_p$ έχουν p στοιχεία. Επομένως, μπορούμε να ταυτίζουμε τα δύο σώματα. Αντιστοιχίζουμε το σύμπλοκο του n στο $\mathbb{F}_p$ στο σύμπλοκο του n στο $D/\pi D$. Με βάση την πρόταση 4.1.11(4), παρακάτω, η τιμή του συμβόλου $\left(\frac{\alpha}{\pi}\right)_3$ εξαρτάται αποκλειστικά από την κλάση του α. Άρα, έχουμε μία καλά ορισμένη συνάρτηση $\left(\frac{\cdot}{\pi}\right):D/\pi D\longrightarrow\mathbb{C}$. Όπως είδαμε παραπάνω, για π με $\mathrm{N}\pi=p\equiv 1\pmod 3$, ισχύει $D/\pi D\cong\mathbb{F}_p$. Ουσιαστικά έχουμε λοιπόν μία απεικόνιση $\left(\frac{\cdot}{\pi}\right):\mathbb{F}_p\longrightarrow\mathbb{C}$ που πληροί τις ιδιότητες των χαρακτήρων. Αυτό μας επιτρέπει να θεωρήσουμε το χ_π σαν κυβικό χαρακτήρα του $\mathbb{F}_p$ και να εκμεταλλευτούμε χρήσιμες ιδιότητες των αθροισμάτων Gauss $g_\alpha(\chi_\pi)$ και Jacobi $J(\chi_\pi,\chi_\pi)$.

Πρόταση 4.1.11.

1. $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *εάν* $x^3 \equiv \alpha \pmod{\pi}$ *είναι επιλύσιμη, δηλαδή, εάν* α *είναι κυβικό υπόλοιπο.*
2. $\alpha^{(\mathrm{N}\pi-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$.
3. $\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$.
4. *Εάν* $\alpha \equiv \beta \pmod{\pi}$, *τότε* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Απόδειξη. Γνωρίζουμε ότι $D/\pi D \cong \mathbb{F}_p$ (4.1.6) και εργαζόμαστε στην αντίστοιχη πολλαπλασιαστική ομάδα του σώματος.

1. Η εξίσωση $x^3 = \alpha$ επιλύεται εάνν $\alpha^{\frac{p-1}{d}} = 1$, όπου $d = (3, p-1)$ (πρόταση 3.5.3). Επειδή $p \equiv 1 \pmod{3}$, έχουμε $d = 3$ και η $x^3 = \alpha$ επιλύεται εάνν $\alpha^{\frac{\mathrm{N}\pi-1}{3}} = 1$, δηλαδή εάν και μόνο εάν $\left(\frac{\alpha}{\pi}\right)_3 = 1$. Επιπλέον, η επιλυσιμότητα της $x^3 = \alpha$ στο σώμα $D/\pi D$ ισοδυναμεί με την επιλυσιμότητα της $x^3 \equiv \alpha \pmod{\pi}$ στην D.

2. Είναι άμεσο από τον ορισμό 4.1.10(2).

3. Έχουμε

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{(N\pi-1)/3} \equiv \alpha^{(\mathrm{N}\pi-1)/3}\beta^{(\mathrm{N}\pi-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}.$$

Δηλαδή,

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$$

και λόγω του λήμματος 4.1.9,

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3.$$

4. Από την υπόθεση ότι $\alpha \equiv \beta \pmod{\pi}$, συνάγεται ότι $\alpha^{(\mathrm{N}\pi-1)/3} \equiv \beta^{(\mathrm{N}\pi-1)/3} \pmod{\pi}$, απ¨ όπου, ισοδύναμα, έχουμε ότι $\left(\frac{\alpha}{\pi}\right)_3 \equiv \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$. Επομένως, λόγω του λήμματος 4.1.9, είναι $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

□

Πρόταση 4.1.12.

1. $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.
2. $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

Απόδειξη. **1.** Εξ ορισμού το $\chi_\pi(\alpha)$ είναι $1, \omega$ ή ω^2. Το τετράγωνο καθενός από αυτούς τους αριθμούς είναι ίσο με τον συζυγή τους. Επίσης, επειδή χ_π είναι χαρακτήρας, ισχύει $\chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.

2. Από τη σχέση

$$\alpha^{\frac{\mathrm{N}\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi},$$

παίρνοντας τη μιγαδική συζυγή της, έχουμε

$$\overline{\alpha}^{\frac{\mathrm{N}\pi-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$$

Όμως, $N\pi = \mathrm{N}\overline{\pi}$, άρα $\overline{\alpha}^{(\mathrm{N}\overline{\pi}-1)/3} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$.
Από την άλλη, είναι, εξ ορισμού,

$$\overline{\alpha}^{(\mathrm{N}\overline{\pi}-1)/3} \equiv \chi_{\overline{\pi}}(\overline{\alpha}) \pmod{\overline{\pi}}$$

Άρα $\chi_{\overline{\pi}}(\overline{\alpha}) \equiv \overline{\chi_\pi(\alpha)} \pmod{\pi}$ και από το Λήμμα 4.1.9, $\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\chi_\pi(\alpha)}$.

□

Πόρισμα 4.1.13.

1. $\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$.
2. *Εάν n είναι ρητός ακέραιος πρώτος προς το q, τότε $\chi_q(n) = 1$.*

Απόδειξη. Εφαρμόζουμε την πρόταση 4.1.12.

1. Επειδή $q = \overline{q}$, έχουμε $\chi_q(\overline{\alpha}) = \chi_{\overline{q}}(\overline{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$.

2. Επειδή $n = \overline{n}$, έχουμε $\chi_q(n) = \chi_{\overline{q}}(\overline{n}) = \overline{\chi_q(n)} = \chi_q(n^2) = \chi_q(n)^2$.
Επειδή $(n, q) = 1$, έχουμε $q \not| n$ άρα $\chi_q(n) \neq 0$. Έπεται ότι $\chi_q(n) = 1$.

□

Πρόταση 4.1.14. *Υποθέτουμε ότι $\mathrm{N}\pi = p \equiv 1 \pmod 3$. Μεταξύ των συνεταιρικών στοιχείων του π ακριβώς ένα είναι πρώτιστος πρώτος.*

Απόδειξη. Έστω $\pi = a + b\omega$. Τότε τα συνεταιρικά του π είναι $\pm\pi, \pm\omega\pi, \pm\omega^2\pi$, δηλαδή, τα $\pm(a + b\omega), \pm(-b + (a - b)\omega), \pm((b - a) - a\omega)$.
Η σχέση $a^2 - ab + b^2 = \mathrm{N}\pi = p \equiv 1 \pmod 3$ συνεπάγεται τις εξής δυνατότητες: $(a, b) \equiv (0, 1), (0, 2), (1, 0), (1, 1), (2, 0), (2, 2) \pmod 3$.
Σε κάθε μία από αυτές τις έξι πιθανές τιμές του $(a, b) \pmod 3$, ένας άμεσος έλεγχος δείχνει ότι αντιστοιχεί ένα συνεταιρικό του π το οποίο είναι $\equiv 2 \pmod 3$.

□

4.2 Νόμος κυβικής αντιστροφής

Ο βασικός στόχος αυτής της παραγράφου είναι να αποδειχθεί το εξής θεώρημα, το οποίο γενικεύεται αργότερα, στην παράγραφο 4.5.

Θεώρημα 4.2.1. -**Νόμος της κυβικής αντιστροφής.** *Εάν π_1 και π_2 είναι πρώτιστοι πρώτοι, $\mathrm{N}\pi_1, \mathrm{N}\pi_2 \neq 3$ και $\mathrm{N}\pi_1 \neq \mathrm{N}\pi_2$, τότε $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$.*

Πριν προχωρήσουμε στην απόδειξη του νόμου κυβικής αντιστροφής, αποδεικνύουμε κάποιες χρήσιμες προτάσεις.

Εάν χ είναι τυχών κυβικός χαρακτήρας, δείξαμε ότι (πόρισμα 3.3.3 και πρόταση 3.3.4)

$$g(\chi)^3 = pJ(\chi,\chi) \tag{4.1}$$

και εάν $J(\chi,\chi) = a + b\omega$, τότε $a \equiv -1 \pmod 3$ και $b \equiv 0 \pmod 3$ (4.2)

Αφού $J(\chi,\chi)\overline{J(\chi,\chi)} = p$, η σχέση (4.2) μας δίνει την πληροφορία ότι το $J(\chi,\chi)$ είναι πρώτιστος πρώτος της D με στάθμη p.

Λήμμα 4.2.2. *Εάν ο π είναι πρώτιστος πρώτος, με $\mathrm{N}\pi = p$, τότε $J(\chi_\pi, \chi_\pi) = \pi$.*

Απόδειξη. Έστω $J(\chi_\pi,\chi_\pi) = \pi'$. Αφού $\pi\overline{\pi} = p = \pi'\overline{\pi'}$, έχουμε $\pi|\pi'$ ή $\pi|\overline{\pi'}$. Επειδή όλοι οι πρώτοι που έχουμε είναι πρώτιστοι, θα πρέπει $\pi = \pi'$ ή $\pi = \overline{\pi'}$. Σκοπός μας είναι να αποκλείσουμε την τελευταία περίπτωση. Είναι

$$J(\chi_\pi,\chi_\pi) = \sum_{x\in\mathbb{F}_p} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x\in\mathbb{F}_p} x^{(p-1)/3}(1-x)^{(p-1)/3} \pmod\pi$$

Έχουμε $\sum_{x\in\mathbb{F}_p} x^{(p-1)/3}(1-x)^{(p-1)/3} = \sum_{x\in\mathbb{F}_p} (x-x^2)^{(p-1)/3}$. Με χρήση του διωνυμικού τύπου του Newton έχουμε ότι

$$\begin{aligned}
(x-x^2)^{(p-1)/3} &= \sum_{k=0}^{(p-1)/3} \binom{(p-1)/3}{k} x^k(-x^2)^{(p-1)/3-k} \\
&= \sum_{k=0}^{(p-1)/3} \binom{(p-1)/3}{k} (-1)^{(p-1)/3-k}\, x^{k+2\,[\,(p-1)/3-k]} \\
&= \sum_{k=0}^{(p-1)/3} \binom{(p-1)/3}{k} (-1)^{(p-3k-1)/3}\, x^{[2\,(p-1)/3-k]},
\end{aligned}$$

όπου, από υπόθεση, είναι $p \equiv 1 \pmod 3$, δηλαδή $(p-1)/3 \in \mathbb{N}$. Επιπλέον, $0 < 2\,(p-1)/3 - k < p-1$ για κάθε $k = 0, \cdots, (p-1)/3$.
Έχουμε

$$\begin{aligned}
J(\chi_\pi,\chi_\pi) &= \sum_{x\in\mathbb{F}_p} \sum_{k=0}^{(p-1)/3} \binom{(p-1)/3}{k} (-1)^{(p-3k-1)/3} x^{[2\,(p-1)/3-k]} \\
&= \sum_{k=0}^{(p-1)/3} \binom{(p-1)/3}{k} (-1)^{(p-3k-1)/3} \sum_{x\in\mathbb{F}_p} x^{[2\,(p-1)/3-k]}
\end{aligned}$$

Επομένως, από την πρόταση 4.6.5, έχουμε ότι $\sum_{x\in\mathbb{F}_p} x^{[2\,(p-1)/3-k]} \equiv 0 \pmod p$, για κάθε $k = 0, \cdots, (p-1)/3$. Άρα, $J(\chi_\pi,\chi_\pi) \equiv 0 \pmod p$, απ' όπου έπεται ότι $J(\chi_\pi,\chi_\pi) \equiv 0 \pmod\pi$, δηλαδή $\pi' \equiv 0 \pmod\pi$. Άρα, $\pi|\pi'$, δηλαδή $\pi = \pi'$.

□

Πόρισμα 4.2.3. $g(\chi_\pi)^3 = p\pi$.

Απόδειξη. Απόδειξη άμεση από τη σχέση (4.1) και την πρόταση 4.2.2.

□

Απόδειξη του νόμου κυβικής αντιστροφής

Θεωρούμε πρώτα την περίπτωση όπου $\pi_1 = q_1 \equiv 2 \pmod 3$ και $\pi_2 = q_2 \equiv 2 \pmod 3$. Εξ υποθέσεως, οι q_1, q_2 είναι πρώτοι μεταξύ τους. Επομένως, από το πόρισμα 4.1.13, ισχύει $\chi_{q_1}(q_2) = 1$ και $\chi_{q_2}(q_1) = 1$, δηλαδή $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$.

Θεωρούμε τώρα την περίπτωση $\pi_1 = q \equiv 2 \pmod 3$ και $\pi_2 = \pi$, όπου $\mathrm{N}\pi = p$. Από το πόρισμα 4.2.3, ισχύει $g(\chi_\pi)^3 = p\pi$ και διαδοχικά έχουμε :

$$\begin{aligned}
\left(g(\chi_\pi)^3\right)^{(\mathrm{N}q-1)/3} &= (p\pi)^{(\mathrm{N}q-1)/3} \\
g(\chi_\pi)^{q^2-1} &= (p\pi)^{(q^2-1)/3} \\
g(\chi_\pi)^{q^2-1} &\equiv \chi_q(p\pi) \pmod q \\
g(\chi_\pi)^{q^2} &\equiv \chi_q(\pi)\chi_q(p)g(\chi_\pi) \pmod q \\
g(\chi_\pi)^{q^2} &\equiv \chi_q(\pi)g(\chi_\pi) \pmod q. \qquad (4.3)
\end{aligned}$$

Η (4.3) ισχύει διότι $\chi_q(p) = 1$ (από το πόρισμα 4.1.13). Υπολογίζουμε το $g(\chi_\pi)^{q^2}$ με τη βοήθεια του αθροίσματος Gauss,

$$g(\chi_\pi)^{q^2} = \left(\sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta^t\right)^{q^2} \overset{*}{\equiv} \sum_{t\in\mathbb{F}_p} \chi_\pi^{q^2}(t)\zeta^{q^2 t} \pmod q. \qquad (4.4)$$

Η (*) ισχύει διότι δουλεύουμε σε σώμα χαρακτηριστικής q.
Έχουμε $q \equiv 2 \pmod 3$. Άρα $q^2 \equiv 1 \pmod 3$. Δηλαδή,

$$\chi_\pi^{q^2} = (\omega^m)^{q^2} = \omega^{mq^2} = \omega^m = \chi_\pi, \text{ όπου } m = 0, 1 \text{ ή } 2.$$

Άρα, η (4.4) δίνει

$$g(\chi_\pi)^{q^2} \equiv \sum_{t\in\mathbb{F}_p} \chi_\pi(t)\zeta^{q^2 t} \equiv g_{q^2}(\chi_\pi) \pmod q. \qquad (4.5)$$

Από την πρόταση 3.2.2 και επειδή οι τιμές του χαρακτήρα χ_π είναι κυβικές ρίζες της μονάδας, ισχύει

$$g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi^{-2}(q)g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi). \qquad (4.6)$$

Επομένως, από τις (4.3) και (4.5), σε συνδυασμό με την (4.6), έχουμε

$$\chi_q(\pi)g(\chi_\pi) \equiv \chi_\pi(q)g(\chi_\pi) \pmod q.$$

Άρα, $\chi_q(\pi)g(\chi_\pi)\overline{g(\chi_\pi)} \equiv \chi_\pi(q)g(\chi_\pi)\overline{g(\chi_\pi)} \pmod{q}$, οπότε

$$\chi_q(\pi)p \equiv \chi_\pi(q)p \pmod{q}.$$

Επειδή οι p, q είναι πρώτοι μεταξύ τους, έχουμε $\chi_q(\pi) \equiv \chi_\pi(q) \pmod{q}$. Επομένως, από το λήμμα 4.1.9, έχουμε

$$\chi_\pi(q) = \chi_q(\pi).$$

Τέλος, θεωρούμε την περίπτωση όπου π_1, π_2 είναι μιγαδικοί πρώτοι, με $\mathrm{N}\pi_1 = p_1 \equiv 1 \pmod 3$ και $\mathrm{N}\pi_2 = p_2 \equiv 1 \pmod 3$. Έστω $\gamma_1 = \overline{\pi_1}$ και $\gamma_2 = \overline{\pi_2}$. Τότε γ_1, γ_2 είναι πρώτιστοι πρώτοι [2] και $p_1 = \pi_1\gamma_1, p_2 = \pi_2\gamma_2$. Από το πόρισμα 4.2.3 είναι $g(\chi_{\gamma_1})^3 = p_1\gamma_1$, άρα, διαδοχικά, έχουμε:

$$\begin{aligned}
\left(g(\chi_{\gamma_1})^3\right)^{(\mathrm{N}\pi_2-1)/3} &= (p_1\gamma_1)^{(\mathrm{N}\pi_2-1)/3} \\
g(\chi_{\gamma_1})^{p_2-1} &= (p_1\gamma_1)^{(p_2-1)/3} \\
g(\chi_{\gamma_1})^{p_2-1} &\equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2} \\
g(\chi_{\gamma_1})^{p_2} &\equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \pmod{\pi_2}. \qquad (4.7)
\end{aligned}$$

Υπολογίζουμε το $g(\chi_{\gamma_1})^3$ με τη βοήθεια του αθροίσματος Gauss,

$$g(\chi_{\gamma_1})^3 = \left(\sum_{t\in\mathbb{F}_{p_1}} \chi_{\gamma_1}(t)\zeta^t\right)^{p_2} \overset{*}{\equiv} \sum_{t\in\mathbb{F}_{p_1}} \chi_{\gamma_1}(t)^{p_2}\zeta^{p_2 t} \pmod{p_2}. \qquad (4.8)$$

Η (*) ισχύει διότι δουλεύουμε σε χαρακτηριστική p_2. Έχουμε $p_2 \equiv 1 \pmod 3$. Άρα, εάν θέσουμε $\chi_{\gamma_1}(t) = \omega^m$, $m = 0, 1$ ή 2, θα είναι $\chi_{\gamma_1}(t)^{p_2} = (\omega^m)^{p_2} = \omega^{mp_2} = \chi_{\gamma_1}(t)$. Δηλαδή, η σχέση (4.8) δίνει

$$g(\chi_{\gamma_1})^{p_2} \equiv \sum_{t\in\mathbb{F}_{p_1}} \chi_{\gamma_1}(t)\zeta^{p_2 t} \equiv g_{p_2}(\chi_{\gamma_1}) \pmod{p_2}.$$

Από την πρόταση 3.2.2,

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}(p_2^{-1})g(\chi_{\gamma_1}) \pmod{p_2}, \qquad (4.9)$$

όπου επειδή το χ_{γ_1} είναι κυβική ρίζα της μονάδας, ισχύει $\chi_{\gamma_1}(p_2^{-1}) = \chi_{\gamma_1}(p_2)^{-1} = \chi_{\gamma_1}(p_2)^2 = \chi_{\gamma_1}(p_2^2)$. Άρα η σχέση (4.9) δίνει

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \pmod{p_2}.$$

Άρα, ισχύει και

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \pmod{\pi_2}. \qquad (4.10)$$

[2] Πράγματι, εάν $\pi = a + b\omega$ πρώτιστος πρώτος, τότε $a \equiv 2 \pmod 3$ και $b \equiv 0 \pmod 3$. Έχουμε $\overline{\pi} = a + b\omega^2 = a + b(1-\omega) = (a-b) + (-b)\omega$ όπου $a - b \equiv 2 - 0 \equiv 2 \pmod 3$ και $-b \equiv 0 \pmod 3$. Άρα $\overline{\pi}$ είναι πρώτιστος πρώτος (είναι πρώτος διότι $\mathrm{N}\overline{\pi} = \mathrm{N}\pi = p \equiv 1 \pmod 3$).

Από τις σχέσεις (4.7) και (4.10) έχουμε διαδοχικά :

$$\begin{aligned}
\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) &\equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \pmod{\pi_2} \\
\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1})\overline{g(\chi_{\gamma_1})} &\equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1})\overline{g(\chi_{\gamma_1})} \pmod{\pi_2} \\
\chi_{\gamma_1}(p_2^2)p_1 &\equiv \chi_{\pi_2}(p_1\gamma_1)p_1 \pmod{\pi_2} \\
\chi_{\gamma_1}(p_2^2) &\equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2} \\
\chi_{\gamma_1}(p_2^2) &= \chi_{\pi_2}(p_1\gamma_1). \qquad (4.11)
\end{aligned}$$

Παρόμοια, επαναλαμβάνοντας τα προηγούμενα βήματα με π_2 στη θέση του γ_1, το p_1 στη θέση του p_2 και το π_1 στη θέση του π_2, δείχνουμε ότι $\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2)$. Από την πρόταση 4.1.12, επειδή $\gamma_1 = \overline{\pi_1}$ και $\overline{p_2} = p_2$, έχουμε

$$\chi_{\gamma_1}(p_2^2) = \chi_{\gamma_1}(p_2)^2 = \overline{\chi_{\gamma_1}(p_2)} = \chi_{\overline{\gamma_1}}(\overline{p_2}) = \chi_{\pi_1}(p_2). \qquad (4.12)$$

Τελικά,

$$\begin{aligned}
\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_1^2) \qquad (\text{από τη σχέση (4.11)}) \\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(p_2\pi_2) \qquad (\text{από τη σχέση (4.12)}) \\
&= \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\gamma_1) \qquad (\text{από τη σχέση } p_1 = \pi_1\gamma_1\gamma\gamma\ ) \\
&= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1).
\end{aligned}$$

Δηλαδή,

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) = \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1)$$

άρα [3]

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

□

Παρατήρηση: Το χ_π είναι χαρακτήρας στο $\mathbb{F}_p$ [4]. Έτσι, στην προηγούμενη απόδειξη, για τους χαρακτήρες χ_π εκμεταλλευτήκαμε κάποιες ιδιότητες των αθροισμάτων Gauss. Για το χ_q δε χρειάστηκε κάτι αντίστοιχο. Αν χρειαζόταν, θα έπρεπε να γενικεύσουμε τα αθροίσματα Gauss, καθώς το χ_q θα ήταν χαρακτήρας στο $\mathbb{F}_{q^2}$ (διότι $\mathrm{N}q = q^2$).

4.3 Ο κυβικός χαρακτήρας του πρώτου $1-\omega$

Ο βασικός στόχος αυτής της παραγράφου είναι να αποδειχθεί το εξής θεώρημα, το οποίο γενικεύεται αργότερα, στην παράγραφο 4.5.

[3] το $\chi_{\pi_2}(p_1\gamma_1)$ είναι κυβική ρίζα της μονάδας, άρα $\neq 0$.

[4] Όπως είδαμε, το $D/\pi D$ είναι σώμα ισόμορφο με το $\mathbb{F}_p$.

Θεώρημα 4.3.1. **-Συμπλήρωμα του νόμου κυβικής αντιστροφής**
Έστω ότι ο $\pi = a + b\omega$ *είναι πρώτιστος πρώτος με* $N\pi \neq 3$. *Αν θέσουμε* $a = 3m - 1$, *τότε*

$$\chi_\pi(1-\omega) = \omega^{2m}.$$

Πριν προχωρήσουμε στην απόδειξη του συμπληρώματος του νόμου κυβικής αντιστροφής, γενικεύουμε τους κυβικούς χαρακτήρες και αποδεικνύουμε ορισμένες ενδιαφέρουσες προτάσεις, τις οποίες θα χρησιμοποιήσουμε.

Ξέρουμε ότι, για p πρώτο στο $\mathbb{Z}$, το σύμβολο του Legendre ορίζει ένα χαρακτήρα μέσω της σχέσης $\chi_p(t) = \left(\frac{t}{p}\right)$. Το σύμβολο Jacobi, είναι γενίκευση του συμβόλου Legendre και ορίζεται από τη σχέση

$$\chi_{p_1 p_2 \cdots p_m}(t) \overset{ορσ}{=} \chi_{p_1}(t)\chi_{p_2}(t)\cdots\chi_{p_m}(t),$$

όπου p_i πρώτοι στο $\mathbb{Z}$, για κάθε $i = 1, \cdots, m$. Παρακάτω κάνουμε την αντίστοιχη γενίκευση για τον κυβικό χαρακτήρα.

Ορισμός 4.3.2. *Ένα στοιχείο* $\gamma \in D$ *λέγεται* **πρώτιστο** *εάν* $\gamma \equiv 2 \pmod 3$.

Πρόταση 4.3.3.

1. *Εάν* γ *και* ϱ *είναι πρώτιστα στοιχεία της* D, *τότε* $-\gamma\varrho$ *είναι πρώτιστο.*
2. *Κάθε πρώτιστο στοιχείο* γ *έχει μία ανάλυση της μορφής* $\gamma = \pm\gamma_1\gamma_2\cdots\gamma_t$, *όπου* $\gamma_1, \cdots, \gamma_t$ *είναι πρώτιστοι πρώτοι, όχι απαραίτητα διαφορετικοί.*
   Η ανάλυση αυτή του γ *σε πρώτιστους πρώτους λέγεται* **πρώτιστη ανάλυση** *του* γ.
3. *Εάν* γ *και* ϱ *είναι συνεταιρικά πρώτιστα στοιχεία της* D, *τότε* $\gamma = \varrho$.

Απόδειξη. **1.** Θέτουμε $\gamma = a + b\omega, a, b \in \mathbb{Z}$, οπότε, από την υπόθεση, $a \equiv 2 \pmod 3$ και $b \equiv 0 \pmod 3$. Ομοίως, $\varrho = c + d\omega, c, d \in \mathbb{Z}$, έχουμε $c \equiv 2 \pmod 3$ και $d \equiv 0 \pmod 3$. Οπότε,

$$-\varrho\gamma = -(c+d\omega)(a+b\omega) \equiv -ca \equiv -2\cdot 2 \equiv 2 \pmod 3,$$

άρα το στοιχείο $-\varrho\gamma$ είναι πρώτιστο.

2. Από την πρόταση 4.6.2, το γ παραγοντοποιείται ως εξής: $\gamma = (-1)^a\omega^b\lambda^c\pi_1\cdots\pi_m$, όπου π_i πρώτιστοι πρώτοι, όχι αναγκαστικά διακεκριμένοι. Αρχικά, θα περιοριστούμε στο γινόμενο $\pi_1, \cdots, \pi_m$ και θα δείξουμε, με επαγωγή ως προς m, ότι $\pi_1\cdots\pi_m = \pm$ πρώτιστο στοιχείο της D.

Για $m = 1$, π_1 είναι πρώτιστο στοιχείο διότι είναι πρώτιστος πρώτος.

Υποθέτουμε ότι για $m = k$ με $k \geq 1$ το $\pi_1\cdots\pi_k = \pm\delta$, όπου δ πρώτιστο

στοιχείο της D. Για $m = k+1$, έχουμε $\pi_1 \cdots \pi_{k+1} = (\pi_1 \cdots \pi_k)\pi_{k+1} = \pm\delta\pi_{k+1} = \mp(-\delta\pi_{k+1})$, όπου $-\delta\pi_{k+1}$ γνωρίζουμε ότι είναι πρώτιστο από το (1). Επομένως, $\pi_1 \cdots \pi_m = \pm$ πρώτιστο στοιχείο της D.

Το γ είναι πρώτιστο στοιχείο της D, δηλαδή $\gamma \equiv 2 \pmod 3$. Άρα $\gamma \equiv 2 \pmod \lambda$, το οποίο δείχνει ότι στην ανάλυση του γ, είναι $c = 0$, οπότε $\gamma = \pm\omega^b\delta$, με δ πρώτιστο στοιχείο της D, έστω $\delta = k + n\omega, k, n \in \mathbb{Z}$ όπου $k \equiv 2 \pmod 3$ και $n \equiv 0 \pmod 3$. Επειδή $\omega^3 = 1$, το b θα είναι 0, 1 ή 2.
Αν $b = 1$, τότε
$\gamma = \pm\omega\delta = \pm\omega(k+n\omega) = \pm(k\omega+n\omega^2) = \pm(k\omega + n(1-\omega)) = \pm(n + (k-n)\omega)$, το οποίο προφανώς δεν είναι πρώτιστο στοιχείο της D.
Αν $b = 2$, τότε
$\gamma = \pm\omega^2\delta = \pm\omega^2(k+n\omega) = \pm(k\omega^2+n\omega^3) = \pm(k(1-\omega)+n) = \pm((k+n)-k\omega)$, το οποίο προφανώς δεν είναι πρώτιστο στοιχείο της D.
Άρα $b = 0$. Δηλαδή, το πρώτιστο στοιχείο της D, γ είναι $\gamma = \pm\omega^0\delta = \pm\delta$, όπου δ πρώτιστο της D.

3. Θέτουμε $\gamma = a + b\omega$ και $\varrho = c + d\omega$. Επειδή τα γ, ϱ είναι πρώτιστα στοιχεία, έχουμε $a \equiv c \equiv 2 \pmod 3$ και $b \equiv d \equiv 0 \pmod 3$. Από υπόθεση, τα γ, ϱ είναι συνεταιρικά, άρα υπάρχει μονάδα u της D, $u \in \{\pm 1, \pm\omega, \pm\omega^2\}$, ώστε $\gamma = u\varrho$, δηλαδή $a + b\omega = u(c + d\omega)$.
Είναι $u \neq -1$, διότι το $-c - d\omega$ δεν είναι πρώτιστο, αφού $-c \not\equiv 2 \pmod 3$. Επίσης, $\pm\omega(c+d\omega) = \pm d \pm (c-d)\omega$ δεν είναι πρώτιστο διότι $\pm d \not\equiv 2 \pmod 3$. Άρα, $u \neq \pm\omega$. Τέλος, το $\pm\omega^2(c+d\omega) = \pm(c+d) \mp c\omega$ δεν είναι πρώτιστο διότι $\pm c \not\equiv 0 \pmod 3$, άρα $u \neq \pm\omega^2$.

Επομένως, $u = 1$, δηλαδή $\gamma = \varrho$.

□

Ορισμός 4.3.4. *Έστω $\gamma = \pm\gamma_1\gamma_2\cdots\gamma_t$ η πρώτιστη ανάλυση του πρώτιστου στοιχείου γ. Τότε, για κάθε $\alpha \in D$ ορίζουμε (ανεξάρτητα εάν στην παραπάνω ισότητα έχουμε το πρόσημο + ή το πρόσημο -)*

$$\chi_\gamma(\alpha) = \chi_{\gamma_1}(\alpha)\cdots\chi_{\gamma_t}(\alpha).$$

Πρόταση 4.3.5. *Έστω γ πρώτιστο στοιχείο. Τότε:*

1. *εάν $\alpha \equiv \beta \pmod\gamma$ τότε $\chi_\gamma(\alpha) = \chi_\gamma(\beta)$.*
2. *$\chi_\gamma(\alpha\beta) = \chi_\gamma(\alpha)\chi_\gamma(\beta)$.*
3. *εάν το ϱ είναι, επίσης, πρώτιστο, τότε $\chi_\varrho(\alpha)\chi_\gamma(\alpha) = \chi_{-\varrho\gamma}(\alpha)$.*

Απόδειξη. **1.** Από την υπόθεση $\alpha \equiv \beta \pmod\gamma$, έχουμε $\alpha \equiv \beta \pmod{\gamma_i}$ για κάθε $i \in \{1, \cdots, t\}$. Από την πρόταση 4.1.11(4) έχουμε, τότε, ότι $\chi_{\gamma_i}(\alpha) = \chi_{\gamma_i}(\beta)$ για κάθε $i \in \{1, \cdots, t\}$. Άρα,

$$\chi_\gamma(\alpha) = \chi_{\gamma_1}(\alpha)\chi_{\gamma_2}(\alpha)\cdots\chi_{\gamma_t}(\alpha) = \chi_{\gamma_1}(\beta)\chi_{\gamma_2}(\beta)\cdots\chi_{\gamma_t}(\beta) = \chi_\gamma(\beta).$$

2. Επίσης από την πρόταση 4.1.11(3) έχουμε ότι $\chi_{\gamma_i}(\alpha\beta) = \chi_{\gamma_i}(\alpha)\chi_{\gamma_i}(\beta)$ για κάθε $i \in \{1, \cdots, t\}$. Άρα, κάνοντας χρήση της πολλαπλασιαστικότητας καθενός από τα χ_{γ_i}, έχουμε

$$\begin{aligned}\chi_\gamma(\alpha\beta) &= \chi_{\gamma_1}(\alpha\beta)\chi_{\gamma_2}(\alpha\beta)\cdots\chi_{\gamma_t}(\alpha\beta)\\ &= (\chi_{\gamma_1}(\alpha)\chi_{\gamma_1}(\beta))\ (\chi_{\gamma_2}(\alpha)\chi_{\gamma_2}(\beta))\ \cdots\ (\chi_{\gamma_t}(\alpha)\chi_{\gamma_t}(\beta))\\ &= (\chi_{\gamma_1}(\alpha)\chi_{\gamma_2}(\alpha)\cdots\chi_{\gamma_t}(\alpha))\ (\chi_{\gamma_1}(\beta)\chi_{\gamma_2}(\beta)\cdots\chi_{\gamma_t}(\beta))\\ &= \chi_\gamma(\alpha)\chi_\gamma(\beta).\end{aligned}$$

3. Είδαμε ότι τα πρώτιστα στοιχεία γ και ϱ παραγοντοποιούνται ως εξής:

$$\begin{aligned}\gamma &= (-1)^\delta\gamma_1\gamma_2\cdots\gamma_m,\\ \varrho &= (-1)^\theta\varrho_1\varrho_2\cdots\varrho_n,\end{aligned}$$

όπου $\delta, \theta \in \{-1, 1\}$, γ_i είναι πρώτιστοι πρώτοι, για κάθε $i = 1, \cdots, m$, όχι αναγκαστικά διακεκριμένοι και ϱ_j είναι πρώτιστοι πρώτοι, για κάθε $j = 1, \cdots, n$, όχι αναγκαστικά διακεκριμένοι. Οπότε,

$$-\varrho\gamma = (-1)^{\delta+\theta}\prod_{j=1}^{n}\varrho_j\prod_{i=1}^{m}\gamma_i$$

Άρα, έχουμε

$$\chi_{-\varrho\gamma}(\alpha) = \prod_{j=1}^{n}\chi_{\varrho_j}(\alpha)\prod_{i=1}^{m}\chi_{\gamma_i}(\alpha) = \chi_\varrho(\alpha)\chi_\gamma(\alpha)$$

□

Πρόταση 4.3.6. *Έστω $\gamma = a + b\omega$ πρώτιστος πρώτος και θέτουμε $a = 3m - 1$ και $b = 3n$. Τότε,*

$$\chi_\gamma(\omega) = \omega^{m+n}.$$

Πιο αναλυτικά, $\chi_\gamma(\omega) = 1, \omega$ ή ω^2 ανάλογα με το εάν το γ είναι ισότιμο με 8, 2 ή 5 $\bmod 3\lambda$, αντιστοίχως. Ειδικά, εάν q ρητός πρώτος, $q \equiv 2 \pmod 3$, τότε $\chi_q(\omega) = 1, \omega$ ή ω^2, ανάλογα με το εάν $q \equiv 8, 2$ ή $5 (mod\, 9)$, αντιστοίχως.

Απόδειξη. Γνωρίζουμε ότι $\chi_\gamma(\omega) \equiv \omega^{\frac{\mathrm{N}\gamma-1}{3}} \pmod\gamma$. Από την άλλη, έχουμε

$$\mathrm{N}\gamma = (3m-1)^2 - (3m-1)3n + (3n)^2 = 9m^2 - 6m + 1 - 9mn + 3n + 9n^2,$$

απ¨ όπου $\frac{\mathrm{N}\gamma-1}{3} = 3m^2 - 2m - 3mn + n + 3n^2 \equiv m + n \pmod 3$, και συνεπώς

$$\omega^{(\mathrm{N}\gamma-1)/3} = \omega^{m+n}.$$

Άρα $\chi_\gamma(\omega) \equiv \omega^{m+n} \pmod\gamma$ και, από το λήμμα 4.1.9,

$$\chi_\gamma(\omega) = \omega^{m+n}.$$

Έχουμε $3\lambda = (-\omega^2(1-\omega)^2)(1-\omega) = -\omega^2\lambda^3$. Άρα, η διαιρετότητα δια 3λ ισοδυναμεί με διαιρετότητα δια λ^3. Εξετάζουμε τώρα κάθε μία από τις περιπτώσεις

$\chi_\gamma(\omega) = 1, \omega, \omega^2$.

Εάν $\chi_\gamma(\omega) = 1$, δηλαδή $\omega^{m+n} = 1$, έπεται ότι $m+n \equiv 0 \pmod 3$. Άρα, υπάρχει $k \in \mathbb{Z}$ τέτοιο ώστε $n = 3k - m$.
Το γ έχει τη μορφή $\gamma = (3m-1) + 3n\omega$. Επομένως, στην περίπτωση αυτή,

$$\begin{aligned} \gamma &= (3m-1) + 3(3k-m)\omega = 3m - 1 + 9k\omega - 3m\omega \\ &\equiv 3m - 3m\omega - 1 \pmod{\lambda^3} \\ &\equiv 3m(1-\omega) - 1 \equiv 3m\lambda - 1 \equiv -1 \equiv 8 \pmod{\lambda^3}, \end{aligned}$$

όπου η τελευταία ισοτιμία ισχύει διότι $\lambda^3 | (8 - (-1)) = 9 = \omega^4\lambda^4$.

Εάν $\chi_\gamma(\omega) = \omega$, τότε $\omega^{m+n} = \omega$. Ισοδύναμα, $m+n \equiv 1 \pmod 3$, άρα υπάρχει $k \in \mathbb{Z}$ τέτοιος ώστε $n = 3k + 1 - m$. Επομένως, στην περίπτωση αυτή,

$$\begin{aligned} \gamma &= (3m-1) + 3(3k+1-m)\omega = 3m - 1 + 9k\omega + 3\omega - 3m\omega \\ &\equiv 3m - 3m\omega - 1 + 3\omega \equiv 3m(1-\omega) - 3(1-\omega) + 2 \pmod{\lambda^3} \\ &\equiv 3m\lambda - 3\lambda + 2 \equiv 2 \pmod{\lambda^3}. \end{aligned}$$

Εάν $\chi_\gamma(\omega) = \omega^2$, δηλαδή $\omega^{m+n} = \omega^2$, τότε $m+n \equiv 2 \pmod 3$. Άρα, υπάρχει $k \in \mathbb{Z}$ ώστε $n = 3k + 2 - m$. Επομένως, στην περίπτωση αυτή,

$$\begin{aligned} \gamma &= (3m-1) + 3(3k+2-m)\omega = 3m - 1 + 9k\omega + 6\omega - 3m\omega \\ &\equiv 3m - 3m\omega - 1 + 6\omega \equiv 3m(1-\omega) - 3(1-\omega) + 5 \pmod{\lambda^3} \\ &\equiv 3m\lambda - 3\lambda + 5 \equiv 5 \pmod{\lambda^3}. \end{aligned}$$

□

Πρόταση 4.3.7. *Εάν $\gamma = A + B\omega$ είναι πρώτιστο και $A = 3M - 1$, $B = 3N$, τότε $\chi_\gamma(\omega) = \omega^{M+N}$.*

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή στο πλήθος των πρωτίστων πρώτων, οι οποίοι εμφανίζονται στην πρώτιστη ανάλυση του γ (βλ. πρόταση 4.3.3). Εάν ένα πρώτιστο στοιχείο $\gamma \in D$ έχει στην πρώτιστη ανάλυσή του έναν μόνο πρώτιστο πρώτο, τότε το ίδιο το γ είναι πρώτιστος πρώτος, οπότε εφαρμόζεται η πρόταση 4.3.6.

Έστω ότι ισχύει το ζητούμενο για τυχόν πρώτιστο στοιχείο της D, με k πρώτιστους πρώτους παράγοντες. Έστω γ πρώτιστο στοιχείο της D με $k+1$ πρώτιστους πρώτους παράγοντες,

$$\gamma = \varepsilon\gamma_1 \cdots \gamma_k\gamma_{k+1}. \tag{4.13}$$

Για κατάλληλο $\varepsilon' = \pm 1$, το $\delta = \varepsilon'\gamma_1 \cdots \gamma_k$, είναι πρώτιστο στοιχείο της D. Άρα για το δ ισχύει η επαγωγική υπόθεση. Τα δ, γ_{k+1} είναι πρώτιστα στοιχεία της D, άρα,από την πρόταση 4.3.3(1), το $-\delta\gamma_{k+1}$ είναι πρώτιστο, ενώ, λόγω της (4.13), είναι $\gamma = \pm\delta\gamma_{k+1}$. Αυτά, σε συνδυασμό με την πρόταση 4.3.3(3), οδηγούν στη σχέση $\gamma = -\delta\gamma_{k+1}$. Θέτουμε τώρα $\gamma_{k+1} = a + bi$, όπου $a = 3m - 1, b = 3n$ και

$\delta = c + di$, όπου $c = 3K - 1, d = 3L$ και, χρησιμοποιώντας την πρόταση 4.3.5, έχουμε

$$\chi_\gamma(\omega) = \chi_{-\delta\gamma_{k+1}}(\omega) = \chi_\delta(\omega)\chi_{\gamma_{k+1}}(\omega) = \omega^{K+L}\omega^{m+n} = \omega^{K+L+m+n}.$$

Αρκεί να δείξουμε ότι $K+L+m+n \equiv M+N \pmod 3$. Πράγματι, από τη σχέση $\gamma = -\delta\gamma_{k+1}$, έχουμε

$$\begin{aligned} 3M - 1 + 3N\omega &= -(3K - 1 + 3L\omega)\,(3m - 1 + 3n\omega) \\ &= -9Km + 3m - 9Lm\omega + 3K - 1 + 3L\omega - 9nK\omega + 3n\omega - 9Ln\omega^2 \\ &= (3m + 3K - 1) + 3(L+n)\omega + 9(Ln - Km) + 9(Ln - Lm - nK)\omega, \end{aligned}$$

απ¨ όπου διαδοχικά είναι

$$\begin{aligned} 3M - 1 \equiv 3m + 3K - 1 \pmod 9 \quad &\text{και} \quad 3N \equiv 3(L+n) \pmod 9, \\ 3M \equiv 3(m+K) \pmod 9 \quad &\text{και} \quad 3N \equiv 3(L+n) \pmod 9, \\ M \equiv m + K \pmod 3 \quad &\text{και} \quad N \equiv L + n \pmod 3, \\ M + N \quad &\equiv \quad m + K + L + n \pmod 3. \end{aligned}$$

□

Πρόταση 4.3.8. *Εάν γ και ϱ είναι πρώτιστα στοιχεία της D με $(\mathrm{N}\gamma, \mathrm{N}\varrho) = 1$, τότε $\chi_\gamma(\varrho) = \chi_\varrho(\gamma)$.*

Απόδειξη. Θεωρούμε τις πρώτιστες αναλύσεις των γ, ϱ (πρόταση 4.3.3), $\gamma = \varepsilon\gamma_1 \cdots \gamma_k$ και $\varrho = \varepsilon'\varrho_1 \cdots \varrho_\mu$, όπου $\varepsilon, \varepsilon' = \pm 1$. Αφού τα γ_i, ϱ_j είναι πρώτιστα, δεν είναι συνεταιρικά με το λ, άρα $\mathrm{N}\gamma_i \neq 3$ και $\mathrm{N}\varrho_j \neq 3$, για κάθε $i = 1, \cdots, k$ και $j = 1, \cdots, \mu$. Από την ορισμό 4.3.4 έχουμε

$$\chi_\gamma(\varrho) = \prod_{1 \le i \le k,\ 1 \le j \le \mu} \chi_{\gamma_i}(\varrho_j) \tag{4.14}$$

και

$$\chi_\varrho(\gamma) = \prod_{1 \le i \le k,\ 1 \le j \le \mu} \chi_{\varrho_j}(\gamma_i) \tag{4.15}$$

Για κάθε ζεύγος δεικτών i, j ισχύει $\mathrm{N}\gamma_i \neq \mathrm{N}\varrho_j$. Οπότε, για κάθε ζεύγος δεικτών, ισχύει ο νόμος κυβικής αντιστροφής (θεώρημα 4.2.1), δηλαδή

$$\chi_{\gamma_i}(\varrho_j) = \chi_{\varrho_j}(\gamma_i).$$

Από την παρατήρηση αυτή και τις σχέσεις (4.14) και (4.15) έπεται αμέσως το ζητούμενο.

□

Απόδειξη του συμπληρώματος του νόμου κυβικής αντιστροφής

Μέχρι τέλους αυτής της παραγράφου ο $\pi \in D$ θα συμβολίζει πρώτιστο πρώτο με $\mathrm{N}\pi = p \equiv 1 \pmod 3$.

Πρόταση 4.3.9. *Έστω $\pi = a + b\omega$ μιγαδικός πρώτος της D, $a = 3m-1$, $b = 3n$ και $p = \mathrm{N}\pi$. Ισχύουν τα ακόλουθα:*

1. $\dfrac{p-1}{3} \equiv -2m + n \pmod 3$.
2. $a^2 - 13 \equiv m \pmod 3$.
3. $\chi_\pi(a) = \omega^m$.
4. $\chi_\pi(a+b) = \omega^{2n}\chi_\pi(1-\omega)$.

Απόδειξη. **1.** Έχουμε, διαδοχικά,

$$\begin{aligned}
\mathrm{N}\pi = a^2 - ab + b^2 &\Leftrightarrow p = (3m-1)^2 - (3m-1)3n + (3n)^2 \\
&\Leftrightarrow p = 9m^2 - 6m + 1 - 9mn + 3n + 9n^2 \\
&\Rightarrow p \equiv -6m + 3n + 1 \pmod 9 \Leftrightarrow p - 1 \equiv -6m + 3n \pmod 9 \\
&\Leftrightarrow \frac{p-1}{3} \equiv -2m + n \pmod 3
\end{aligned}$$

2. Από την υπόθεση, έχουμε $a^2 = (3m-1)^2 = 9m^2 - 6m + 1$, δηλαδή $a^2 - 1 = 9m^2 - 6m$. Επομένως, $a^2 \equiv -6m \equiv 3m \pmod 9$, απ¨ όπου $\frac{a^2-1}{3} \equiv m \pmod 3$.

3. Το $a = 3m-1$ είναι πρώτιστο στοιχείο της D και $(a, p) = 1$. Επομένως, $(\mathrm{N}a, \mathrm{N}\pi) = 1$ και, από την πρόταση 4.3.8, έχουμε ότι

$$\chi_\pi(a) = \chi_a(\pi)\ . \tag{4.16}$$

Έχουμε $\pi = a + b\omega$, επομένως $\pi \equiv b\omega \pmod a$. Οπότε

$$\chi_a(\pi) = \chi_a(b\omega) = \chi_a(b)\chi_a(\omega). \tag{4.17}$$

Από την πρόταση 4.3.7, γνωρίζουμε ότι ισχύει $\chi_a(\omega) = \omega^m$. Από αυτή τη σχέση και τις σχέσεις (4.16) και (4.17), προκύπτει ότι

$$\chi_\pi(a) = \chi_a(b)\omega^m. \tag{4.18}$$

Άρα, αρκεί να δείξουμε ότι $\chi_a(b) = 1$. Πράγματι, εάν $a = \pm\gamma_1 \cdots \gamma_t$ είναι η ανάλυση του a σε πρώτιστους πρώτους παράγοντες, από τον ορισμό 4.3.4, έχουμε

$\chi_a(b) = \chi_{\gamma_1}(b)\cdots\chi_{\gamma_t}(b)$. Άρα, $\overline{\chi_a(b)} = \overline{\chi_{\gamma_1}(b)}\cdots\overline{\chi_{\gamma_t}(b)}$, οπότε, από την πρόταση 4.1.12, έχουμε

$$\overline{\chi_a(b)} = \chi_{\overline{\gamma_1}}(\overline{b})\cdots\chi_{\overline{\gamma_t}}(\overline{b}) = \chi_{\overline{a}}(\overline{b}) \tag{4.19}$$

Επειδή $a, b \in \mathbb{Z}$, είναι $\overline{a} = a$ και $\overline{b} = b$. Άρα,

$$\chi_a(b) = \chi_{\overline{a}}(\overline{b}) = \overline{\chi_a(b)}$$

και επειδή $\chi_a(b) \in \{1, \omega, \omega^2\}$, συμπεραίνουμε ότι $\chi_a(b) = 1$.

4. Είναι $a + b = a + b\omega - b\omega + b = p - b(1-\omega) \equiv -b(1-\omega) \pmod{\pi}$. Επομένως από την πρόταση 4.1.11 (4) έχουμε

$$\chi_\pi(a+b) = \chi_\pi(-b(1-\omega)) = \chi_\pi(-b)\chi_\pi(1-\omega).$$

Άρα αρκεί να δείξουμε ότι $\chi_\pi(-b) = \omega^{2n}$. Πράγματι, έχουμε

$$\pi = a + b\omega \;\Rightarrow\; -b\omega \equiv a \pmod{\pi} \;\Rightarrow\; -b \equiv a\omega^2 \pmod{\pi}$$

οπότε (πρόταση 4.1.11 (4).)

$$\chi_\pi(-b) = \chi_\pi(a\omega^2) = \chi_\pi(a)\chi_\pi(\omega^2) = \chi_\pi(a)\chi_\pi(\omega)^2. \tag{4.20}$$

Τα a, π είναι πρώτιστα στοιχεία με $(\mathrm{N}a, \mathrm{N}\pi) = 1$, επομένως από την πρόταση 4.3.8 ισχύει $\chi_\pi(a) = \chi_a(\pi)$. Από το σημείο (3) της τρέχουσας πρότασης $\chi_a(\pi) = \omega^m$, άρα $\chi_\pi(a) = \omega^m$. Επιπλέον, από την πρόταση 4.3.6 έχουμε ότι $\chi_\pi(\omega) = \omega^{m+n}$. Συνεπώς, η σχέση (4.20) δίνει

$$\chi_\pi(-b) = \omega^m\omega^{2(m+n)} = \omega^{2n}$$

□

Πρόταση 4.3.10. *Έστω $\pi = a + b\omega$ μιγαδικός πρώτος της D, $a = 3m-1$, $b = 3n$ και $p = \mathrm{N}\pi$. Τότε:*

1. $\chi_{a+b}(\pi) = \chi_{a+b}(1-\omega)$.
2. $\chi_{a+b}(\pi) = \omega^{2(m+n)}$.

Απόδειξη. **1.** Έχουμε $\pi = a + b\omega = a + b - b + b\omega = -b(1-\omega) + (a+b)$. Άρα, $\pi \equiv -b(1-\omega) \pmod{a+b}$. Επομένως, με χρήση της πρότασης 4.1.11(4),

$$\chi_{a+b}(\pi) = \chi_{a+b}\left(-b(1-\omega)\right) = \chi_{a+b}(-1)\chi_{a+b}(b)\chi_{a+b}(1-\omega) = \chi_{a+b}(b)\chi_{a+b}(1-\omega).$$

Η τελευταία ισότητα ισχύει διότι $-1 = (-1)^3$ και, εφαρμόζοντας την πρόταση 4.1.11(1), έχουμε $\chi_{a+b}(-1) = 1$. Συνεπώς, αρκεί να δείξουμε ότι $\chi_{a+b}(b) = 1$. Πράγματι, εάν $a + b = \pm\gamma_1\cdots\gamma_t$ είναι η πρώτιστη ανάλυση του $a+b$ (βλ. ορισμό 4.3.4), τότε έχουμε $\chi_{a+b}(b) = \chi_{\gamma_1}(b)\cdots\chi_{\gamma_t}(b)$. Απ' όπου $\overline{\chi_{a+b}(b)} = \overline{\chi_{\gamma_1}(b)}\cdots\overline{\chi_{\gamma_t}(b)}$, δηλαδή, με χρήση της πρότασης 4.1.12, έχουμε

$$\overline{\chi_{a+b}(b)} = \chi_{\overline{\gamma_1}}(\overline{b}) \cdots \chi_{\overline{\gamma_t}}(\overline{b}) = \chi_{\overline{a+b}}(\overline{b}).$$

Επειδή $a, b \in \mathbb{Z}$, είναι $\overline{a+b} = a+b$, άρα,

$$\chi_{a+b}(b) = \chi_{\overline{a+b}}(\overline{b}) = \overline{\chi_{a+b}(b)}.$$

Αλλά $\chi_{a+b}(b) \in \{1, \omega, \omega^2\}$, οπότε η τελευταία ισότητα συνεπάγεται ότι $\chi_{a+b}(b) = 1$.

2. Παρατηρούμε ότι το $a+b$ είναι πρώτιστο στοιχείο, καθώς $a+b = 3m - 1 + 3n \equiv 2 \pmod 3$. Θεωρούμε την πρώτιστη ανάλυση του $a+b$,

$$a+b = \pm\pi_1 \cdots \pi_k q_1 \cdots q_\ell,$$

όπου π_i είναι μη-ρητός πρώτιστος πρώτος με στάθμη $p_i \equiv 1 \pmod 3$, για κάθε $i = 1, \cdots, k$ και q_j είναι ρητός πρώτος $\equiv 2 \pmod 3$ για κάθε $j = 1, \cdots, \ell$.

Από το σημείο (1.) της τρέχουσας πρότασης, έχουμε ότι $\chi_{a+b}(\pi) = \chi_{a+b}(1-\omega)$. Επομένως, αρκεί να δείξουμε ότι

$$\chi_{a+b}(1-\omega) = \omega^{2(m+n)}.$$

Από τον ορισμό 4.3.4, έχουμε

$$\chi_{a+b}(1-\omega) = \prod_{i=1}^{k} \chi_{\pi_i}(1-\omega) \prod_{j=1}^{\ell} \chi_{q_j}(1-\omega). \tag{4.21}$$

Για κάθε π_i παρατηρούμε ότι ισχύει $\chi_{\pi_i}(1-\omega) = (\chi_{\pi_i}(1-\omega))^4$, απ᾽ όπου διαδοχικά έχουμε

$$\begin{aligned} \chi_{\pi_i}(1-\omega) &= \left(\chi_{\pi_i}\left((1-\omega)^2\right)\right)^2 = \chi_{\pi_i}\left(-3\omega\right)^2 = \chi_{\pi_i}(-3)^2 \chi_{\pi_i}(\omega)^2 \\ &= \chi_{\pi_i}\left((-3)^2\right) \omega^{2\,(\mathrm{N}\pi_i - 1)/3} = \chi_{\pi_i}(9) \omega^{2\,(p_i-1)/3} \end{aligned}$$

και δουλεύοντας ανάλογα για κάθε q_j έχουμε

$$\chi_{q_j}(1-\omega) = \chi_{q_j}(9)\, \omega^{2\,(\mathrm{N}q_j - 1)/3} = \chi_{q_j}(9)\, \omega^{2\left(q_j^2-1\right)/3}.$$

Από την πρόταση 4.1.13 (2), είναι $\chi_{q_j}(9) = 1$, οπότε

$$\chi_{q_j}(1-\omega) = \omega^{2\left(q_j^2-1\right)/3}.$$

Από τις παραπάνω παρατηρήσεις, η σχέση 4.21 γίνεται

$$\begin{aligned} \chi_{a+b}(1-\omega) &= \prod_{i=1}^{k} \chi_{\pi_i}(9) \prod_{i=1}^{k} \omega^{2\,(p_i-1)/3} \prod_{j=1}^{\ell} \omega^{2\left(q_j^2-1\right)/3} \\ &= \prod_{i=1}^{k} \chi_{\pi_i}(9)\, \omega^{2\sum_{i=1}^{k}(p_i-1)/3}\, \omega^{2\sum_{j=1}^{\ell}\left(q_j^2-1\right)/3} \\ &= \prod_{i=1}^{k} \chi_{\pi_i}(9)\, \omega^{2\left(\sum_{i=1}^{k}(p_i-1)/3 + \sum_{j=1}^{\ell}\left(q_j^2-1\right)/3\right)}. \end{aligned} \tag{4.22}$$

Από το λήμμα 4.6.7, έχουμε ότι ισχύει $m+n \equiv \sum_{i=1}^{k}(p_i-1)/3 + \sum_{j=1}^{\ell}\left(q_j^2-1\right)/3 \pmod 3$, απ᾽ όπου έπεται ότι η σχέση 4.22 γίνεται

$$\chi_{a+b}(1-\omega) = \prod_{i=1}^{k} \chi_{\pi_i}(9)\, \omega^{2(m+n)}. \tag{4.23}$$

Παρατηρούμε ότι, καθώς $a+b = \overline{a+b}$, η

$$a+b = \pm \prod_{i=1}^{k} \overline{\pi_i} \prod_{j=1}^{\ell} q_j$$

θα είναι επίσης πρώτιστη ανάλυση του $a+b$. Επομένως, κατ¨ αναλογία με τη σχέση 4.23, ισχύει

$$\chi_{a+b}(1-\omega) = \prod_{i=1}^{k} \chi_{\overline{\pi_i}}(9)\, \omega^{2(m+n)},$$

άρα

$$\chi_{a+b}(1-\omega) = \prod_{i=1}^{k} \overline{\chi_{\pi_i}(9)}\, \omega^{2(m+n)}. \tag{4.24}$$

Πολλαπλασιάζοντας τις σχέσεις 4.23 και 4.24 κατά μέλη, έχουμε διαδοχικά

$$\begin{aligned} \chi_{a+b}(1-\omega)^2 &= \prod_{i=1}^{k} \chi_{\pi_i}(9) \prod_{i=1}^{k} \overline{\chi_{\pi_i}(9)}\ \omega^{4(m+n)} \\ &= \prod_{i=1}^{k} \chi_{\pi_i}(9)\ \overline{\chi_{\pi_i}(9)}\ \omega^{m+n} \\ &= \prod_{i=1}^{k} |\, \chi_{\pi_i}(9)\,|^2\, \omega^{m+n}\ , \end{aligned}$$

όπου, για κάθε $i = 0, \cdots, k$, είναι $\chi_{\pi_i}(9) = 1, \omega$ ή ω^2, οπότε, επειδή το ω είναι κυβική ρίζα της μονάδας, σε κάθε περίπτωση είναι $|\,\chi_{\pi_i}(9)\,| = 1$, δηλαδή $|\,\chi_{\pi_i}(9)\,|^2 = 1$. Επομένως, έχουμε

$$\chi_{a+b}(1-\omega)^2 = \prod_{i=1}^{k} 1\ \ \omega^{m+n} = \omega^{m+n}.$$

Πολλαπλασιάζοντας την τελευταία σχέση επί $\chi_{a+b}(1-\omega)\cdot\omega^{2(m+n)}$, έχουμε

$$\chi_{a+b}(1-\omega)^3\ \omega^{2(m+n)} = \chi_{a+b}(1-\omega)\ \omega^{3(m+n)},$$

απ¨ όπου έπεται άμεσα το ζητούμενο.

□

Συνεχίζουμε να χρησιμοποιούμε τους συμβολισμούς της πρότασης 4.3.10 και επιπλέον έχουμε ότι $N\pi \neq 3$. Παρατηρούμε ότι $p = (a+b)^2 - 3ab$, άρα $((a+b)^2, p) = 1$, που σημαίνει ότι $(\mathrm{N}(a+b), \mathrm{N}\pi) = 1$. Συνεπώς, από την πρόταση 4.3.8, έχουμε ότι ισχύει

$$\chi_{\pi}(a+b) = \chi_{a+b}(\pi). \tag{4.25}$$

Από τις προτάσεις 4.3.10 και 4.3.9 έχουμε, αντιστοίχως

$$\chi_{a+b}(\pi) = \omega^{2m+2n} \tag{4.26}$$

$$\text{και} \quad \chi_{\pi}(a+b) = \omega^{2n}\chi_{\pi}(1-\omega) \tag{4.27}$$

Οπότε, η σχέση (4.25), σε συνδυασμό με τις (4.26) και (4.27), δίνει

$$\omega^{2n}\chi_\pi(1-\omega) = \omega^{2m}\omega^{2n},$$

απ' όπου προκύπτει το ζητούμενο:

$$\chi_\pi(1-\omega) = \omega^{2m}.$$

Το ακόλουθο πόρισμα δίνει έναν πιο άμεσο τρόπο υπολογισμού του κυβικού χαρακτήρα του $\lambda = 1-\omega$.

Πόρισμα 4.3.11.

1. $\chi_\gamma(\lambda) = 1$ *για* $\gamma \equiv 8, 8+3\omega, 8+6\omega \pmod 9$.
2. $\chi_\gamma(\lambda) = \omega$ *για* $\gamma \equiv 5, 5+3\omega, 5+6\omega \pmod 9$.
3. $\chi_\gamma(\lambda) = \omega^2$ *για* $\gamma \equiv 2, 2+3\omega, 2+6\omega \pmod 9$.

Απόδειξη. **1.** Εάν $\chi_\gamma(\lambda) = 1$, δηλαδή $\omega^{2m} = 1$, τότε $2m \equiv 0 \pmod 3$. Άρα, $m \equiv 0 \pmod 3$. Επομένως, υπάρχει $k \in \mathbb{Z}$ ώστε $m = 3k$.
Διακρίνουμε τρεις περιπτώσεις ανάλογα με την κλάση του $m \bmod 3$.
(**i**). Εάν $m \equiv 0 \pmod 3$, τότε υπάρχει $\mu \in \mathbb{Z}$ ώστε $m = 3\mu$. Επομένως,

$$\gamma = 3(3k) - 1 + 3(3\mu)\omega = 9k - 1 + 9\mu\omega \equiv -1 \equiv 8 \pmod 9.$$

(**ii**). Εάν $m \equiv 1 \pmod 3$, τότε υπάρχει $\mu \in \mathbb{Z}$ ώστε $m = 3\mu + 1$. Επομένως,

$$\gamma = 3(3k) - 1 + 3(3\mu+1)\omega = 9k - 1 + 9\mu\omega + 3\omega \equiv -1 + 3\omega \equiv 8 + 3\omega \pmod 9.$$

(**iii**). Εάν $m \equiv 2 \pmod 3$, τότε υπάρχει $\mu \in \mathbb{Z}$ ώστε $m = 3\mu + 2$. Επομένως,

$$\gamma = 3(3k) - 1 + 3(3\mu+2)\omega = 9k - 1 + 9\mu\omega + 6\omega \equiv -1 + 6\omega \equiv 8 + 6\omega \pmod 9.$$

2. Εάν $\chi_\gamma(\lambda) = \omega$, δηλαδή $\omega^{2m} = \omega$, τότε $2m \equiv 1 \pmod 3$. Άρα, $m \equiv 2 \pmod 3$. Επομένως, υπάρχει $k \in \mathbb{Z}$ ώστε $m = 3k + 2$.
Διακρίνουμε τρεις περιπτώσεις ανάλογα με την κλάση του $m \bmod 3$ και εργαζόμαστε ακριβώς όπως στην περίπτωση 1.

3. Εάν $\chi_\gamma(\lambda) = \omega^2$, δηλαδή $\omega^{2m} = \omega^2$, τότε $2m \equiv 2 \pmod 3$. Άρα, $m \equiv 1 \pmod 3$. Επομένως, υπάρχει $k \in \mathbb{Z}$ ώστε $m = 3k + 1$.
Διακρίνουμε τρεις περιπτώσεις ανάλογα με την κλάση του $m \bmod 3$ και εργαζόμαστε ακριβώς όπως στην περίπτωση 1.

□

4.4 Ο κυβικός χαρακτήρας του 2

Σε αυτή την παράγραφο προσδιορίζουμε τους πρώτους π της D για τους οποίους το 2 είναι κυβικό υπόλοιπο. Από την απλή παρατήρηση ότι, εάν η $x^3 \equiv 2 \mod \pi$, τότε επιλύεται για κάθε π" συνεταιρικό του π, σε συνδυασμό με το λήμμα 4.6.1 (βλ. Βοηθητικές προτάσεις, κεφάλαιο 4.6) μπορούμε να υποθέσουμε ότι ο π είναι πρώτιστος πρώτος. Εάν $\pi = q$ είναι ρητός πρώτος, τότε από το πόρισμα 4.1.13 έχουμε ότι $\chi_q(2) = 1$. Κατά συνέπεια, το 2 είναι κυβικό υπόλοιπο για όλους τους πρώτους αυτής της κατηγορίας.

Πρόταση 4.4.1. *Η $x^3 \equiv 2 \pmod{\pi}$ επιλύεται εάν $\pi \equiv 1 \pmod 2$, δηλαδή εάν $a \equiv 1 \pmod 2$ και $b \equiv 0 \pmod 2$.*

Απόδειξη. Έχουμε

$$\begin{aligned} \chi_\pi(2) &= \chi_2(\pi) \quad \text{(ν.κυβικής αντιστροφής)} \\ &\equiv \pi^{(\mathrm{N}2-1)/3} \text{ (πρόταση 4.1.11) } \equiv \pi^{(4-1)/3} \equiv \pi \pmod 2. \end{aligned} \tag{4.28}$$

Η $x^3 \equiv 2 \pmod{\pi}$ επιλύεται εάν $\chi_\pi(2) = 1$. Από τη σχέση (4.28), αποδεικνύεται άμεσα το ζητούμενο.

Πρόταση 4.4.2. *Εάν $p \equiv 1 \pmod 3$, τότε η $x^3 \equiv 2 \pmod{p}$ είναι επιλύσιμη εάν υπάρχουν ακέραιοι K και L τέτοιοι ώστε $p = K^2 + 27L^2$.*

Απόδειξη. Έστω $p = \pi\overline{\pi}$ η ανάλυση του p σε πρώτιστους πρώτους. Θέτουμε $\pi = a + b\omega$, οπότε $a \equiv 2$ και $b \equiv 0 \pmod 3$. Παρατηρούμε ότι $p = \pi\overline{\pi} = a^2 - ab + b^2$, οπότε και $4p = A^2 + 27B^2$, όπου $A = 2a - b$ και $B = b/3$.

Έστω τώρα ότι η $x^3 \equiv 2 \pmod{p}$ επιλύεται. Τότε επιλύεται και η $x^3 \equiv 2 \pmod{\pi}$, άρα, από την πρόταση 4.4.1 έχουμε ότι $\pi \equiv 1 \pmod 2$. Δηλαδή, ο b είναι άρτιος, οπότε και οι A, B είναι άρτιοι. Θέτοντας $K = \frac{B}{2}$ και $L = \frac{A}{2}$ έχουμε $p = K^2 + 27L^2$.

Αντίστροφα, υπόθετουμε ότι $p = K^2 + 27L^2$ για κάποιους $K, L \in \mathbb{Z}$. Τότε $4p = (2K)^2 + 27(2L)^2$, ενώ στην αρχή της απόδειξης είδαμε ότι $4p = A^2 + 27B^2$. Αλλά η πρόταση 3.3.5 μας λέει, ουσιαστικά, ότι τέτοιες αναπαραστάσεις του $4p$ είναι μοναδικές μέχρι προσήμου, οπότε $B = \pm 2K$. Συνεπώς, ο B είναι άρτιος, άρα και το ίδιο ισχύει και για τον b. Επομένως, $\pi \equiv a \pmod 2$. Εάν $a \equiv 0 \pmod 2$, τότε $p \equiv 0 \mod 2$, το οποίο είναι άτοπο διότι ο p είναι ρητός πρώτος $\equiv 1 \pmod 3$, άρα διάφορος του 2. Έπεται ότι $\pi \equiv a \equiv 1 \pmod 2$, οπότε (πρόταση 4.4.1) η $x^3 \equiv 2 \pmod{\pi}$ επιλύεται. Έστω $\beta \in \mathbb{Z}[\omega]$ μία λύση της. Τότε (βλ. πρόταση 4.6.3 (1)) υπάρχει $m \in \mathbb{Z}$ τέτοιος ώστε $m \equiv \beta \pmod{\pi}$, οπότε έχουμε $m^3 \equiv 2 \pmod{\pi}$, δηλαδή $m^3 - 2 \equiv 0 \pmod{\pi}$, όπου $m^3 - 2 \in \mathbb{Z}$. Από την

πρόταση 4.6.3 (2) έχουμε ότι $m^3 - 2 \equiv 0 \pmod{p}$, δηλαδή η $x^3 \equiv 2 \pmod{p}$ επιλύεται (στο $\mathbb{Z}$).

□

Παράδειγμα: Η $x^3 \equiv 2 \pmod{103}$ (ο 103 ειναι πρώτος) δεν επιλύεται, διότι δεν υπάρχουν $K, L \in \mathbb{Z}$ που να ικανοποιούν την ισότητα $103 = K^2 + 27L^2$. Πράγματι, αν υπήρχαν τέτοια K, L, θα ήταν, αναγκαστικά, $L^2 = 1$, αφού $27 \cdot 2^2 = 108 > 103$, άρα $K^2 = 103 - 27 = 76$, άτοπο.

Από την άλλη, για τον πρώτο 691 έχουμε $691 = 4^2 + 27 \cdot 5^2$. Επομένως, η $x^3 \equiv 2 \pmod{691}$ επιλύεται. Πράγματι, $94^3 \equiv 2 \pmod{31}$.

4.5 Γενικεύσεις.

Θεώρημα 4.5.1. [5] *Εάν γ, ϱ είναι πρώτιστα στοιχεία της D, τότε $\chi_\gamma(\varrho) = \chi_\varrho(\gamma)$. Στην ειδική περίπτωση που $\gamma = \pi$ (πρώτιστος πρώτος) και $\varrho = \overline{\pi}$, έχουμε $\chi_\pi(\overline{\pi}) = \chi_{\overline{\pi}}(\pi) = 1$.*

Απόδειξη. Θεωρούμε τις πρώτιστες αναλύσεις των γ, ϱ όπως στην απόδειξη της πρότασης 4.3.8, οπότε ισχύουν οι σχέσεις 4.14 και 4.15. Έστω γ_i τυχών πρώτος στην πρώτιστη ανάλυση του γ και ϱ_j τυχών πρώτος στην πρώτιστη ανάλυση του ϱ. Θα δείξουμε ότι

$$\chi_{\gamma_i}(\varrho_j) = \chi_{\varrho_j}(\gamma_i) \tag{4.29}$$

Εάν $(\mathrm{N}\gamma_i, \mathrm{N}\varrho_j) = 1$, τότε η (4.29) ισχύει από το θεώρημα 4.2.1.

Εάν $(\mathrm{N}\gamma_i, \mathrm{N}\varrho_j) > 1$, τότε διακρίνουμε περιπτώσεις.
Εξετάζουμε πρώτα την περίπτωση όπου $\mathrm{N}\gamma_i = \mathrm{N}\varrho_j = p^2$ για κάποιο ρητό πρώτο $p \equiv 2 \pmod{3}$. Από την πρόταση 4.1.4, έχουμε ότι οι γ_i, ϱ_j είναι ρητοί πρώτοι ίσοι με p. Δηλαδή, έχουμε $\gamma_i = p = \varrho_j$. Άρα, $\varrho_j | \gamma_i$ και $\gamma_i | \varrho_j$, απ¨ όπου (βλ. ορισμό 4.1.10) έχουμε $\chi_{\varrho_j}(\gamma_i) = 0$ και $\chi_{\gamma_i}(\varrho_j) = 0$, αντίστοιχα.
Στην περίπτωση όπου $\mathrm{N}\gamma_i = \mathrm{N}\varrho_j = p$ για κάποιο ρητό πρώτο $p \equiv 1 \pmod{3}$, παρατηρούμε ότι ισχύει $\gamma_i\overline{\gamma_i} = \varrho_j\overline{\varrho_j} = p$. Καθώς στην D έχουμε μονοσήμαντη ανάλυση, το ϱ_j θα είναι συνεταιρικό με το γ_i ή με το $\overline{\gamma_i}$. Από την πρόταση 4.3.3(3) γνωρίζουμε ότι δύο πρώτιστα στοιχεία που είναι συνεταιρικά, κατ' ανάγκη, ταυτίζονται. Δηλαδή, έχουμε $\varrho_j = \gamma_i$ ή $\varrho_j = \overline{\gamma_i}$.
Εάν $\varrho_j = \gamma_i$, τότε $\varrho_j | \gamma_i$ και $\gamma_i | \varrho_j$, απ' όπου $\chi_{\varrho_j}(\gamma_i) = 0$ και $\chi_{\gamma_i}(\varrho_j) = 0$ αντίστοιχα (από τον ορισμό 4.1.10).
Άρα, σε αυτές τις περιπτώσεις και τα δύο μέλη της (4.29) είναι μηδέν.
Εάν $\varrho_j = \overline{\gamma_i}$, θέτουμε $\gamma_i = \mu = a + bi$, όπου $a = 3m - 1$ και $b = 3n$, άρα $\varrho_j = \overline{\mu} = a + b\omega^2$. Παρατηρούμε ότι $-a \equiv b\omega \pmod{\mu}$, δηλαδή $-a\omega \equiv b\omega^2 \pmod{\mu}$. Άρα

[5] Γενίκευση του θεωρήματος 4.2.1.

$\overline{\mu} = a + b\omega^2 \equiv a - a\omega \equiv a\lambda \pmod{\mu}$. Επομένως, $\chi_\mu(\overline{\mu}) = \chi_\mu(a\lambda) = \chi_\mu(a)\chi_\mu(\lambda)$ και χρησιμοποιώντας την πρόταση 4.3.9 (3) και το θεώρημα 4.3.1 έχουμε

$$\chi_\mu(\overline{\mu}) = \omega^m\omega^{2m} = \omega^{3m} = 1$$

Επομένως,

$$1 = \chi_\mu(\overline{\mu}) = \chi_{\overline{\mu}}(\overline{\mu}) \overset{4.1.12}{=} \chi_{\overline{\mu}}(\mu)^2$$

Από τον ορισμό 4.1.10 γνωρίζουμε ότι $\chi_{\overline{\mu}}(\mu)$ είναι $1, \omega$ ή ω^2, άρα $\chi_{\overline{\mu}}(\mu) = 1 = \chi_\mu(\overline{\mu})$.

□

Θεώρημα 4.5.2. *Για κάθε ρητό πρώτο $p \equiv 1 \pmod 3$ υπάρχουν $a, b \in \mathbb{Z}$, $a \equiv 2 \pmod 3$, $b \equiv 0 \pmod 3$ και $p = a^2 - ab + b^2$. Αν οι a, b έχουν αυτές τις ιδιότητες, τότε οι $2a - b$ και $\frac{b}{3}$ είναι κυβικά ισοϋπόλοιπα $\bmod p$.*

Απόδειξη. Από το θεώρημα 3.3.1 ξέρουμε ότι υπάρχουν $a_1, b_1 \in \mathbb{Z}$, τέτοιοι ώστε $p = a_1^2 - a_1b_1 + b_1^2$. Θέτουμε $\pi_1 = a_1 + b_1\omega$, οπότε ο π_1 είναι πρώτος της D (πρόταση 4.1.3). Χάρη στο λήμμα 4.6.1 μπορούμε, πολλαπλασιάζοντας τον π_1 με κατάλληλη μονάδα της D, να βρούμε πρώτιστο πρώτο π με $\mathrm{N}\pi = \mathrm{N}\pi_1 = p$, οπότε, αν θέσουμε $\pi = a + b\omega$ με $a, b \in \mathbb{Z}$, είναι $a \equiv 2 \pmod 3$ και $b \equiv 0 \pmod 3$.

Από την πρόταση 4.5.1 έχουμε ότι $\chi_\pi(\overline{\pi}) = 1 = \chi_{\overline{\pi}}(\pi)$.
Παρατηρούμε ότι $\pi = a + b\omega = 2a - b - ((a - b) - b\omega) \equiv 2a - b \pmod{\overline{\pi}}$. Επομένως, (βλ. πρόταση 4.1.11 (4)) έχουμε ότι $1 = \chi_{\overline{\pi}}(\pi) = \chi_{\overline{\pi}}(2a - b)$. Από την βοηθητική πρόταση 4.6.4 συμπεραίνουμε τώρα ότι η $x^3 \equiv 2a - b \pmod p$ επιλύεται στο $\mathbb{Z}$, δηλαδή το $2a - b$ είναι κυβικό υπόλοιπο $\bmod p$.

Τώρα θέτουμε $b = 3B$, $B \in \mathbb{Z}$ και θα δείξουμε ότι και ο B είναι κυβικό ισοϋπόλοιπο $\bmod p$. Έχουμε $4p = (2a-b)^2+3b^2 = (2a-b)^2+27B^2$ και η σχέση αυτή στο $\mathbb{F}_p$ γράφεται $B^2 = -27^{-1}(2a-b)^2$. Παραπάνω δείξαμε ότι το $2a-b$ είναι κύβος στο $\mathbb{F}_p$, συνεπώς και το $(2a-b)^2$ είναι κύβος. Επιπλέον, $-27^{-1} = (-3^{-1})^3$, επομένως, το B^2 είναι κύβος στην ομάδα $\mathbb{F}_p^*$, άρα, από την συμπληρωματική πρόταση 4.6.6, έπεται ότι και το B είναι κύβος στην ομάδα $\mathbb{F}_p^*$. Το συμπέρασμα αυτό ισοδυναμεί με το ότι ο ακέραιος B είναι κυβικό ϋπόλοιπο $\bmod p$.

□

Εξαιρετικά ενδιαφέρον είναι το γεγονός ότι, ενώ η διατύπωση του παραπάνω θεωρήματος είναι της στοιχειώδους Θεωρίας Αριθμών, η απόδειξη γίνεται με τη βοήθεια των κυβικών χαρακτήρων.

Θεώρημα 4.5.3. [6] *Εάν το $\gamma = A + B\omega$ είναι πρώτιστο, $A = 3M - 1$ και $B = 3N$ με $M, N \in \mathbb{Z}$, τότε $\chi_\gamma(\lambda) = \omega^{2M}$.*

Απόδειξη. Θα χρησιμοποιήσουμε επαγωγή ως προς το πλήθος t των πρωτίστων πρώτων, οι οποίοι εμφανίζονται στην πρώτιστη ανάλυση του γ (βλ. πρόταση 4.3.3).

[6] Γενίκευση του θεωρήματος 4.3.1.

Εάν $t = 1$, τότε $\gamma = \varepsilon\gamma_1$. Τα γ, γ_1 είναι πρώτιστα στοιχεία άρα $\varepsilon = 1$. Δηλαδή $\gamma = \gamma_1$ είναι πρώτιστος πρώτος. Επομένως, από το θεώρημα 4.3.1 ισχύει $\chi_\gamma(\lambda) = \omega^{2M}$.
Έστω ότι ισχύει το ζητούμενο για τυχόν πρώτιστο στοιχείο της D με k πρώτιστους πρώτους παράγοντες.
Έστω γ πρώτιστο στοιχείο της D με $k+1$ πρώτιστους πρώτους παράγοντες γράφεται όπως στην (4.13). Το $\delta = \varepsilon'\gamma_1 \cdots \gamma_k$ για κάποιο $\varepsilon' = \pm 1$, είναι πρώτιστο στοιχείο της D. Άρα, για το δ ισχύει η επαγωγική υπόθεση. Τα δ, γ_{k+1} είναι πρώτιστα στοιχεία της D, άρα, από τη σχέση (4.13) και την πρόταση 4.3.3, έχουμε $\gamma = -\delta\gamma_{k+1}$. Άρα, εάν $\gamma_{k+1} = a + bi$ όπου $a = 3m - 1, b = 3n$ και $\delta = c + di$ όπου $c = 3K - 1, d = 3L$, έχουμε

$$\begin{aligned} \chi_\gamma(\lambda) &= \chi_{-\delta\gamma_{k+1}}(\lambda) = \chi_\delta(\lambda)\chi_{\gamma_{k+1}}(\lambda) \\ &= \omega^{2K}\omega^{2m} = \omega^{2(K+m)} \end{aligned}$$

Αρκεί να δείξουμε ότι $2(K + m) \equiv 2M \pmod 3$. Η σχέση αυτή ισοδυναμεί με $K + m \equiv M \pmod 3$, το οποίο δείχθηκε στην απόδειξη της πρότασης 4.3.7.

□

4.6 Παράρτημα - Βοηθητικές Προτάσεις.

Λήμμα 4.6.1. *Για κάθε πρώτο $\pi \in D$, με $\mathrm{N}\pi = p \equiv 1 \pmod 3$, όπου p ρητός πρώτος, υπάρχει μονάδα ε τέτοια ώστε ο $\varepsilon\pi$ να είναι πρώτιστος πρώτος.*

Απόδειξη. Έστω $\pi = a + b\omega, a, b \in \mathbb{Z}$. Από την υπόθεση $\mathrm{N}\pi = p \equiv 1 \pmod 3$, και επειδή $\mathrm{N}\pi = a^2 - ab + b^2 \equiv (a+b)^2 \pmod 3$, έχουμε ότι $(a+b)^2 \not\equiv 0 \pmod 3$, απ¨ όπου έπεται ότι $a + b \not\equiv 0 \pmod 3$.

Άρα, διακρίνουμε τις εξής περιπτώσεις:

1. $a \equiv 2 \pmod 3$ και $b \equiv 0 \pmod 3$. Τότε ο π είναι πρώτιστος πρώτος.

2. $a \equiv 2 \pmod 3$ και $b \equiv 2 \pmod 3$. Τότε υπάρχουν $k, \ell \in \mathbb{Z}$ ώστε $a = 3k+2$ και $b = 3\ell + 2$. Δηλαδή, $\pi = (3k + 2) + (3\ell + 2)\omega$ και

$-\omega\pi = -3k\omega - 2\omega - 3\ell\omega^2 - 2\omega^2 = -3k\omega - 2\omega + 3\ell(1+\omega) + 2(1+\omega) = (3\ell+2) + 3(\ell-k)\omega.$

Άρα, ο $-\omega\pi$ είναι πρώτιστος πρώτος.

3. $a \equiv 0 \pmod 3$ και $b \equiv 1 \pmod 3$. Τότε $\pi = 3k + (3\ell + 1)\omega$ για κάποια $k, \ell \in \mathbb{Z}$ και έχουμε

$-\omega^2\pi = 3k(-\omega^2) + (3\ell+1)(-\omega^3) = 3k(1+\omega) - 3\ell - 1 = [3(k-\ell-1)+2] + 3k\omega.$

Άρα, ο $-\omega^2\pi$ είναι πρώτιστος πρώτος.

4. $a \equiv 0 \pmod 3$ και $b \equiv 2 \pmod 3$. Τότε υπάρχουν $k, \ell \in \mathbb{Z}$ ώστε $a = 3k$ και $b = 3\ell + 2$. Δηλαδή, $\pi = 3k + (3\ell + 2)\omega$ και

$\omega^2\pi = 3k(\omega^2) + (3\ell+1)(\omega^3) = -3k(1+\omega) + 3\ell + 1 = [3(-k+\ell)+2] - 3k\omega.$
Άρα, ο $\omega^2\pi$ είναι πρώτιστος πρώτος.

5. $a \equiv 1 \pmod 3$ και $b \equiv 0 \pmod 3$. Τότε υπάρχουν $k, \ell \in \mathbb{Z}$ ώστε $a = 3k+1$ και $b = 3\ell$. Δηλαδή, $\pi = 3k + 1 + 3\ell\omega$ και

$$-\pi = (-3k-1) - 3\ell\omega = [3(-k-1)+2] - 3\ell\omega.$$

Άρα, ο $-\pi$ είναι πρώτιστος πρώτος.

6. $a \equiv 1 \pmod 3$ και $b \equiv 1 \pmod 3$. Τότε υπάρχουν $k, \ell \in \mathbb{Z}$ ώστε $a = 3k+1$ και $b = 3\ell + 1$. Δηλαδή, $\pi = 3k + 1 + (3\ell+1)\omega$ και
$\omega\pi = 3k\omega+\omega+3\ell\omega^2+\omega^2 = 3k\omega+\omega+3\ell(-1-\omega)+(-1-\omega) = [-3(\ell+1)+2]+3(k-\ell)\omega.$
Άρα, ο $\omega\pi$ είναι πρώτιστος πρώτος.

□

Πρόταση 4.6.2. *Κάθε μ στο D αναλύεται σε γινόμενο της μορφής*

$$\mu = (-1)^a\, \omega^b\, \lambda^c\, \pi_1^{a_1}\, \pi_2^{a_2} \cdots \pi_t^{a_t}$$

όπου $\pi_1, \cdots, \pi_t$ είναι πρώτιστοι πρώτοι, $a_1, \cdots, a_t$ είναι θετικοί ακέραιοι και a, b, c είναι μη αρνητικοί ακέραιοι.

Απόδειξη. Από τον ορισμό 4.1.5 και το λήμμα 4.6.1 έχουμε ότι, κάθε πρώτος μη συνεταιρικός του λ, είναι συνεταιρικός με κάποιο πρώτιστο πρώτο. Άρα, αν αναλύσουμε τον μ σε πρώτους παράγοντες, θα έχουμε

$$\mu = \lambda^c \varepsilon \pi_1^{a_1} \cdots \pi_t^{a_t}$$

όπου $\pi_1, \cdots, \pi_t$ είναι πρώτιστοι πρώτοι, $a_1, \cdots, a_t$ είναι θετικοί ακέραιοι, ε είναι μονάδα της D και c ακέραιος ≥ 0. Επειδή $\varepsilon \in \{\pm 1, \pm\omega, \pm\omega^2\}$, μπορούμε αντί του ε να γράψουμε $(-1)^a\omega^b$, όπου $a \in \{0,1\}$ και $b \in \{0,1,2\}$.

□

Έστω γ πρώτος πρώτιστος. Για τον υπολογισμό του $\chi_\gamma(\mu)$ βλέπουμε στην πρόταση 4.6.2 ότι αρκεί να υπολογίσουμε $\chi_\gamma(-1), \chi_\gamma(\omega), \chi_\gamma(\lambda)$ και $\chi_\gamma(\pi)$, όπου π είναι πρώτιστος πρώτος. Αφού $-1 = (-1)^3$ έχουμε $\chi_\gamma(-1) = 1$.

Πρόταση 4.6.3. *Έστω π πρώτος στη D με $\mathrm{N}\pi = p \equiv 1 \pmod 3$. Τότε:*

1. *για κάθε $\mu \in D$, υπάρχει ακέραιος M ώστε $\mu \equiv M \pmod \pi$.*
2. *εάν $m \in \mathbb{Z}$ και $m \equiv 0 \pmod \pi$ (στη D) , τότε $m \equiv 0 \pmod p$ (στο $\mathbb{Z}$).*
3. *εάν $m \in \mathbb{Z}$ και $m \equiv 0 \pmod \lambda$ (στη D) , τότε $m \equiv 0 \pmod 3$ (στο $\mathbb{Z}$).*

Απόδειξη. Έστω $\pi = a + b\omega$, οπότε $p = a^2 - ab + b^2$, άρα $p \not| b$. Πράγματι, διότι, διαφορετικά, η τελευταία ισότητα θα συνεπαγόταν $p|a^2$, άρα $p|a$. Αλλά τότε $p^2|(a^2 - ab + b^2) = p$, άτοπο.

1. Έστω $\mu = m + n\omega$ για κάποια $m, n \in \mathbb{Z}$. Θεωρούμε $c \in \mathbb{Z}$ τέτοιο ώστε $bc \equiv n \pmod{p}$. Αυτό είναι δυνατό, διότι δείξαμε παραπάνω ότι $p \nmid b$. Τότε,

$$\begin{aligned} \mu - c\pi &= m + n\omega - c(a + b\omega) = (m - ca) + (n - cb)\omega \\ &\equiv m - ca \pmod{p} \\ &\equiv m - ca \pmod{\pi} \end{aligned}$$

Άρα, $\mu \equiv \mu - c\pi \equiv m - ca \pmod{\pi}$ και θέτοντας $m - ca = M \in \mathbb{Z}$, έχουμε το αποδεικτέο.

2. Εάν $m \equiv 0 \pmod{\pi}$, υπάρχει $\mu \in D$ ώστε $m = \mu\pi$. Απ' όπου $\mathrm{N}m = \mathrm{N}\mu\mathrm{N}\pi$, δηλαδή $m^2 = kp$, με $k = \mathrm{N}\mu \in \mathbb{Z}$. Άρα $p|m^2$, οπότε $p|m$ (στο $\mathbb{Z}$).

3. Έστω $m \equiv 0 \pmod{\lambda}$. Τότε υπάρχει $\mu \in D$ ώστε $m = \mu\lambda$. Επομένως, $\mathrm{N}m = \mathrm{N}\mu\mathrm{N}\lambda$, δηλαδή $m^2 = k3$, όπου $k = \mathrm{N}\mu \in \mathbb{Z}$. Άρα, $3|m^2$ (στο $\mathbb{Z}$), οπότε $3|m$ (στο $\mathbb{Z}$).

□

Πρόταση 4.6.4. *Έστω $a \in \mathbb{Z}$, πρώτος $p \equiv 1 \pmod{3}$ και $p = \pi\overline{\pi}$, όπου π πρώτιστος πρώτος της D. Η $x^3 \equiv a \pmod{p}$ επιλύεται στο $\mathbb{Z}$ εάν $\chi_\pi(a) = 1$.*

Απόδειξη. Έστω $\chi_\pi(a) = 1$. Τότε $\pi \nmid a$ διότι, διαφορετικά, θα είχαμε $\chi_\pi(a) = 0$. Οπότε, από την πρόταση 4.1.11(1), η $x^3 \equiv a \pmod{\pi}$ επιλύεται, δηλαδή υπάρχει $\beta \in D$ ώστε

$$\beta^3 \equiv a \pmod{\pi} \tag{4.30}$$

Από την πρόταση 4.6.3, (1) υπάρχει $B \in \mathbb{Z}$ ώστε $B \equiv \beta \pmod{\pi}$, άρα

$$B^3 \equiv \beta^3 \pmod{\pi} \tag{4.31}$$

Από την (4.30), λόγω της (4.31), έχουμε ισοδύναμα $B^3 \equiv a \pmod{\pi}$, άρα $B^3 - a \equiv 0 \pmod{\pi}$, όπου $B^3 - a \in \mathbb{Z}$. Από την πρόταση 4.6.3, (2), έπεται ότι $B^3 - a \equiv 0 \pmod{p}$, δηλαδή $B^3 \equiv a \pmod{p}$. Οπότε, η $x^3 \equiv a \pmod{p}$ επιλύεται στο $\mathbb{Z}$.

Αντίστροφα, έστω ότι η $x^3 \equiv a \pmod{p}$ επιλύεται στο $\mathbb{Z}$. Τότε επιλύεται στην D, διότι $\mathbb{Z} \subset D$. Επειδή $\pi|p$, έχουμε ότι η $x^3 \equiv a \pmod{\pi}$ επιλύεται στην D. Οπότε, από την πρόταση 4.1.11(1) έπεται ότι $\chi_\pi(a) = 1$.

□

Πρόταση 4.6.5. *Εάν ο $p \in \mathbb{Z}$ είναι πρώτος στο $\mathbb{Z}$, τότε*

$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} 0 \pmod{p}, & \text{εάν} p - 1 \nmid k \\ -1 \pmod{p}, & \text{εάν} p - 1 | k. \end{cases}$$

Απόδειξη. Έστω a πρωταρχική ρίζα mod$p$. Δηλαδή, $a^{p-1} \equiv 1 \pmod{p}$ και $a^m \not\equiv 1 \pmod{p}$ για $0 < m < p - 1$. Άρα, τα $a, a^2, \cdots, a^{p-1}$ μας δίνουν ένα πλήρες σύστημα υπολοίπων mod$p$. Επομένως,

$$1^k + 2^k + \cdots + (p-1)^k \equiv a^k + a^{2k} + \cdots + a^{(p-1)k} \pmod{p} \tag{4.32}$$

Εάν $p-1|k$, τότε υπάρχει ακέραιος ℓ ώστε $k=(p-1)\ell$. Οπότε, $a^k=a^{(p-1)\ell}=(a^{p-1})^\ell\equiv 1^\ell\equiv 1 \pmod p$. Άρα,

$$1^k+2^k+\cdots+(p-1)^k\equiv \underbrace{1+1+\cdots+1}_{p-1 \text{ φορές}}\equiv p-1\equiv -1 \pmod p.$$

Εάν $p-1\not| k$, τότε $a^k\not\equiv 1 \pmod p$. Επομένως, χρησιμοποιώντας την (4.32),

$$1^k+2^k+\cdots+(p-1)^k\equiv \frac{a^{(p-1)k}-1}{a^k-1}\equiv \frac{1^k-1}{a^k-1}\equiv 0 \pmod p.$$

□

Πρόταση 4.6.6. *Έστω $(G,\cdot)$ πολλαπλασιαστική ομάδα, $a\in G$ και $m\in\mathbb{N}$, τέτοια ώστε $a^m=b^n$ για κάποια $b\in G$, $n\in\mathbb{N}$, όπου $(m,n)=1$. Τότε το a είναι $n-$οστή δύναμη.*

Απόδειξη. Από υπόθεση έχουμε $(m,n)=1$, άρα υπάρχουν ακέραιοι k,ℓ, τέτοιοι ώστε $m\,k+n\,\ell=1$. Επομένως, $a=(a^m)^k(a^\ell)^n=(b^n)^k(a^\ell)^n=(b^ka^\ell)^n$.

□

Λήμμα 4.6.7. *Έστω $\gamma=A+B\omega$ πρώτιστο στοιχείο και $A=3M-1$, $B=3N$. Θεωρούμε την πρώτιστη ανάλυση του γ , $\gamma=\pm\pi_1\cdots\pi_k q_1\cdots q_\ell$, όπου π_i είναι μη-ρητός πρώτιστος πρώτος με στάθμη $p_i\equiv 1 \pmod 3$, για κάθε $i=1,\cdots,k$ και q_j είναι ρητός πρώτος $\equiv 2 \pmod 3$ για κάθε $j=1,\cdots,\ell$. Τότε ισχύει*

$$M+N\equiv\sum_{i=1}^{k}\frac{p_i-1}{3}+\sum_{j=1}^{\ell}\frac{q_j^2-1}{3} \pmod 3.$$

Απόδειξη. Από τον ορισμό

$$\chi_\gamma(\omega)=\prod_{i=1}^{k}\chi_{\pi_i}(\omega)\prod_{j=1}^{\ell}\chi_{q_j}(\omega). \tag{4.33}$$

Από την πρόταση

$$\chi_\gamma(\omega)=\omega^{M+N}. \tag{4.34}$$

Επιπλέον, για κάθε $i=1,\cdots,k$ και για κάθε $j=1,\cdots,\ell$ ισχύει

$$\begin{aligned} & \chi_{\pi_i}(\omega) \equiv \omega^{(\mathrm{N}\pi_i-1)/3}\equiv\omega^{(p_i-1)/3} \pmod{\pi_i} \\ \text{και} \quad & \chi_{q_j}(\omega) \equiv \omega^{(\mathrm{N}q_j-1)/3}\equiv\omega^{(q^2-1)/3} \pmod{q_j} \end{aligned}$$

αντίστοιχα, όπου $\chi_{\pi_i}(\omega)=\omega^{\mu_i}$, για κάποιο $\mu_i=0,1$ ή 2 και $\chi_{q_j}(\omega)=\omega^{\nu_j}$, για κάποιο $\nu_j=0,1$ ή 2. Επομένως, από το λήμμα

$$\chi_{\pi_i}(\omega)=\omega^{(p_i-1)/3} \qquad \text{και} \qquad \chi_{q_j}(\omega)=\omega^{(q^2-1)/3}, \tag{4.35}$$

για κάθε $i = 1, \cdots, k$ και q_j και για κάθε $j = 1, \cdots, \ell$, αντίστοιχα.

Επομένως, από τη σχέση 4.33, σε συνδυασμό με τις 4.34 και 4.35, έχουμε διαδοχικά

$$\begin{aligned} \omega^{M+N} &= \prod_{i=1}^{k} \omega^{(p_i-1)/3} \prod_{j=1}^{\ell} \omega^{(q_j^2-1)/3} \\ &= \omega^{\sum_{i=1}^{k}(p_i-1)/3}\, \omega^{\sum_{j=1}^{\ell}(q_j^2-1)/3} \\ &= \omega^{\sum_{i=1}^{k}(p_i-1)/3 + \sum_{j=1}^{\ell}(q_j^2-1)/3}, \end{aligned}$$

απ¨ όπου έπεται άμεσα το ζητούμενο.

□