Νόμοι Αντιστροφής στην Θεωρία Αριθμών- Ιστορική προσέγγιση

Ασπασία Χαλκιαδάκη

Ιούνιος 2025

Πανεπιστήμιο Κρήτης

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών

Επιβλέπων καθηγητής: Ιωάννης Αντωνιάδης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

"The history of the general reciprocity law
is long and complicated
involving the creation of a good portion
of algebraic number theory and class field theory."
(Michael Rosen "Number Theory in Function Fields")

Εισαγωγή

Η κινητήρια δύναμη ανάπτυξης της Θεωρίας Αριθμών οφείλεται σε δύο κυρίως θέματα-προβλήματα. Το πρώτο είναι η Εικασία του Fermat και το δεύτερο οι Νόμοι Αντιστροφής. Θα μπορούσε κανείς να ισχυριστεί ότι και οι Νόμοι Αντιστροφής ξεκινούν από την έρευνα του Fermat.

Ο Fermat απέδειξε ότι ένας περιττός, πρώτος αριθμός μπορεί να παρασταθεί από άθροισμα τετραγώνων δύο ακεραίων, τότε και μόνο τότε όταν $p \equiv 1 \pmod 4$, κάτι το οποίο είναι ισοδύναμο με το $\left(\frac{-1}{p}\right) = 1$. Αλλά, μια προκαταρκτική εκδοχή του Τετραγωνικού Νόμου Αντιστροφής ανακαλύφθηκε γύρω στο 1742 από τον Euler στην έρευνά του σχετικά με τους πρώτους διαιρέτες αριθμών της μορφής $a^n \pm b^n$ (όπως, για παράδειγμα οι αριθμοί Mersenne και οι αριθμοί Fermat). Η τελική εκδοχή του Euler, δημοσιεύτηκε το 1785, δύο χρόνια μετά το θάνατό του. Ξαναανακαλύφθηκε από τον Legendre το 1788. Ο Legendre έδωσε μία απόδειξη, η οποία, όμως, ήταν ατελής. Παρά τις προσπάθειές του, ο Legendre δεν κατάφερε τελικά να δώσει πλήρη απόδειξη. Η πρώτη πλήρης απόδειξη, δόθηκε από τον Gauss στα 18 χρόνια του. Του πήρε ένα ολόκληρο χρόνο για να παρουσιάσει την πρώτη του απόδειξη (8 Απριλίου του 1796). Δέκα εβδομάδες αργότερα, έδωσε μία δεύτερη απόδειξη, η οποία είναι πιο απλή, αλλά χρησιμοποίησε τη θεωρία τετραγωνικών μορφών.
[[4] σελ. 61 για τα ιστορικά στοιχεία]
Η πιο συνηθισμένη απόδειξή του, που εμφανίζεται στη βιβλιογραφία μέχρι σήμερα, είναι αυτή που χρησιμοποιεί το λεγόμενο Λήμμα του Gauss και είναι η τρίτη απόδειξη. Η τέταρτη απόδειξη χρησιμοποιεί αθροίσματα του Gauss, τα οποία, όπως θα δούμε στην εργασία, γενικεύοντάς τα καταλλήλως χρησιμοποιούνται για τις αποδείξεις ανωτέρων Νόμων Αντιστροφής. Συνολικά, δόθηκαν τελικά 8 διαφορετικές αποδείξεις από τον Gauss. Ονόμασε, μάλιστα, ¨θεμελιώδες¨ θεώρημα ή ¨χρυσό¨ θεώρημα τον Τετραγωνικό Νόμο Αντιστροφής.

Η παρούσα εργασία αναφέρεται στους Νόμους Αντιστροφής και, μάλιστα, με μία ιστορική προσέγγιση. Στο δεύτερο Κεφάλαιο αναπτύσσεται ο διτετραγωνικός νόμος αντιστροφής. Πέρα από την απόδειξη του τετραγωνικού νόμου αντιστροφής, ο Gauss εργάστηκε και στον διτετραγωνικό νόμο αντιστροφής και μάλιστα κατάφερε και διατύπωσε την Πρόταση σωστά, αλλά δεν κατάφερε να το αποδείξει. Στην προσπάθειά του να το αποδείξει όρισε για πρώτη φορά το ομώνυμο δακτύλιο $\mathbb{Z}[i]$.

Οι πρώτες πλήρεις αποδείξεις για τον διτετραγωνικό και κυβικό νόμο αντιστροφής δημοσιεύθηκαν το 1844 από τον Eisenstein (μαζί με τους αντίστοιχους συμπληρωματικούς νόμους). Βέβαια, ο Jacobi τους είχε αποδείξει πριν από τον Eisenstein το 1837 στις παραδόσεις του μαθήματός του στο Königsberg. Ο Jacobi εργαζόταν σε μία γενίκευση του κυβικού και διτετραγωνικού νόμου αντιστροφής χρησιμοποιώντας την κυκλοτομία, αλλά η μη-ύπαρξη

(εν γένει) μονοσήμαντης παραγοντοποίησης ήταν ένα σημαντικό εμπόδιο. Μόνο ύστερα από την εισαγωγή τον λεγόμενων ιδεωδών αριθμών από τον Kummer (με σκοπό την εφαρμογή της θεωρίας στην εύρεση ενός γενικού νόμου αντιστροφής) έγινε δυνατό να κάνει κανείς αριθμητική στα κυκλοτομικά σώματα $\mathbb{Q}(\zeta_l)$.

Ο Eisenstein, ο οποίος είχε μέχρι τότε προτίμηση στη γλώσσα των μορφών, αναγνώρισε γρήγορα την ανωτερότητα της προσέγγισης του Kummer και κατάφερε να αποδείξει μία ειδική μορφή του γενικού νόμου αντιστροφής που φέρει το όνομα ¨Νόμος Αντιστροφής του Eisenstein".

Ο Kummer είχε τελικά καταφέρει να αποδείξει ανάλογο Νόμο με αυτόν του Eisenstein, αλλά μόνο για τους λεγόμενους ομαλούς πρώτους αριθμούς l, δηλαδή αυτούς που δεν διαιρούν τον αριθμό κλάσεων ιδεωδών του αντίστοιχου κυκλοτομικού σώματος $\mathbb{Q}(\zeta_l)$.

Στο τέταρτο Κεφάλαιο της εργασίας αποδεικνύεται ο ¨Νόμος Αντιστροφής του Eisenstein". Κατά την απόδειξη γίνεται χρήση ενός σημαντικού Θεωρήματος του Stickelberger (της λεγόμενης σχέσης του Stickelberger), από το 1890.

Στις 8 Αυγούστου του 1900 διοργανώθηκε στο Παρίσι το Δεύτερο Διεθνές συνέδριο Μαθηματικών. Ως ένας από τους κύριους ομιλητές (main speakers) προσκλήθηκε ο David Hilbert. Στη διάλεξή του παρουσίασε 23 προβλήματα των Μαθηματικών, τα οποία θεωρούσε σημαντικά και τα οποία ¨έμπαιναν¨ άλυτα στο κατώφλι του 20ου αιώνα. Ένα από αυτά, συγκεκριμένα το ένατο πρόβλημα, αφορούσε την εύρεση ενός γενικού νόμου αντιστροφής:
Für einen beliebigen Zahlkörper soll das Reziprozitätsgesetz der l-ten Potenzreste bewiesen werden."
Η μετάφραση του οποίου είναι: ¨Θα πρέπει να αποδειχθεί ο Νόμος Αντιστροφής των l-οστών συμβόλων υπολοίπων για οποιοδήποτε αλγεβρικό σώμα αριθμών.¨

Αλλά αυτό είναι μία άλλη ιστορία...

Ηράκλειο, Ιούνιος 2025

Περιεχόμενα

1 Ο Νόμος Τετραγωνικής Αντιστροφής

1.1 Διατύπωση του Τετραγωνικού Νόμου Αντιστροφής

Ορισμός:

Ο ακέραιος a θα λέγεται ότι είναι τετραγωνικό υπόλοιπο modp όταν η ισοτιμία $x^2 \equiv a \pmod{p}$, $p \in \mathbb{P}$, $p \neq 2$, $p \nmid a$, έχει λύση και ότι δεν είναι τετραγωνικό υπόλοιπο όταν η παραπάνω ισοτιμία δεν έχει λύση.

Ορισμός- Σύμβολο του Legendre:

Αν $a \in \mathbb{Z}$ και $p \in \mathbb{P}$, $p \neq 2$, $p \nmid a$ τότε το σύμβολο του Legendre $\left(\frac{a}{p}\right)$ ορίζεται:

$\left(\frac{a}{p}\right)$ $\begin{cases} +1, & \text{αν ο } a \text{ είναι τετραγωνικό υπόλοιπο modp} \\ -1, & \text{όταν δεν είναι τετραγωικό υπόλοιπο modp.} \end{cases}$

Παρατήρησεις: 1) Αν $a \equiv b \pmod{p}$, τότε $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ με το αντίστροφο να μην ισχύει.
2) Αν $p|a$ τότε ορίζουμε $\left(\frac{a}{p}\right) = 0$.

Πρόταση 1.1.1:

Έστω $a \in \mathbb{Z}$ και p πρώτος αριθμός, $p \neq 2$.
Ισχύουν:
a) $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$

b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

c) Αν $a \equiv b \pmod{p}$, τότε $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Απόδειξη
Αν το p διαιρεί το a ή το b, όλα τα παραπάνω είναι τετριμμένα. Υποθέτουμε, λοιπόν, ότι $p \nmid a$ και ότι $p \nmid b$.
Ξέρουμε ότι $a^{p-1} \equiv 1 \pmod{p}$ και έτσι $(a^{(p-1)/2} + 1) \cdot (a^{(p-1)/2} - 1) = a^{p-1} - 1 \equiv 0 \pmod{p}$.
Έπεται ότι $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Ισχύει ότι $a^{(p-1)/2} \equiv 1 \pmod{p}$ αν και μόνο αν το a είναι τετραγωνικό υπόλοιπο modp.

Αυτό γιατί η $\mathbb{Z}_p{}^*$ είναι κυκλική ομάδα τάξης $p-1$, δηλαδή υπάρχει ένας γεννήτορας g τέτοιος ώστε κάθε στοιχείο μπορεί να γραφεί ως δύναμη του g.

Ισχύει, δηλαδή, $a = g^k \pmod p$. Τότε: $a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} = g^{\frac{k(p-1)}{2}} \pmod p$.

Αν, τώρα, το k είναι άρτιος, τότε το $a = g^{2m}$ είναι τέλειο τετράγωνο (δηλ. τετραγωνικό υπόλοιπο) και:
$a^{\frac{p-1}{2}} \equiv g^{\frac{2m(p-1)}{2}} \equiv g^{(p-1)m} \equiv (g^{p-1})^m \equiv 1^m = 1 \pmod p$.

Αν, τώρα, το k είναι περιττός, έστω $k = 2m + 1$, τότε:
$a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} \equiv g^{\frac{(2m+1)(p-1)}{2}} \equiv g^{(p-1)m} \cdot g^{\frac{(p-1)}{2}} \equiv 1 \cdot g^{\frac{p-1}{2}} \pmod p$.

Όμως, το $g^{\frac{p-1}{2}}$ είναι ισότιμο με -1 modp, γιατί η τάξη του g είναι $p - 1$ και άρα το $g^{\frac{p-1}{2}}$ είναι στοιχείο τάξης 2. Αλλά, τα μοναδικά στοιχεία με $x^2 \equiv 1 \pmod p$ είναι τα 1 και -1. Επειδή, όμως, το g είναι γεννήτορας, το $g^{\frac{p-1}{2}}$ δεν μπορεί να είναι ισότιμο με 1 modp και άρα θα είναι ισότιμο με -1 modp.
Αυτό αποδεικνύει το a).

Για να αποδείξουμε το b) εφαρμόζουμε το a).
Έχουμε $ab^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod p$ και $ab^{(p-1)/2} = a^{(p-1)/2} \cdot b^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
Άρα $\left(\frac{ab}{p}\right) \equiv \left(\frac{\alpha}{p}\right) \cdot \left(\frac{b}{p}\right) \pmod p$ που συνεπάγεται και την αντίστοιχη ισότητα.

Το c) είναι προφανές από τον ορισμό.

Πόρισμα 1.1.2: [[1] Πρόταση 5.1.4]

Για κάθε περιττό πρώτο p υπάρχουν ακριβώς $\frac{p-1}{2}$ μη ισοδύναμα τετραγωνικά υπόλοιπα modp και συνεπώς $\frac{p-1}{2}$ που δεν είναι τετραγωνικά υπόλοιπα modp.

Παρατήρηση:

Άμεση συνέπεια του Πορίσματος 1.1.2 είναι ότι $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

Πόρισμα 1.1.3:

Το γινόμενο δύο τετραγωνικών υπολοίπων είναι κι αυτό τετραγωνικό υπόλοιπο, το γινόμενο δύο μη τετραγωνικών υπολοίπων είναι τετραγωνικό υπόλοιπο και το γινόμενο ενός τετραγωνικού υπολοίπου με ένα μη τετραγωνικό υπόλοιπο είναι μη τετραγωνικό υπόλοιπο modp.

ΘΕΩΡΗΜΑ-ΤΕΤΡΑΓΩΝΙΚΟΣ ΝΟΜΟΣ ΑΝΤΙΣΤΡΟΦΗΣ:

Έστω p,q περιττοί πρώτοι. Τότε:

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

b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

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

1.2 Πρώτη απόδειξη του Τετραγωνικού Νόμου Αντιστροφής

Ο ίδιος ο Gauss δημοσίευσε κατά τη διάρκεια της ζωής του 6 συνολικά αποδείξεις και 2 βρέθηκαν, μετά τον θάνατό του, στο αρχείο του. Η πιο συνηθισμένη απόδειξη που συνήθως αναφέρεται σε όλα σχεδόν τα βιβλία στοιχειώδους Θεωρίας Αριθμών, είναι αυτή που χρησιμοποίησε το Λήμμα του Gauss.

Λήμμα του Gauss: [[1] Πρόταση 5.2.9]

Έστω p περιττός πρώτος και a ακέραιος, $p \nmid a$.
Έστω S το ελάχιστο σύστημα των αντιπροσώπων των κλάσεων υπολοίπων modp των ακεραίων $a, 2a, ..., \frac{p-1}{2}a$.
Αν r το πλήθος των στοιχείων του S που είναι μεγαλύτερα από $\frac{p}{2}$ τότε $\left(\frac{a}{p}\right) = (-1)^r$.

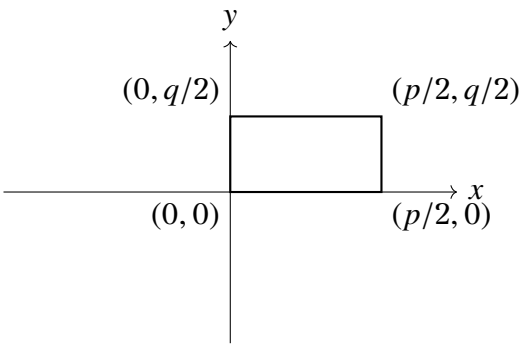
καθώς και η άμεση συνέπειά του:

Συνέπεια Λήμματος Gauss: [[1] Πρόταση 5.2.11]

Αν p περιττός πρώτος και a ακέραιος $p \nmid a$ τότε:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor}.$$

Πρώτη απόδειξη του Τετραγωνικού Νόμου Αντιστροφής:



Θεωρούμε το ορθογώνιο στο x-y καρτεσιανό επίπεδο, του οποίου οι κορυφές είναι τα σημεία $(0,0)$,(p/2,0), (0,q/2), (p/2,q/2).

Έστω R το εσωτερικό του ορθογωνίου χωρίς το σύνορό του. Το σχέδιό μας θα είναι να μετρήσουμε το πλήθος των ακεραίων σημείων που περιέχονται στο R με δύο διαφορετικούς τρόπους. Εφόσον οι p, q είναι και οι δύο περιττοί, τα ακέραια σημεία του R είναι τα σημεία με συντεταγμένες (n,m), όπου $1 \leq n \leq \frac{p-1}{2}$, $1 \leq m \leq \frac{q-1}{2}$. Είναι σαφές ότι το πλήθος αυτών των σημείων είναι $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

Η διαγώνιος δ που ενώνει τα (0,0), $(\frac{p}{2}, \frac{q}{2})$ έχει εξίσωση $y = \frac{q}{p} \cdot x$ ή ισοδύναμα $py = qx$.
Αφού $(p,q) = 1$, κανένα από τα ακέραια σημεία δεν ανήκει στην δ.

Έστω τώρα T1 το χωρίο εκείνο του R που είναι κάτω από την δ και T2 το χωρίο από πάνω. Θα μετρήσουμε τα ακέραια σημεία σε καθένα από τα δύο χωρία. Το πλήθος των ακεραίων στο διάστημα $0 < y < \frac{kq}{p}$ είναι ίσο με $\lfloor \frac{kq}{p} \rfloor$.
Επομένως, για κάθε k τέτοιο ώστε $1 \leq k \leq \frac{p-1}{2}$ υπάρχουν ακριβώς $\lfloor \frac{kq}{p} \rfloor$ ακέραια σημεία στο T1 ακριβώς πάνω από το σημείο $(k, 0)$ και κάτω από την δ, δηλαδή στο κατακόρυφο τμήμα που ενώνει το $(k, 0)$ με το $(k, \frac{kq}{p})$.
Επομένως, ο συνολικός αριθμός ακεραίων σημείων στο T1 είναι ίσος με $\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor$.

Ένας ανάλογος υπολογισμός με τον ρόλο των p,q να έχει εναλλαχθεί, δείχνει ότι ο συνολικός αριθμός ακεραίων σημείων στο T2 είναι ίσος με $\sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor$.

Ο συνολικός αριθμός ακεραίων σημείων στο R είναι ίσος με το άθροισμα του πλήθους των ακεραίων σημείων στο T1 και στο T2 και άρα:

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor.$$

Χρησιμοποιώντας την Συνέπεια του Λήμματος του Gauss έχουμε:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor} \cdot (-1)^{\sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor}$$

το οποίο λόγω της παραπάνω ισότητας ισούται με $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

Ειδικές περιπτώσεις Νόμου Αντιστροφής:

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

(2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Απόδειξη:
Για το πρώτο εφαρμόζουμε την Πρόταση 1.1.1 a) για $a = -1$.
Για το δεύτερο ξεκινάμε παίρνοντας την περίπτωση για $a = 2$ στο Λήμμα του Gauss.
Σύμφωνα με αυτό, θα πρέπει να υπολογίσουμε τους άρτιους ανάμεσα στο $\frac{p}{2}$ και το p.
Αρκεί να υπολογίσουμε το πλήθος των ακεραίων στο διάτημα $(\frac{p}{4}, \frac{p}{2})$.
Γράφουμε τον p στη μορφή $8k + l, l = 1, 3, 5$ ή 7.
Επομένως,θα πρέπει να ελέγξουμε αν το πλήθος των ακεραίων στο διάστημα $(2k + \frac{l}{4}, 4k + \frac{l}{2})$ είναι άρτιο ή περιττό.
Στο υποδιάστημα $(2k + \frac{l}{4}, 4k + \frac{l}{4})$ υπάρχει άρτιο πλήθος ακεραίων, επομένως αρκεί να υπολογίσουμε το πλήθος των ακεραίων στο
διάστημα $(4k + \frac{l}{4}, 4k + \frac{l}{2})$, ή αλλιώς στο διάστημα $(\frac{l}{4}, \frac{l}{2})$.

Αν $l = 1 \Rightarrow r = 0$, αν $l = 3 \Rightarrow r = 1$, αν $l = 5 \Rightarrow r = 1$ και αν $l = 7 \Rightarrow r = 2$.
Άρα, έχουμε δείξει ότι $\left(\frac{2}{p}\right) = 1$, όταν $p = \pm 1 \pmod 8$ και $\left(\frac{2}{p}\right) = -1$,όταν $p = \pm 3 \pmod 8$.
Αυτή η έκφραση και αυτή που θέλουμε να αποδείξουμε είναι ισοδύναμες, και άρα έχουμε το ζητούμενο.

Στην πορεία ακολούθησε σωρεία άλλων αποδείξεων από τον Eisenstein με χρήση της Πρότασης 3.13 [2], καθώς και από τον Dirichlet, τον Jacobi κτλ.
Το 1963 ο M.Gersterhaber δημοσίευσε εργασία με τίτλο "The 152nd proof of the Law of Quadratic Reciprocity" [Am. Math Month 70 (1963)] .Όταν ρωτήθηκε από τον F.Lemmermeyer πώς γνωρίζει ότι η απόδειξή του είναι η 152nαπάντησε:
"The origin of the title was not a list but a statement of André Weil in a seminar at the Institute for Advanced Study in Princeton: he said that he knew 50 proofs of the Law and that for each he had seen there were two he had not. So that made 150 proofs. Then he called my attention to Kubota's, which would have been 151st. So mine had to be the 152nd."

Σύμφωνα με [[2]-Appendix B σελ.413-417], μέχρι το 1963 οι αποδείξεις ήταν 149, δηλαδή ο André Weil έπεσε πολύ κοντά στην πρόβλεψή του.

Μέχρι σήμερα είναι γνωστές 332 αποδείξεις του νόμου τετραγωνικής αντιστροφής. Από

την Wikipedia [3] για το άρθρο του F.Lemmermeyger αναφέται ότι: "Chronology and biography of proofs of the Quadratic Reciprocity Laws: 332 proofs, last edited 30 August 2024 11:53(UTC)".

1.3 Πολλαπλασιαστικοί χαρακτήρες

Στη συνέχεια θα παρουσιάσουμε μία ακόμη απόδειξη. Για να πετύχει τον σκοπό του ο Gauss όρισε τα ομώνυμα αθροίσματα, τα οποία χρησιμοποίησε στην τέταρτη και στην έκτη απόδειξή του.
Πριν τα ορίσουμε απαραίτητη είναι η εισαγωγή της έννοιας του πολλαπλασιαστικού χαρακτήρα.

Ορισμός:

Ένας πολλαπλασιαστικός χαρακτήρας στο πεπερασμένο σώμα F_p με p στοιχεία είναι μία συνάρτηση χ από την πολλαπλασιαστική ομάδα F_p^* στους μη μηδενικούς μιγαδικούς αριθμούς που ικανοποιεί:

$$\chi(ab) = \chi(a) \cdot \chi(b) \quad \text{για κάθε} \quad a, b \in F_p^*.$$

Παρατηρήσεις:

-Το σύμβολο του Legendre $\left(\frac{a}{p}\right)$ είναι παράδειγμα τέτοιου χαρακτήρα αν θεωρηθεί συνάρτηση από το σύνολο των κλάσεων των a modp.
-Ένα άλλο παράδειγμα είναι ο τετριμμένος πολλαπλαστικός χαρακτήρας ορισμένος από τη σχέση $\varepsilon(a) = 1$ για κάθε $a \in F_p^*$.
-Είναι συχνά χρήσιμο να επεκτείνουμε το πεδίο ορισμού του πολλαπλασιαστικού χαρακτήρα σε όλο το F_p.
Αν $\chi \neq \varepsilon$, το κάνουμε αυτό ορίζοντας $\chi(0) = 0$. Για το ε ορίζουμε ε(0)=1.
Η χρησιμότητα αυτών των ορισμών θα φανεί κυρίως στη συνέχεια.

Πρόταση 1.3.1:

Έστω χ ένας πολλαπλασιαστικός χαρακτήρας και $a \in F_p^*$. Τότε ισχύουν:
a) $\chi(1) = 1$
b) $\chi(a)$ είναι μία (p-1)- ρίζα της μονάδας
c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Απόδειξη:
Για το *a*) $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$. Άρα $\chi(1) = 1$, αφού $\chi(1) \neq 0$.
Για το b) παρατηρούμε ότι από τη σχέση $a^{p-1} = 1$ έπεται ότι $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.
Για το c) παρατηρούμε ότι $1 = \chi(1) = \chi(a^{-1} \cdot a) = \chi(a^{-1}) \cdot \chi(a)$. Αυτό δείχνει ότι $\chi(a^{-1}) = \chi(a)^{-1}$.
Το γεγονός ότι $\chi(a)^{-1} = \overline{\chi(a)}$ έπεται από το ότι ο $\chi(a)$ είναι ένας μιγαδικός αριθμός απόλυτης τιμής 1 από το b).

Πρόταση 1.3.2:

Έστω χ πολλαπλασιαστικός χαρακτήρας. Αν $\chi \neq \varepsilon$, τότε $\sum_t \chi(t)=0$ όπου το άθροισμα είναι πάνω από όλα τα $t \in F_p$. Αν $\chi=\varepsilon$, η τιμή του αθροίσματος είναι p.

Απόδειξη:
Ο τελευταίος ισχυρισμός είναι προφανής, οπότε μπορούμε να υποθέσουμε εξ΄ αρχής ότι $\chi \neq \varepsilon$. Σε αυτήν την περίπτωση, υπάρχει ένα $a \in F_p^*$ τέτοιο ώστε $\chi(a) \neq 1$. Έστω $T= \sum_t \chi(t)$. Τότε έχουμε:

$$\chi(a) \cdot T = \sum_t \chi(a)\chi(t) = \sum_t \chi(at) = T.$$

Η τελευταία ισότητα προκύπτει γιατί το at διατρέχει όλα τα στοιχεία του F_p όπως κάνει και το t. Εφόσον $\chi(a) \cdot T = T$ και $\chi(a) \neq 1$ ακολουθεί ότι $T = 0$.

Ορισμός:

Έστω χ και λ χαρακτήρες της F_p^*. Το γινόμενο των χαρακτήρων χ και λ ορίζεται ως
$(\chi \cdot \lambda)(a) = \chi(a)\lambda(a)$, για κάθε $a \in F_p$.
Επιπλέον, αν χ χαρακτήρας, τότε χ^{-1} είναι η απεικόνιση που στέλνει το $a \in F_p^*$ στο $\chi(a)^{-1}$.

Παρατηρήσεις:

-Οι πολλαπλασιαστικοί χαρακτήρες φτιάχνουν μία ομάδα με βάση τους παραπάνω ορισμούς. Προφανώς οι $\chi \cdot \lambda$ και χ^{-1} είναι και αυτοί χαρακτήρες και από αυτούς τους πα-

ραπάνω ορισμούς καταλήγουμε ότι το σύνολο των χαρακτήρων φτιάχνουν μία ομάδα με ουδέτερο στοιχείο της ομάδας τον τετριμμένο χαρακτήρα ε.

Πρόταση 1.3.3:

Η ομάδα των χαρακτήρων είναι μια κυκλική ομάδα τάξης $p-1$. Αν $a \in F_p^*$ και $a \neq 1$, τότε υπάρχει χαρακτήρας χ τέτοιος ώστε $\chi(a) \neq 1$.

Απόδειξη:
Είναι γνωστό ότι η F_p^* είναι κυκλική ομάδα. Έστω $g \in F_p^*$ ένας γεννήτοράς της. Τότε, κάθε $a \in F_p^*$ ισούται με κάποια δύναμη του g. Αν $a = g^t$ και χ είναι ένας χαρακτήρας, τότε $\chi(\alpha) = \chi(g)^t$. Αυτό δείχνει ότι ο χ είναι πλήρως ορισμένος από την τιμή $\chi(g)$. Αφού το $\chi(g)$ είναι μία $(p-1)$-ρίζα της μονάδας, και αφού υπάρχουν ακριβώς $p-1$ από αυτές, έπεται ότι η ομάδα των χαρακτήρων έχει τάξη το πολύ $p-1$.

Τώρα ορίζουμε μία συνάρτηση λ από την εξίσωση $\lambda(g)^k = e^{\frac{2\pi ik}{p-1}}$ για κάθε $k = 0, 1, 2, ..., p-1$. Είναι εύκολο να ελέγξουμε ότι ο λ είναι καλά ορισμένος και είναι χαρακτήρας. Ισχυριζόμαστε ότι ο $p-1$ είναι ο μικρότερος ακέραιος η τέτοιος ώστε λ^n=ε.

Αν λ^n=ε, τότε $\lambda^n(g)$=ε$(g) = 1$. Ωστόσο $\lambda^n(g) = \lambda(g)^n = e^{\frac{2\pi in}{p-1}}$. Επομένως, το $p-1$ διαιρεί το η.

Αφού $\lambda^{p-1}(a) = \lambda(a)^{p-1} = \lambda(a^{p-1}) = \lambda(1) = 1$, έχουμε λ^{p-1} =ε.

Έχουμε εξασφαλίσει ότι τα ε,$\lambda, \lambda^2, ..., \lambda^{p-2}$ είναι όλα διαφορετικά.

Αφού, από την πρώτη απόδειξη, υπάρχουν το πολύ $p-1$ χαρακτήρες, έχουμε τώρα ότι υπάρχουν ακριβώς $p-1$ χαρακτήρες και ότι η ομάδα είναι κυκλική με το λ ως γεννήτορά της.
Αν $a \in F_p^*$ και $a \neq 1$, τότε $a = g^l$ με $(p-1) \nmid l$. Υπολογίζουμε το $\lambda(a)$ και έχουμε $\lambda(a) = \lambda(g)^l = e^{\frac{2\pi il}{p-1}} \neq 1$.
Αυτό ολοκληρώνει και την απόδειξη.

Πόρισμα 1.3.4:

Αν $a \in F_p^*$ και $a \neq 1$, τότε $\sum_\chi \chi(a)$=0, όπου η άθροιση γίνεται πάνω από όλους τους χαρακτήρες της ομάδας F_p^*.

Απόδειξη:
Έστω S=$\sum_\chi \chi(a)$. Αφού $a \neq 1$, υπάρχει από την Πρόταση 1.3.3 ένας χαρακτήρας λ τέτοιος ώστε $\lambda(a) \neq 1$. Τότε:

$$\lambda(a) \cdot S = \sum_\chi \lambda(a)\chi(a) = \sum_\chi (\lambda \cdot \chi)(a) = S.$$

Η τελευταία ισότητα ισχύει αφού το $\lambda \cdot \chi$ τρέχει πάνω από όλους τους χαρακτήρες με τον ίδιο τρόπο που το κάνει και το χ. Έπεται ότι $(\lambda(a) - 1) \cdot S = 0$ και άρα S=0.

1.4 Τετραγωνικά αθροίσματα Gauss

-Από εδώ και πέρα για αυτήν την παράγραφο, θα θεωρούμε ζ μία πρωταρχική p-ρίζα της μονάδας και συγκεκριμένα την $e^{\frac{2\pi i}{p}}$.

Λήμμα 1.4.1 :

$\sum_{t=0}^{p-1} \zeta^{at}$ είναι ίσο με p αν $a \equiv 0 \pmod p$. Αλλιώς είναι 0.

Απόδειξη:
Αν $a \equiv 0 \pmod p$, τότε $\zeta^a = 1$ και άρα $\sum_{t=0}^{p-1} \zeta^{at} = p$.

Αν $a \not\equiv 0 \pmod p$, τότε $\zeta^a \neq 1$ και $\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap}-1}{\zeta^a-1} = 0$.

Πόρισμα 1.4.2:

Ισχύει ότι, $p^{-1} \sum_{t=0}^{p-1} \zeta^{t\cdot(x-y)} = \delta(x,y)$ όπου $\delta(x,y) = 1$ αν $x \equiv y \pmod p$ και $\delta(x,y) = 0$ αν $x \not\equiv y \pmod p$.

-Από εδώ και πέρα θα παραλείπουμε για ευκολία τα όρια άθροισης εννοώντας πάντα ότι το άθροισμα τρέχει από 0 έως $p-1$.

Ορίζουμε τώρα τα αθροίσματα Gauss.

Ορισμός:

Έστω $a \in \mathbb{Z}$. Το άθροισμα $g_a = \sum_t \left(\frac{t}{p}\right) \zeta^{at}$ καλείται τετραγωνικό άθροισμα Gauss.

Πρόταση 1.4.3:

Έστω a ακέραιος. Τότε για το άθροισμα Gauss ισχύει $g_a = \left(\frac{a}{p}\right) g_1$.

Απόδειξη:
Αν $a \equiv 0 \pmod{p}$, τότε $\zeta^{at} = 1$ για κάθε t και $g_a = \sum_t \left(\frac{t}{p}\right) = 0$ από Παρατήρηση Πορίσματος 1.1.2. Αυτό μας δίνει το αποτέλεσμα στην περίπτωση που $a \equiv 0 \pmod{p}$.
Τώρα ας υποθέσουμε ότι $a \not\equiv 0 \pmod{p}$. Τότε:

$$\left(\frac{a}{p}\right) g_a = \sum_t \left(\frac{at}{p}\right) \zeta^{at} = \sum_x \left(\frac{x}{p}\right) \zeta^x = g_1.$$

Έχουμε χρησιμοποιήσει το γεγονός ότι το at διατρέχει σε ένα πλήρες σύστημα υπολοίπων modp όταν το ίδιο κάνει το t και ότι $\left(\frac{x}{p}\right)$ και ζ^x εξαρτάται μόνο από την κλάση υπολοίπου του x modulo p.
Αφού $\left(\frac{a}{p}\right)^2 = 1$ όταν $a \not\equiv 0 \pmod{p}$, το αποτέλεσμά μας έπεται πολλαπλασιάζοντας και τα δύο μέλη της εξίσωσης $\left(\frac{a}{p}\right) g_a = g_1$ με $\left(\frac{a}{p}\right)$.

-Από εδώ και πέρα θα γράφουμε για ευκολία το g_1=g. Έχουμε δηλαδή από την προηγούμενη πρόταση ότι αν $a \not\equiv 0 \pmod{p}$, τότε $g_a{}^2 = g^2$.

Πρόταση 1.4.4:

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

Απόδειξη:
Η ιδέα της απόδειξης είναι να υπολογίσουμε το άθροισμα $\sum_a g_a g_{-a}$ με δύο διαφορετικούς τρόπους.

Αν $a \not\equiv 0 \pmod{p}$ τότε $g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2$. Επομένως έχουμε ότι:

$$\sum_a g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1) g^2.$$

Τώρα παρατηρούμε ότι $g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{a(x-y)}$.

Αθροίζοντας και τα δύο μέλη πάνω από το α και χρησιμοποιώντας το Λήμμα 1.4.1, παίρνουμε:

$$\sum_a g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\delta(x,y)p = (p-1)\cdot p.$$

Τοποθετόντας όλα τα αποτελέσματα μαζί παίρνουμε $\left(\frac{-1}{p}\right)(p-1)g^2 = (p-1)\cdot p$. Άρα, $g^2 = \left(\frac{-1}{p}\right)p$.

-Στη συνέχεια με p^* θα συμβολίζουμε τον αριθμό $p^* = (-1)^{\frac{p-1}{2}}p$.

-Έστω p,q περιττοί πρώτοι με p ≠ q. Θα αποδείξουμε τον τετραγωνικό νόμο αντιστροφής δουλεύοντας με ισοτιμίες modq στο δακτύλιο των ακέραιων αλγεβρικών.

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

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

Χρησιμοποιώντας την γνωστή Πρόταση ότι αν $a_1, a_2 \in F_p$ όπου p πρώτος, τότε $(a_1 + a_2)^p \equiv a_1^p + a_2^p \pmod{p}$ έχουμε:

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

Άρα, έχουμε ότι $g^q \equiv g_q \equiv \left(\frac{q}{p}\right) g \pmod{q}$ και συνεπώς $\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{p}\right) g \pmod{q}$.

Πολλαπλασιάζοντας και τα δύο μέλη με g και χρησιμοποιώντας ότι $g^2 = p^*$, έχουμε:

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

άρα και $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$ (αφού $(p^*, q) = 1$) και τελικά $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$.

Αυτό είναι πράγματι το αποτέλεσμα που θέλουμε αφού:

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

Καταλήγουμε, τελικά, όντως στην εξίσωση του τετραγωνικού νόμου αντιστροφής!

2 Ο Διτετραγωνικός Νόμος Αντιστροφής

2.1 Εισαγωγή

Στο δεύτερο κεφάλαιο θα γενικεύσουμε τον τετραγωνικό νόμο αντιστροφής. Παρατηρούμε ότι το σύμβολο του Legendre παίρνει τιμές στο σύνολο $\{\pm 1\}$ (και φυσικά το σύμβολο του Kronecker παίρνει τιμές στο σύνολο $\{0, \pm 1\}$).
Το σύνολο $\{\pm 1\}$ είναι το σύνολο των μονάδων του δακτυλίου των ακεραίων $\mathbb{Z}$, οι οποίες μάλιστα είναι και ρίζες της μονάδας.
Για να είμαστε σε θέση να διατυπώσουμε και να αποδείξουμε τον Διτετραγωνικό Νόμο Αντιστροφής, θα πρέπει να μελετήσουμε κάποιον αντίστοιχο δακτύλιο. Αυτός θα είναι ο δακτύλιος του Gauss: $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$.
Ο δακτύλιος ορίστηκε πρώτη φορά από τον Gauss στην προσπάθειά του να αποδείξει τον Διτετραγωνικό Νόμο Αντιστροφής.
Εδώ το σύνολο των ριζών της μονάδας του δακτυλίου $\mathbb{Z}[i]$ είναι το σύνολο $\{\pm 1, \pm i\}$.
Για αντίστοιχο σύμβολο, επομένως, θα πρέπει να ισχύει $x^4 \equiv \alpha \pmod{p}$, για $\alpha \in \mathbb{Z}, p \in \mathbb{P}$ και $p \nmid \alpha \Leftrightarrow \left(\frac{\alpha}{p}\right)_4 = 1$.
Σχετικά με την ιστορία παραπέμπουμε στο [2] σελ. 199-202.
Όπως και στον τετραγωνικό νόμο αντιστροφής, η αριθμητική του $\mathbb{Z}$ παίζει σημαντικό ρόλο στην απόδειξη του, έτσι και στον διτετραγωνικό νόμο αντιστροφής σημαντική είναι η αριθμητική του δακτυλίου $\mathbb{Z}[i]$.
Τέλος, θα πρέπει να γενικεύσουμε την έννοια των αθροισμάτων του Gauss.

2.2 Αθροίσματα του Gauss και Αθροίσματα του Jacobi

Gauss Sums

Ορισμός:

Έστω χ ένας χαρακτήρας στο F_p και $a \in F_p$. Θέτουμε $g_a = \sum_t \chi(t)\zeta^{at}$, όπου η άθροιση είναι πάνω από όλα τα $t \in F_p$, και $\zeta = e^{2\pi i/p}$. Το g_a ονομάζεται Gauss Sum (Άθροισμα Gauss) στο F_p που αντιστοιχεί στον χαρακτήρα χ.

Πρόταση 2.2.1:

Αν $a \neq 0$ και $\chi \neq \varepsilon$, έχουμε $g_a(\chi) = \chi(a^{-1})g_1(\chi)$.
Αν $a \neq 0$ και $\chi = \varepsilon$, έχουμε ότι $g_a(\varepsilon) = 0$.
Αν $a = 0$ και $\chi \neq \varepsilon$, έχουμε $g_0(\chi) = 0$.
Αν $a = 0$ και $\chi = \varepsilon$, έχουμε] $g_0(\varepsilon) = p$.

Απόδειξη:
Υποθέτουμε ότι $a \neq 0$ και $\chi \neq \varepsilon$. Τότε:
$\chi(a)g_a(\chi) = \chi(a)\sum_t \chi(t)\zeta^{at} = \sum_t \chi(at)\zeta^{at} = g_1(\chi)$.
Όταν το t διατρέχει τα στοιχεία του F_p και $a \neq 0$, το ίδιο κάνει και το at. Αυτό εξηγεί την παραπάνω ισότητα και αποδεικνύει την πρώτη υπόθεση.
Αν $a \neq 0$, τότε $g_a(\varepsilon) = \sum_t \varepsilon(t)\zeta^{at} = \sum_t \zeta^{at} = 0$, με την τελευταία ισότητα να προκύπτει από το Λήμμα 1.4.1.
Για να ολοκληρώσουμε την απόδειξη ας παρατηρήσουμε ότι $g_0(\chi) = \sum_t \chi(t)\zeta^{0t} = \sum_t \chi(t)$.
Αν $\chi = \varepsilon$, το αποτέλεσμα είναι p, αν $\chi \neq \varepsilon$, το αποτέλεσμα είναι μηδέν από την Πρόταση 1.3.2.

-Θυμίζουμε ότι για ευκολία θέτουμε $g_1 = g$. Στη συνέχεια θα υπολογίσουμε την απόλυτη τιμή του $g(\chi)$.

Πρόταση 2.2.2:

Αν $\chi \neq \varepsilon$, τότε $|g(\chi)| = \sqrt{p}$.

Απόδειξη:
Η ιδέα είναι να υπολογίσουμε το άθροισμα $\sum_a g_a(\chi)\overline{g_a(\chi)}$ με δύο διαφορετικούς τρόπους.

Αν $a \neq 0$, τότε από Πρόταση 2.2.1, $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$ και $g_a(\chi) = \chi(a^{-1})g(\chi)$.
Άρα, $g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = |g(\chi)|^2$. Αφού $g_0(\chi) = 0$, το άθροισμά μας θα έχει την τιμή $(p-1)|g(\chi)|^2$.

Από την άλλη, $g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}$.
Αθροίζοντας και τα δύο μέλη ως προς a και χρησιμοποιώντας το Πόρισμα 1.4.2, έχουμε ότι:
$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p$.

Άρα, $(p-1)|g(\chi)|^2 = (p-1)p$ και, επομένως, έπεται το ζητούμενο.

Παρατηρήσεις:

Η σχέση του παραπάνω αποτελέσματος με την Πρόταση 1.4.4 γίνεται πιο ξεκάθαρη με τις παρακάτω παρατηρήσεις:
Είναι $\overline{g(\chi)} = \sum_t \overline{\chi(t)}\zeta^{-t} = \chi(-1)\sum_t \overline{\chi(-t)}\zeta^{-t} = \chi(-1)g(\overline{\chi})$.
Το $\overline{\chi}$ είναι ο χαρακτήρας που στέλνει το a στο $\overline{\chi(a)}$ και συμπίπτει με τον χαρακτήρα χ^{-1}.
Έχουμε χρησιμοποιήσει το γεγονός ότι $\overline{\chi(-1)} = \chi(-1)$ που είναι προφανές αφού $\chi(-1) = \pm 1$.
Άρα, το γεγονός ότι $|g(\chi)|^2 = p$ μπορεί να γραφεί ως $g(\chi)g(\overline{\chi}) = \chi(-1)p$. Αν ο χ είναι το σύμβολο του Legendre, τότε η σχέση που θα προκύψει θα είναι ακριβώς η Πρόταση 1.4.4.

Jacobi Sums:

-Ας θεωρήσουμε την εξίσωση $x^2 + y^2 = 1$ πάνω από το σώμα F_p. Αφού το F_p είναι πεπερασμένο, η εξίσωση έχει μόνο πεπερασμένο πλήθος λύσεων. Έστω $N(x^2 + y^2 = 1)$ να είναι αυτός ο αριθμός. Θα θέλαμε να υπολογίσουμε ακριβώς την τιμή του.
Παρατηρούμε ότι:

$N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a)N(y^2 = b)$, όπου το άθροισμα είναι πάνω από όλα τα ζευγάρια $a, b \in F_p$ τέτοια ώστε $a + b = 1$.

Αφού $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$, έχουμε ότι $N(x^2 + y^2 = 1) = p + \sum_a \left(\frac{a}{p}\right) + \sum_b \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Τα πρώτα δύο αθροίσματα είναι μηδέν, οπότε μας μένει να υπολογίσουμε το τελευταίο άθροισμα. Ισχύει ότι η τιμή του είναι $-(-1)^{(p-1)/2}$, κάτι που θα αποδειχθεί στη συνέχεια.
Δηλαδή, $N(x^2 + y^2 = 1)$ είναι $p - 1$ αν $p \equiv 1 \pmod 4$ και $p + 1$ αν $p \equiv 3 \pmod 4$.

-Στη συνέχεια, ας υπολογίσουμε να το $N(x^3 + y^3 = 1) = \sum_{a+b=1} N(x^3 = a)N(y^3 = b)$, $a, b \in F_p$.
Αν $p \equiv 2 \pmod 3$, τότε $N(x^3 = a) = 1$ για κάθε a αφού $(3, p-1) = 1$. ([5] Πρόταση 7.1.2 σελ. 80 αιτιολογεί το πλήθος των λύσεων)

Έπεται ότι $N(x^3 + y^3 = 1) = p$ σε αυτήν την περίπτωση.
Υποθέτουμε ότι $p \equiv 1 \pmod 3$. Έστω $\chi \neq \varepsilon$ ένας χαρακτήρας τάξης 3.
Τότε χ^2 είναι χαρακτήρας τάξης 3 και $\chi^2 \neq \varepsilon$. Επομένως, οι $\varepsilon, \chi, \chi^2$ είναι όλοι χαρακτήρες τάξης διαιρέτη του 3 και από δω και πέρα θα λέγονται κυβικοί χαρακτήρες.
Αντιστοίχως με πριν, θα έχουμε $N(x^3 = a) = 1 + \chi(a) + \chi^2(a)$.

Άρα, $N(x^3 + y^3 = 1) = \sum_{a+b=1} \sum_{i=0}^{2} \chi^i(a) \sum_{j=0}^{2} \chi^j(b) = \sum_i \sum_j (\sum_{a+b=1} \chi^i(a)\chi^j(b))$.

Το εσωτερικό άθροισμα είναι παρόμοιο με το άθροισμα που προέκυψε στην ανάλυση του

$N(x^2 + y^2 = 1)$.

Ορισμός:

Έστω χ και λ χαρακτήρες στον F_p. Ορίζουμε $J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$, $\alpha, b \in F_p$. Το $J(\chi, \lambda)$ ονομάζεται Jacobi Sum (Άθροισμα Jacobi).
-Για να ολοκληρώσουμε την ανάλυση των $N(x^2 + y^2 = 1)$, $N(x^3 + y^3 = 1)$ πρέπει να αποκτήσουμε πληροφορίες για την τιμή των Jacobi sums. Το ακόλουθο Θεώρημα μας παρέχει αυτήν την πληροφορία και επιπλέον δηλώνει μια σχέση μεταξύ των Gauss και Jacobi Sums.

Θεώρημα 2.2.3:

Έστω χ, λ μη-τετριμμένοι χαρακτήρες. Ισχύουν:
a) $J(\varepsilon,\varepsilon)=p$
b) $J(\chi,\varepsilon)=0$
c) $J(\chi,\chi^{-1}) = -\chi(-1)$
d) Αν $\chi \cdot \lambda \neq \varepsilon$, τότε $J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.

Απόδειξη:
Το *a*) είναι προφανές και το *b*) είναι άμεση συνέπεια της Πρότασης 1.3.2.
Για να αποδείξουμε το *c*) παρατηρούμε ότι για $a, b \in F_p$:

$$J(\chi,\chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{a+b=1, b\neq 0} \chi(\tfrac{a}{b}) = \sum_{a\neq 1} \chi(\tfrac{a}{1-a}).$$

Θέτουμε $a/(1-a) = c$. Αν $c \neq -1$, τότε $a = \frac{c}{1+c}$.

Έχουμε, λοιπόν, ότι όσο το a διατρέχει τις τιμές του F_p εκτός από την τιμή 1, το c διατρέχει τα στοιχεία του F_p εκτός από την τιμή -1. Έτσι:

$$J(\chi,\chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1).$$

Για να αποδείξουμε το d) παρατηρούμε ότι:
$g(\chi)g(\lambda) = (\sum_x \chi(x)\zeta^x) \cdot (\sum_y \lambda(y)\zeta^y) = \sum_{x,y} \chi(x)\lambda(y)\zeta^{x+y} = \sum_t (\sum_{x+y=t} \chi(x)\lambda(y))\zeta^t$ (1)

Αν $t = 0$ τότε $\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0$, αφού από υπόθεση ισχύει ότι $\chi \cdot \lambda \neq \varepsilon$.

Αν $t \neq 0$ ορίζουμε x' και y' μέσω των σχέσεων $x = tx'$ και $y = ty'$. Αν $x + y = t$, τότε $x' + y' = 1$. Επομένως, έπεται ότι:

$$\sum_{x+y=t}\chi(x)\lambda(y) = \sum_{x'+y'=1}\chi(tx')\lambda(ty') = (\chi\cdot\lambda)(t)J(\chi,\lambda).$$

Αντικαθιστώντας στην εξίσωση (1) παίρνουμε $g(\chi)g(\lambda) = \sum_t(\chi\cdot\lambda)(t)J(\chi,\lambda)\zeta^t = J(\chi,\lambda)g(\chi\lambda)$, άρα έχουμε το ζητούμενο.

-Γυρνώντας πίσω στην εκκρεμότητα που είχαμε αφήσει για τον υπολογισμό του $\sum_{a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, σύμφωνα με το c) του Θεωρήματος 2.2.3, εφόσον το σύμβολο του Legendre είναι χαρακτήρας τάξης 2, θα έχουμε $J(\chi,\chi) = \sum_{a+b=1}\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -\chi(-1) = -\left(\frac{-1}{p}\right) = -(-1)^{\frac{p-1}{2}}$ και έτσι προκύπτει το αποτέλεσμα που θέλαμε να δείξουμε.

Πόρισμα 2.2.4:

Αν χ, λ και $\chi\cdot\lambda$ δεν είναι ίσα με ε, τότε $|J(\chi,\lambda)| = \sqrt{p}$.

Απόδειξη:
Προκύπτει άμεσα παίρνοντας απόλυτη τιμή στο d) της παραπάνω Πρότασης και χρησιμοποιώντας την Πρόταση 2.2.2.

Πρόταση 2.2.5:

Αν $p \equiv 1 \pmod 3$, τότε υπάρχουν ακέραιοι a, b τέτοιοι ώστε $a^2 - ab + b^2 = p$.

Απόδειξη:
Αν $p \equiv 1 \pmod 3$, τότε υπάρχει χαρακτήρας τάξης 3 (αν λ έχει τάξη $p-1$ θέτουμε $\chi = \lambda^{(p-1)/3}$).
Οι τιμές του χ ανήκουν στο σύνολο $\{1, \omega, \omega^2\}$, όπου $\omega = e^{2\pi i/3} = (-1+\sqrt{-3})/2$.
Άρα, $J(\chi,\chi) \in \mathbb{Z}[\omega]$. Επομένως, έχουμε $J(\chi,\chi) = a + b\omega$, με $a, b \in \mathbb{Z}$ και

$$p = |J(\chi,\chi)|^2 = |a+b\omega|^2 = a^2 - ab + b^2.$$

-Για $p \equiv 1 \pmod 3$, η αναπαράσταση $p = a^2 - ab + b^2$ δεν είναι μοναδική ακόμα και αν υποθέσουμε ότι $a, b > 0$. Αυτό φαίνεται και από τις ισότητες :
$a^2 - ab + b^2 = (b-a)^2 - (b-a)b + b^2 = a^2 - a(a-b) + (a-b)^2$.

-Ωστόσο, μπορούμε να τροποποιήσουμε το αποτέλεσμα ώστε να πάρουμε μοναδικό αποτέλεσμα. Αν $p = a^2 - ab + b^2$, τότε $4p = (2a-b)^2 + 3b^2 = (2b-a)^2 + 3a^2 = (a+b)^2 + 3(a-b)^2$.

Ισχυριζόμαστε ότι το 3 διαιρεί είτε το a είτε το b ή το $a-b$. Υποθέτουμε ότι $3 \nmid a$ και $3 \nmid b$.
Τότε έχουμε 4 περιπτώσεις : είτε $a, b \equiv 1 \pmod 3$ είτε $a, b \equiv 2 \pmod 3$
είτε ($a \equiv 1 \pmod 3, b \equiv 2 \pmod 3$) ή ($a \equiv 2 \pmod 3, b \equiv 1 \pmod 3$).

Στις δύο πρώτες περιπτώσεις προκύπτει άμεσα ότι $3 \mid (a-b)$. Τώρα, στις δύο τελευταίες περιπτώσεις: $a^2 - ab + b^2 = p \equiv 0 \pmod 3$ και άρα έχουμε ότι $3 \mid p$, πράγμα άτοπο. Σαν συμπέρασμα έχουμε, λοιπόν, ότι $3 \mid (a-b)$ σε όλες τις περιπτώσεις.

Λόγω της παραπάνω παρατήρησης προκύπτει η παρακάτω Πρόταση.

Πρόταση 2.2.6:

Αν $p \equiv 1 \pmod 3$, τότε υπάρχουν ακέραιοι A και B, τέτοιοι ώστε $4p = A^2 + 27B^2$. Σε αυτήν την αναπαράσταση, τα $4p, A, B$ είναι μοναδικά ορισμένα αν δεν λάβουμε υπόψιν τα πρόσημά τους.

Απόδειξη:
Έχουμε ήδη δείξει ότι αν $p \equiv 1 \pmod 3$, τότε υπάρχουν ακέραιοι $A, B \in \mathbb{Z}$ τέτοιοι ώστε $4p = A^2 + 27B^2$. Τώρα, αν υποθέσουμε ότι $A \equiv 1 \pmod 3$, μπορούμε να δείξουμε ότι το A είναι μοναδικά καθορισμένο μέχρι προσήμου. Άρα, το ίδιο θα ισχύει και για το B.
Ξεκινάμε την απόδειξη υποθέτοντας ότι κάτι τέτοιο δεν ισχύει και ότι $4p = A^2 + 27B^2 =$
$= C^2 + 27D^2$, όπου $A \equiv C \equiv 1 \pmod 3$.

Θα δείξουμε, τελικά, ότι $A = C$.

Έστω $\omega = e^{\frac{2\pi i}{3}} = \frac{-1}{2} + \frac{i\sqrt{3}}{2}$. Τότε, $i\sqrt{3} = 2\omega + 1$.
Για τυχαία x, y θα ισχύει: $x^2 + 3y^2 = (x + i\sqrt{3}y) \cdot (x - i\sqrt{3}y) = (x + (2\omega+1)y) \cdot (x - (2\omega+1)y) =$
$= (x + y + 2\omega y) \cdot (x - y - 2\omega y)$.

Αν θέσουμε $x = A,\ y = 3B$ παίρνουμε: $4p = A^2 + 27B^2 = (A + 3B + 6\omega B) \cdot (A - 3B - 6\omega B)$.
Παρατηρούμε ότι οι A, B ή θα είναι και οι δύο άρτιοι ή και οι δύο περιττοί, δηλαδή
$A \equiv B \pmod 2$.
Έτσι, μπορούμε να γράψουμε: $p = (\frac{A+3B}{2} + 3\omega B) \cdot (\frac{A-3B}{2} - 3\omega B)$, αφού τα $A+3B,\ A-3B$ είναι πάντα άρτια.
Παρατηρούμε ότι $p = \pi\overline{\pi}$, όπου $\pi = \frac{A+3B}{2} + 3\omega B \in \mathbb{Z}[\omega]$.
Το π είναι πρώτος στον $\mathbb{Z}[\omega]$, διότι αν δεν ήταν θα μπορούσε να γραφεί στην μορφή: $\pi = u \cdot v,\ u,\ v \in \mathbb{Z}[\omega]$.
Αλλά, $N(\pi) = p = N(u) \cdot N(v)$. Αναγκαστικά, πρέπει $N(u) = 1$ ή $N(v) = 1$, άρα, πρέπει ή το u ή το v να είναι μονάδα του δακτυλίου. Επομένως, το π καταλήγει να είναι ανάγωγο στον $\mathbb{Z}[\omega]$ και κατά συνέπεια και πρώτος.

Τελικά, έχουμε, $\pi\overline{\pi} = (\frac{A+3B}{2} + 3\omega B) \cdot (\frac{A-3B}{2} - 3\omega B) = (\frac{C+3D}{2} + 3\omega D) \cdot (\frac{C-3D}{2} - 3\omega D)$.

Αφού το π είναι πρώτος, θα διαιρεί το $\frac{C+3D}{2} + 3\omega D$ ή τον συζυγή του.

Αφού, όμως, τα στοιχεία αυτά έχουν την ίδια Norm p, πρέπει να είναι συνεταιρικά.
Οι μονάδες του $\mathbb{Z}[\omega]$ είναι οι: $\pm 1, \pm\omega, \pm\omega^2$.
Αρά, υπάρχουν 12 πιθανές περιπτώσεις, οι οποίες, τελικά, ανάγονται σε 6 αντικαθιστώντας το D με $-D$ όπου χρειάζεται.
Όλες οι περιπτώσεις πλην της ισότητας θα καταλήξουν σε άτοπο, διότι δεν θα επαληθεύεται η σχέση $A \equiv C \equiv 1 \pmod 3$. Θα πάρουμε, τελικά ότι $A = C$ και, έτσι, καταλήγουμε στο ζητούμενο.

-Ας δούμε τώρα άλλη μία συσχέτιση των Gauss Sums και των Jacobi Sums.

Πρόταση 2.2.7:

Υποθέτουμε ότι $p \equiv 1 \pmod n$ και ότι χ είναι ένας χαρακτήρας τάξης $n > 2$. Τότε :
$g(\chi)^n = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)...J(\chi,\chi^{n-2})$.

Απόδειξη:
Χρησιμοποιώντας το d) του Θεωρήματος 2.2.3, έχουμε $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$. Πολλαπλασιάζουμε και τα δύο μέλη με $g(\chi)$ και παίρνουμε $g(\chi)^3 = J(\chi,\chi)J(\chi,\chi^2)g(\chi^3)$. Συνεχίζοντας κατ΄ αυτόν τον τρόπο δείχνουμε ότι:

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

Τώρα $\chi^{n-1} = \chi^{-1} = \overline{\chi}$. Άρα, όπως έχουμε δει $g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)p$ (Παρατήρηση Πρότασης 2.2.2). Το αποτέλεσμα έπεται αν πολλαπλασιάσουμε και τα δύο μέλη της (*) με $g(\chi)$.

Πόρισμα 2.2.8:

Αν χ είναι ένας κυβικός χαρακτήρας, τότε $g(\chi)^3 = pJ(\chi,\chi)$.

Απόδειξη:
Πρόκειται για μια ειδική περίπτωση της παραπάνω πρότασης για $n = 3$ παρατηρώντας απλά ότι $\chi(-1) = \chi((-1))^3 = 1$.

-Χρησιμοποιώντας αυτό το Πόρισμα είμαστε σε θέση να αναλύσουμε περαιτέρω τον μιγαδικό αριθμό $J(\chi,\chi)$ που προέκυψε στην ανάλυση του $N(x^3 + y^3 = 1)$. Έχουμε δει ότι $J(\chi,\chi) = a + b\omega$, όπου $a, b \in \mathbb{Z}$ και $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2$.

Πρόταση 2.2.9:

Υποθέτουμε ότι $p \equiv 1 \pmod 3$ και ότι χ είναι ένας κυβικός χαρακτήρας.
Θέτουμε $J(\chi,\chi) = a + b\omega$ όπως πριν. Τότε:
a) $b \equiv 0 \pmod 3$
b) $a \equiv -1 \pmod 3$

Απόδειξη:
Έχουμε ότι $g(\chi)^3 = (\sum_t \chi(t)\zeta^t)^3 \equiv \sum_t \chi(t)^3\zeta^{3t} \pmod 3$.
Αφού $\chi(0) = 0$ και $\chi(t)^3 = 1$, για $t \neq 0$ έχουμε $\sum_t \chi(t)^3\zeta^{3t} = \sum_{t\neq 0} \zeta^{3t} = -1$.
Άρα, $g(\chi)^3 = pJ(\chi,\chi) \equiv a + b\omega \equiv -1 \pmod 3$.

Δουλεύοντας με το $\overline{\chi}$ αντί για το χ και ενθυμούμενοι ότι $\overline{g(\chi)} = g(\overline{\chi})$ βρίσκουμε ότι
$g(\overline{\chi})^3 = pJ(\overline{\chi},\overline{\chi}) = a + b\overline{\omega} \equiv -1 \pmod 3$.
Αφαιρώντας τις δύο σχέσεις προκύπτει $b(\omega - \overline{\omega}) \equiv 0 \pmod 3$ ή $b\sqrt{-3} \equiv 0 \pmod 3$.
Έτσι, $-3b^2 \equiv 0 \pmod 9$ και έπεται ότι $3 \mid b$ και $a + b\omega \equiv -1 \pmod 3$. Πρέπει να έχουμε $a \equiv -1 \pmod 3$ και αυτό ολοκληρώνει την απόδειξη.

Πόρισμα 2.2.10:

Έστω $A = 2a - b$ και $B = b/3$. Τότε $A \equiv 1 \pmod 3$ και $4p = A^2 + 27B^2$.

Απόδειξη:
Αφού $J(\chi,\chi) = a + b\omega$ και $|J(\chi,\chi)|^2 = p$, έχουμε $p = a^2 - ab + b^2$. Τότε, $4p = (2a - b)^2 + 3b^2$ και άρα είναι της μορφής $4p = A^2 + 27B^2$. Από την Πρόταση 2.2.9, έχουμε ότι $3 \mid b$ και $a \equiv -1 \pmod 3$. Άρα, $A = 2a - b \equiv 1 \pmod 3$.

2.3 Primary στοιχεία στο $\mathbb{Z}[i]$

Στη συνέχεια θα μελετήσουμε την αριθμητική του δακτυλίου $\mathbb{Z}[i]$. Προκειμένου να μην επαναλάβουμε την ίδια διαδικασία για τα συνεταιρικά στοιχεία θα ορίσουμε μια καινούρια έννοια μέσω της οποίας από τα τέσσερα συνεταιρικά μεταξύ τους στοιχεία να μπορούμε κάθε φορά να επιλέγουμε ακριβώς ένα. Τα στοιχεία αυτά λέγονται primary και στην περίπτωση του $\mathbb{Z}[i]$ ορίζονται ως εξής:

Ορισμός:

Ένα στοιχείο α που δεν είναι μονάδα στο $\mathbb{Z}$[i] θα λέγεται primary αν $\alpha \equiv 1 \pmod{(1+i)^3}$.

Λήμμα 2.3.1:

Ένα στοιχείο α που δεν είναι μονάδα είναι primary αν και μόνο αν είτε
$(a \equiv 1 \pmod 4, b \equiv 0 \pmod 4)$ ή $(a \equiv 3 \pmod 4, b \equiv 2 \pmod 4)$, όπου $\alpha = a + bi$.

Απόδειξη:
Αφού $(1+i)^3 = 2i - 2$ έπεται ότι $a + bi$ είναι primary αν και μόνο αν:

$$\frac{(a-1)+bi}{2i-2} = \frac{-a+1+b}{4} + \frac{-a-b+1}{4} \cdot i \in \mathbb{Z}[i].$$

Αυτό είναι ισοδύναμο με τις ισοτιμίες: $a + b \equiv 1 \pmod 4$ και $a - b \equiv 1 \pmod 4$.
Το αποτέλεσμα έπεται εύκολα από αυτό το συμπέρασμα.

-Παρατηρούμε ότι για κάθε στοιχείο α του $\mathbb{Z}[i]$ που δεν είναι μονάδα και είναι $\alpha \equiv 1 \pmod 4$, ισχύει ότι $a + bi \equiv 1 \pmod 4 \Rightarrow a + bi = 1 + 4k | k \in \mathbb{Z} \Rightarrow \frac{a-1}{4} + \frac{b}{4} \cdot i \in \mathbb{Z}[i] \Rightarrow \frac{a-1}{4} \in \mathbb{Z}, \ \frac{b}{4} \in \mathbb{Z}$ και άρα είναι primary.

-Επιπλέον, αν α είναι primary, τότε $(1+i) \nmid \alpha$. Αυτό γιατί αν $(1+i) \mid \alpha = a + bi$, τότε θα υπήρχε ένα $x + iy \in \mathbb{Z}[i]$ τέτοιο ώστε $(a + bi) = (1+i) \cdot (x + iy)$. Από αντιστοιχία, στο τέλος θα είχαμε $a = x - y, \ b = x + y$ και άρα $a + b = 2x$, πράγμα άτοπο γιατί από το Λήμμα 6.1 και στις δυο περιπτώσεις του primary έχω ότι $a + b \equiv 1 \pmod 4$.
-Αν q πραγματικός πρώτος με $q \equiv 3 \pmod 4$, τότε $-q$ είναι primary ανάγωγο
(έχουμε $-q \equiv 1 \pmod 4$ που όπως είδαμε τα στοιχεία αυτά είναι primary).

-Όσον αφορά τα ανάγωγα που προκύπτουν από πρώτους $p \equiv 1 \pmod 4$ έχουμε το ακόλουθο σημαντικό αποτέλεσμα:

Λήμμα 2.3.2:

Έστω $\alpha \in \mathbb{Z}[i]$ όχι μονάδα με $(1+i) \nmid \alpha$. Τότε υπάρχει μοναδική μονάδα u του $\mathbb{Z}[i]$ τέτοια ώστε $u\alpha$ να είναι primary.

Απόδεξη:
Υπάρχει πάντα μία μονάδα ε τέτοια ώστε $\varepsilon\alpha = a + bi$, όπου a είναι περιττός και b είναι άρτιος. Έχουμε ότι στις περιπτώσεις όπου τα a, b είναι και τα δύο άρτια ή και τα δύο πε-

ριττά προκύπτει ότι $(1+i) \mid \alpha$, πράγμα άτοπο, ενώ στην περίπτωση όπου το a είναι άρτιος και το b περιττός, πολλαπλασιάζοντας με κατάλληλη μονάδα μπορούμε να αναχθούμε στην αρχική υπόθεση ότι a είναι περιττός και b άρτιος. Πολλαπλασιάζοντας αν χρειάζεται με -1 παίρνουμε την επιθυμητή μορφή του Λήμματος 2.3.1 και προκύπτει ότι ο α έχει συνεταιρικό primary στοιχείο. Στην ουσία οι περιπτώσεις που θα χρειαστεί αυτός ο πολλαπλασιασμός είναι για ($a \equiv 1 \pmod 4, b \equiv 2 \pmod 4$) και ($a \equiv 3 \pmod 4, b \equiv 0 \pmod 4$).

Τώρα για την μοναδικότητα, αν u_1 και u_2 είναι μονάδες τέτοιες ώστε $u_1\alpha$ και $u_2\alpha$ είναι primary, τότε αφού $(1+i) \nmid \alpha$, έπεται ότι $u_1 \equiv u_2 \pmod{(1+i)^3}$.
Εξετάζοντας όλα τα δυνατά τέτοια ζευγάρια των u_1, u_2 δηλαδή όλα τα δυνατά ζευγάρια των μονάδων στο $\mathbb{Z}[i]$ που είναι οι: $\pm 1, \pm i$, καταλήγουμε τελικά ότι $u_1 = u_2$. Άρα, έχουμε τελικά και την μοναδικότητα.

Για τα τελευταία δύο αποτελέσματα ας θυμίσουμε τον Νόμο Ανάλυσης στο $\mathbb{Z}[i]$:
Ο δακτύλιος $\mathbb{Z}[i]$ είναι Περιοχή Μονοσήμαντης Ανάλυσης, άρα οι έννοιες πρώτο και ανάγωγο συμπίπτουν.
Έστω p ένας πρώτος αριθμός (ή ανάγωγος). Η ανάλυση του p στην περιοχή του Gauss είναι:
* Αν $p = 2$ τότε $p = -i\pi^2$ όπου π πρώτος του $\mathbb{Z}[i]$ και $N(\pi) = 2$.
* Αν $p \equiv 3 \pmod 4$ τότε $p = \pi$ είναι πρώτος και $N(\pi) = p^2$.
* Αν $p \equiv 1 \pmod 4$ τότε $p = \pi\pi'$ όπου π και π' μη συνεταιρικοί και $N(\pi) = N(\pi') = p$.

Από εδώ και πέρα ο Νόμος Ανάλυσης θα χρησιμοποιείται χωρίς να γίνεται ιδιαίτερη αναφορά του, πράγμα που αποδεικνύει και πόσο σημαντικός είναι!

Λήμμα 2.3.3:

Ένα primary στοιχείο μπορεί να γραφεί σαν το γινόμενο primary αναγώγων.

Απόδειξη:
Έστω $\alpha \in \mathbb{Z}[i]$ primary. Τότε, από Νόμο Ανάλυσης σε συνδυασμό με το προηγούμενο Λήμμα, έχουμε ότι υπάρχουν πραγματικοί πρώτοι $q_i \equiv 3 \pmod 4$ και primary ανάγωγα π_i, $N(\pi_i) \equiv 1 \pmod 4$ και επιπλέον ίσως μία μονάδα u, ώστε $\alpha = u\pi_1 ... \pi_t(-q_1)...(-q_s)$.
Αυτό ισχύει γιατί τα $(-q_i)$ είναι ήδη primary εφόσον είναι ισότιμα με 1 mod4 και από το προηγούμενο Λήμμα που ισχύει για $p_i \equiv 1 \pmod 4$, δηλαδή, με $N(\pi_i) \equiv 1 \pmod 4$, έχουμε ότι υπάρχουν κατάλληλες μονάδες u_i για το καθένα έτσι ώστε $u_i\pi_i'$ να είναι primary. Αυτό ορίζουμε να είναι το π_i. Τώρα, αν πάρουμε τη σχέση $mod(1+i)^3$, εφόσον πλέον όλα τα $-q_j$, p_i είναι primary και άρα ισότιμα με 1 $mod(1+i)^3$, θα πάρουμε ότι $u \equiv 1 \pmod{(1+i)^3}$.
Από την προηγούμενη διαδικασία με τις μονάδες που κάναμε στο προηγούμενο Λήμμα κα-

ταλήγουμε ότι $u = 1$. Άρα, έπεται το ζητούμενο.

2.4 Το Τετραδικό Σύμβολο Υπολοίπων

Θεωρούμε ένα ανάγωγο π στον $\mathbb{Z}[i]$. Αυτό θα είναι και πρώτο εφόσον $\mathbb{Z}[i]$ είναι Περιοχή Μονοσήμαντης Ανάλυσης.

Πρόταση 2.4.1:

Ο δακτύλιος κλάσεων υπολοίπου $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ είναι ένα πεπερασμένο σώμα με $N(\pi)$ στοιχεία.

Απόδειξη:
Γενικά ισχύει ότι αν π πρώτο του $\mathbb{Z}[i]$, όπου $\mathbb{Z}[i]$ Περιοχή Μονοσήμαντης Ανάλυσης, τότε $< \pi >= \pi\mathbb{Z}[i]$ είναι πρώτο και άρα είναι και μεγιστικό. Αυτό, γιατί σε περιοχή κυρίων ιδεωδών, κάθε μη μηδενικό πρώτο ιδεώδες του $\mathbb{Z}[i]$ είναι και μεγιστικό. Άρα, $\mathbb{Z}[i]/ < \pi >$ είναι σώμα με πλήθος στοιχείων $N(\pi)$ (δεν χρειάζεται απόλυτη τιμή για το συγκεκριμένο πλήθος, γιατί βρισκόμαστε στο $\mathbb{Z}[i]$ και η Norm είναι πάντα ≥ 0).

Πόρισμα 2.4.2:

Αν $\pi \nmid \alpha$, τότε $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Απόδειξη:
Έχουμε ότι η αντίστοιχη πολλαπλασιαστική ομάδα $(R/ < \pi >)^*$ (όπου R έχω ορίσει το $\mathbb{Z}[i]$) έχει $N(\pi) - 1$ στοιχεία. Γνωρίζουμε ότι αν έχουμε ομάδα τάξης m, τότε για κάθε $g \in G$ ισχύει $g^m = 1$. Κι εδώ, λοιπόν, για κάθε μη μηδενικό στοιχείο της πολλαπλασιαστικής ομάδας, δηλαδή για κάθε $\alpha + < \pi > \neq 0 + < \pi > \Leftrightarrow \alpha \notin < \pi > \Leftrightarrow \pi \nmid \alpha$, έχουμε ότι:
$(\alpha + < \pi >)^{N(\pi)-1} \equiv 1 \pmod{\pi} \Rightarrow \alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Πρόταση 2.4.3:

Αν $\pi \nmid \alpha$, $< \pi > \neq < 1+i >$, υπάρχει ένας μοναδικός ακέραιος j, $0 \leq j \leq 3$ τέτοιος ώστε:

$$\alpha^{(N(\pi)-1)/4} \equiv i^j \pmod{\pi}.$$

Απόδειξη:
Είναι εύκολο να δούμε ότι τα $1, -1, i, -i$ ανήκουν σε διαφορετικές κλάσεις $mod\pi$ τσεκάροντας ότι τα διάφορα ζεύγη των μονάδων δεν είναι μεταξύ τους ισότιμα $mod\pi$. Οι μονάδες είναι ρίζες του $x^4 \equiv 1 \pmod{\pi}$ και εφόσον η ισοτιμία κανονικά έχει το πολύ 4 λύσεις και τις βρήκαμε, θα έχει ακριβώς αυτές τις 4 λύσεις. Ωστόσο, η κλάση υπολοίπων του $\alpha^{(N(\pi)-1)/4}$ είναι επίσης λύση αυτής της ισοτιμίας σύμφωνα με το παραπάνω Πόρισμα. Άρα, αναγκαστικά το $\alpha^{(N(\pi)-1)/4}$ ταυτίζεται με μία από τις παραπάνω ρίζες, που αλλιώς μπορούμε να τις γράψουμε υπό την μορφή $i^j, 0 \leq j \leq 3$.

Ορισμός:

Αν το π είναι ανάγωγο, με $N(\pi) \neq 2$, τότε ο διτετραγωνικός χαρακτήρας υπολοίπων του α για $\pi \nmid \alpha$ ορίζεται να είναι: $\chi_\pi(\alpha) = i^j$, όπου j ορίζεται όπως στην Πρόταση 2.4.3.
Αν $\pi|\alpha$, τότε $\chi_\pi(\alpha) = 0$.

Πρόταση 2.4.4:

a) Αν $\pi \nmid \alpha$, τότε $\chi_\pi(\alpha) = 1 \Leftrightarrow x^4 \equiv \alpha \pmod{\pi}$ έχει λύση στον $\mathbb{Z}[i]$
b) $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$
c) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$
d) Αν π είναι primary ανάγωγο, τότε $\chi_\pi(-1) = (-1)^{(a-1)/2}$, όπου $\pi = a + bi$
e) Αν $\alpha \equiv \beta \pmod{\pi}$ τότε $\chi_\pi(\alpha) = \chi_\pi(\beta)$
f) $\chi_\pi(\alpha) = \chi_\lambda(\alpha)$ αν $< \pi > = < \lambda >$.

Απόδειξη:
Για το d) παρατηρούμε ότι τα $\frac{a^2+b^2-1}{4}$ και $\frac{a-1}{2}$ είναι ισότιμα mod 2 για τα γνωστά ζεύγη
($a \equiv 0 \pmod{4}, b \equiv 1 \pmod{4}$) και ($a \equiv 3 \pmod{4}, b \equiv 2 \pmod{4}$) των primary στοιχείων.

Πρόταση 2.4.5:

Έστω q πρώτος, $q \equiv 3 \pmod{4}$. Τότε, $\chi_q(a) = 1$ για $a \in \mathbb{Z}, q \nmid a$.

Απόδειξη:
Ισχύει $N(q) = q^2$ από τον Νόμο Ανάλυσης. Τότε, $\chi_q(a) \equiv a^{(q^2-1)/4} = (a^{q-1})^{(q+1)/4} \equiv 1 \pmod{q}$, αφού $a^{q-1} \equiv 1 \pmod{q}$ σύμφωνα με το μικρό Θεώρημα του Fermat.

Ορισμός:

Έστω $\alpha \in \mathbb{Z}[i]$ όχι μονάδα τέτοιο ώστε $(1+i) \nmid \alpha$ και $\beta \in \mathbb{Z}[i]$. Γράφουμε το α ως $\alpha = \prod_i \lambda_i$, όπου λ_i ανάγωγα. Αν $(\alpha, \beta) = 1$ ορίζουμε το $\chi_a(\beta)$ ως $\chi_a(\beta) = \prod_i \chi_{\lambda_i}(\beta)$.
Αυτό είναι καλά ορισμένο από το f) της Πρότασης 2.4.4. Από το e) της ίδιας Πρότασης προκύπτει ότι αν $\beta \equiv \gamma \pmod{\alpha}$, τότε $\chi_\alpha(\beta) = \chi_\alpha(\gamma)$.

Πρόταση 2.4.6:

Έστω $a \in \mathbb{Z}$, $a \neq 0$ και $b \in \mathbb{Z}$ ένας περιττός όχι μονάδα. Αν $(b, a) = 1$, τότε $\chi_b(a) = 1$.

Απόδειξη:
Μπορούμε να υποθέσουμε ότι $b > 0$. Γράφουμε $b = \prod p_i \prod q_i$ όπου p_i, q_i είναι πρώτοι, $p_i \equiv 1 \pmod{4}$, $q_i \equiv 3 \pmod{4}$, εφόσον υποθέσαμε ότι ο b είναι περιττός.
Από την Πρόταση 2.4.5, αρκεί μόνο να δείξουμε ότι $\chi_{p_i}(a) = 1$. Αν $p_i = \pi\overline{\pi}$, όπου π είναι ανάγωγο, τότε: $\chi_{p_i}(a) = \chi_\pi(a)\chi_{\overline{\pi}}(a) = \chi_\pi(a)\overline{\chi_\pi(a)} = 1$, όπου η προτελευταία ισότητα ισχύει λόγω του c) της Πρότασης 2.4.4 και η τελευταία ισότητα λόγω των τιμών που παίρνει ο χαρακτήρας. Άρα, το συμπέρασμά μας αποδείχτηκε.

Πρόταση 2.4.7:

Αν $n \neq 1$ ένας ακέραιος με $n \equiv 1 \pmod{4}$, τότε $\chi_n(i) = (-1)^{(n-1)/4}$.

Απόδειξη:
Παρατηρούμε ότι ο n μπορεί να είναι και αρνητικός.
Αν το n είναι θετικός πρώτος $p \equiv 1 \pmod{4}$ τότε, γράφοντας $p = \pi\overline{\pi}$, αφού $N(\pi) = N(\overline{\pi}) = p$, παίρνουμε το εξής:

$$\chi_p(i) = \chi_\pi(i)\chi_{\overline{\pi}}(i) = (i^{(p-1)/4})^2 = (-1)^{(p-1)/4}.$$

Από την άλλη, αν $n = -q$, $q \equiv 3 \pmod{4}$ και πρώτος, τότε $\chi_{-q}(i) = i^{(q^2-1)/4} = (i^{q-1})^{(q+1)/4} =$
$= (-1)^{(q+1)/4} = (-1)^{(-q-1)/4}$. Άρα, ισχύει και για αυτήν την περίπτωση.

Αν $n \equiv 1 \pmod{4}$ τυχαίο, τότε μπορούμε να το γράψουμε στη μορφή $n = p_1 \ldots p_t(-q_1)\ldots(-q_s)$, $p_i \equiv 1 \pmod{4}, q_i \equiv 3 \pmod{4}$. Το αποτέλεσμα ακολουθεί σύμφωνα με το ακόλουθο Λήμμα:

Λήμμα: Έστω $n \in \mathbb{Z},\ n = s_1 \cdot ... \cdot s_t,\ n \equiv 1 \pmod 4,\ s_i \equiv 1 \pmod 4$ για κάθε $i = 1, ..., t$. Ισχύει ότι $\frac{n-1}{4} \equiv \sum_{i=1}^{t} \frac{s_i-1}{4} \pmod 4$.

Απόδειξη:
Θα αποδείξουμε την υπόθεση πρώτα για δύο παράγοντες.
Αν $n = s \cdot t,\ s \equiv 1 \pmod 4,\ t \equiv 1 \pmod 4$, τότε $s = 4k + 1,\ t = 4l + 1,\ k,\ l \in \mathbb{Z}$.
Έτσι, $n = (4k + 1) \cdot (4l + 1) = 16kl + 4l + 4k + 1 \Rightarrow \frac{n-1}{4} = 4kl + k + l \equiv k + l = \frac{s-1}{4} + \frac{l-1}{4} \pmod 4$.

Κάνοντας, τώρα, επαγωγή στο πλήθος των όρων έχουμε την επαγωγική μου υπόθεση ότι ισχύει για t όρους, δηλαδή $n = s_1 \cdot ... \cdot s_t$, όπου $s_i \equiv 1 \pmod 4$ μας δίνει ότι:

$$\frac{n-1}{4} \equiv \sum_{i=1}^{t} \frac{s_i-1}{4} \pmod 4.$$

Αν $n' = s_1 \cdot s_2 \cdot ... \cdot s_{t+1} = n \cdot s_{t+1},\ s_i \equiv 1 \pmod 4$, τότε $n \equiv 1 \pmod 4,\ s_{t+1} \equiv 1 \pmod 4$, άρα εφαρμόζοντας τη σχέση που έχουμε αποδείξει για τους δύο όρους, παίρνουμε:

$$\frac{n'-1}{4} \equiv \frac{n-1}{4} + \frac{s_{t+1}-1}{4} \equiv \sum_{i=1}^{t} \frac{s_i-1}{4} + \frac{s_{t+1}-1}{4} \equiv \sum_{i=1}^{t+1} \frac{s_i-1}{4} \pmod 4.$$

2.5 Ο Νόμος Διτετραγωνικής Αντιστροφής

Για την απόδειξη του νόμου από εδώ και πέρα θα υποθέσουμε ότι λ, π είναι δύο primary στοιχεία του $\mathbb{Z}[i]$, τα οποία είναι και πρώτα μεταξύ τους.

Θεώρημα 2.5.1:[[5] Κεφάλαιο 9 παράγραφος 9]

Ισχύει:
$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{N(\lambda)-1}{4} \cdot \frac{N(\pi)-1}{4}}$

Παρατηρήσεις σχετικές με τον Νόμο:

1) Αν τα λ και π είναι primary, όπου $\lambda = c + di,\ \pi = a + bi$, είναι εύκολο να παρατηρήσουμε ότι τα $\frac{N(\lambda)-1}{4} \cdot \frac{N(\pi)-1}{4}$ και τα $\frac{a-1}{2} \cdot \frac{c-1}{2}$ έχουν το ίδιο "parity", δηλαδή είναι ταυτόχρονα ή και τα δύο περιττά ή και τα δύο άρτια δίνοντας, έτσι, και τα δύο την ίδια τιμή +1 ή -1 ως εκθέτες στον Νόμο.
Άρα, ο Νόμος μπορεί να διατυπωθεί και ως: $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{a-1}{2} \cdot \frac{c-1}{2}}$.
Συγκεκριμένα, μετά από υπολογισμούς συμπεραίνουμε ότι αν τα π και λ είναι ισότιμα με 1 (mod 4) τότε τα π και λ έχουν ίσο διτετραγωνικό χαρακτήρα, ενώ αν και τα δύο είναι ισότιμα με $3 + 2i$ (mod 4) (βλ. Λήμμα 2.3.1), τότε τα π και λ έχουν αντίθετους διτετραγωνικούς χαρακτήρες. Δηλαδή, ισχύει ότι $\chi_\pi(\lambda) = -\chi_\lambda(\pi)$.

2) Έστω π primary, ανάγωγο με $N(\pi) = p \equiv 1 \pmod 4$ και έστω χ_π ο συσχετιζόμενος τετραδικός χαρακτήρας υπολοίπων. Τότε μπορούμε να δούμε τον χ_π ως έναν πολλαπλασιαστικό χαρακτήρα πάνω από το πεπερασμένο σώμα $\mathbb{Z}[i]/\pi\mathbb{Z}[i] = F$. Αυτό είναι ένα σώμα με p στοιχεία (όσα η Norm του π) που αποτελείται από τις κλάσεις υπολοίπων $0, 1, ...p-1$. Αν $\zeta = e^{2\pi i/p}$ έστω $g(\chi_\pi) = \sum_{j\in F} \chi_\pi(j)\zeta^j$ το άθροισμα Gauss που ανήκει στον χ_π. Αν $\psi = \chi^2{}_\pi$, τότε ψ είναι ο μη τετριμμένος χαρακτήρας τάξης 2 και άρα είναι το σύμβολο του Legendre.

$$\chi_\pi(\alpha) = \alpha^{\frac{N(\pi)-1}{4}},\ (\chi_\pi(a))^4 = a^{N(\pi)-1} = a^{p-1} \equiv 1 \pmod p$$

απ΄όπου φαίνεται ότι ο χ_π έχει τάξη 4 και ο ψ έχει τάξη 2.

Πρόταση 2.5.2:

Ισχύει: $J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \psi)$, $\psi = \chi_\pi^2$.

Απόδειξη:
Έχουμε από Θεώρημα 2.2.3 d), το οποίο μπορούμε να εφαρμόσουμε για $\chi = \lambda = \chi_\pi$, εφόσον δεν πρόκειται για τον τετριμμένο χαρακτήρα, και αφού $\chi_\pi\chi_\pi = (\chi_\pi)^2 = \psi \neq \varepsilon$, ότι:

$$J(\chi_\pi, \chi_\pi) = \frac{g(\chi_\pi)g(\chi_\pi)}{g(\chi_\pi\cdot\chi_\pi)} = \frac{g^2(\chi_\pi)}{g(\psi)}.$$

Υψώνοντας στο τετράγωνο παίρνω :

$$J(\chi_\pi, \chi_\pi)^2 = \frac{g(\chi_\pi)^4}{g(\psi)^2}.$$

Τώρα, από Πρόταση 2.2.7, παρατηρώντας ότι πληρούνται οι υποθέσεις της, αφού έχουμε $n = 4 > 2$ και $p \equiv 1 \pmod 4$ όπως υποθέσαμε, έχουμε :

$$g(\chi_\pi)^4 = \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, \chi_\pi{}^2) = \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, \psi).$$

Όμως, το $\psi = \chi_\pi^2$ είναι, όπως παρατηρήσαμε, το σύμβολο του Legendre και άρα από Πρόταση 2.2.2 και αφού $p \equiv 1 \pmod 4$, έχουμε $|g(\psi)| = \sqrt{p} \Rightarrow g(\psi)^2 = |g(\psi)|^2 = (\sqrt{p})^2 = p$.
Τα p στο κλάσμα απλοποιούνται και άρα έχουμε τελικά το ζητούμενο.

Πρόταση 2.5.3:

$g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2$.

Απόδειξη:
Αυτή η Πρόταση έπεται άμεσα από την προηγούμενη αν αντικαταστήσουμε το αποτέλεσμά της στη σχέση $g(\chi_\pi)^4 = \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi_\pi, \psi)$ που αναφέραμε και πριν.
Επιπλέον, παρατηρούμε ότι είναι και ειδική περίπτωση της Πρότασης 2.2.7 για $n = 4$.

Πρόταση 2.5.4:

Το στοιχείο $-\chi_\pi(-1)J(\chi_\pi,\chi_\pi)$ είναι primary.

Απόδειξη:
Προφανώς, λόγω συμμετρίας ($t \hookrightarrow 1-t$) ισχύει:

$J(\chi_\pi,\chi_\pi) = 2\sum_{i=1}^{(p-1)/2}\chi_\pi(t)\chi_\pi(1-t) + \chi_\pi(\frac{p+1}{2})^2$.

Αλλά, κάθε μονάδα στο $\mathbb{Z}[i]$ είναι ισότιμη με 1 (mod $(1+i)$), δηλαδή ισχύει $u \equiv 1 \pmod{(1+i)}$ για $u = 1, -1, i, -i$.
Επίσης, είχαμε πάρει $p \equiv 1 \pmod 4$, άρα έχουμε ότι p είναι primary.
Άρα, $p \equiv 1 \pmod{(2i+2)}$.
Επιπλέον, έχουμε $\chi_\pi(\frac{p+1}{2})^2 = (\chi_\pi(2^{-1}))^2 = \chi_\pi(2)^{-2} = \chi_\pi(2)^2 = \chi_\pi(-i(i+1)^2)^2 =$
$= \chi_\pi(-i)^2\chi_\pi(1+i)^4 = \chi_\pi(-i)^2 = \chi_\pi(-1)$.

Στο άθροισμα Jacobi έχουμε ότι τα διάφορα γινόμενα των χαρακτήρων παίρνουν τιμές κάποια 4-ρίζα της μονάδας, αφού το ίδιο κάνει και ο χαρακτήρας και άρα και τα γινόμενα θα πέφτουν πάλι μέσα σε αυτό το σύνολο. Παρατηρούμε ότι το άθροισμα αυτό έχει $\frac{p-3}{2}$ όρους και είδαμε ότι όλες οι μονάδες είναι ισότιμες με 1 (mod $(1+i)$). Άρα, με το 2 που υπάρχει μπροστά από το άθροισμα, παίρνοντας τη σχέση (mod $(2+2i)$) θα έχουμε συνολικά:

$$J(\chi_\pi,\chi_\pi) \equiv 2\cdot(\tfrac{p-3}{2}) + \chi_\pi(-1) \pmod{(2+2i)}.$$

Αφού $p \equiv 1 \pmod 4$, έχουμε $p-3 \equiv -2 \pmod 4$ και άρα συνεχίζοντας έχουμε :

$$J(\chi_\pi,\chi_\pi) \equiv -2 + \chi_\pi(-1) \pmod{(2+2i)}.$$

Πολλαπλασιάζοντας με $\chi_\pi(-1)$ τη σχέση, παίρνουμε:

$$-\chi_\pi(-1)J(\chi_\pi,\chi_\pi) \equiv 2\cdot\chi_\pi(-1) - 1 \pmod{(2+2i)}$$

διότι από Πρόταση 2.4.7, είναι $\chi_\pi(-1) = \pm 1 \Rightarrow (\chi_\pi(-1))^2 = 1$.

Για τις δύο διακριτές τιμές του $\chi_\pi(-1)$ προκύπτει το ίδιο αποτέλεσμα και έχουμε τελικά ότι $-\chi_\pi(-1)J(\chi_\pi,\chi_\pi) \equiv 1 \pmod{(2+2i)}$ και άρα αποδείχτηκε η υπόθεση.

Πρόταση 2.5.5:

$-\chi_\pi(-1)J(\chi_\pi,\chi_\pi) = \pi$

Απόδειξη:
Το π είναι ανάγωγο, οπότε για να ισχύει η ισότητα πρέπει και $-\chi_\pi(-1)J(\chi_\pi,\chi_\pi)$ να είναι ανάγωγο. Ισχύει ότι $N(J(\chi_\pi,\chi_\pi)) = p$, αφού $N(J(\chi_\pi,\chi_\pi)) = J(\chi_\pi,\chi_\pi)\overline{J(\chi_\pi,\chi_\pi)} = |J(\chi_\pi,\chi_\pi)|^2 =$
$= \sqrt{p}\,\sqrt{p} = p$ (βλ. Θεώρημα 2.2.4).
Άρα, έχουμε ότι το $J(\chi_\pi,\chi_\pi)$ είναι ανάγωγο και άρα και πολλαπλασιασμένο με μία μονάδα θα παραμένει ανάγωγο. Έχουμε, τώρα, ότι $J(\chi_\pi,\chi_\pi) \equiv \sum_{t=1}^{p-1} t^{(p-1)/4}(1-t)^{(p-1)/4} \pmod{\pi}$ το οποίο είναι ισοδύναμο με $0 \pmod{\pi}$ βάσει του αποτελέσματος της παρακάτω Πρότασης:

Πρόταση: $1^k + 2^k + ... + (p-1)^k \equiv 0 \pmod{p}$, αν $p-1 \nmid k$ και $\equiv -1 \pmod{p}$ όταν $(p-1)|k$.
Απόδειξη:
Έστω $S_k = 1^k + 2^k + ... + (p-1)^k$. Έστω g μία πρωταρχική ρίζα *modulop*. Τότε $\overline{g}$ είναι γεννήτορας της F_p^*. Άρα, ισχύει ότι $(\overline{1}, \overline{2}, ..., \overline{p-1})$ είναι μια εναλλαγή του $(\overline{1}, \overline{g}, \overline{g}^2, ..., \overline{g}^{p-2})$.

$$\overline{S_k} = \overline{1}^k + \overline{2}^k + ... + \overline{p-1}^k = \sum_{i=0}^{p-2} \overline{g}^{k\cdot i} = \begin{cases} \overline{p-1} = \overline{-1}, & (p-1)|k \\ \frac{\overline{g}^{(p-1)k}-1}{\overline{g}^k-1} = \overline{0}, & (p-1) \nmid k \end{cases}$$

Για την πρώτη περίπτωση, όπου $(p-1)|k$, θα έχουμε ότι όλοι οι όροι υψωμένοι εις την k θα δίνουν 1 και είναι σύνολο $p-1$ όροι, οπότε προκύπτει το αποτέλεσμα.
Για την δεύτερη περίπτωση, αφού $(p-1) \nmid k$, θα έχουμε ότι ο παρανομαστής θα είναι διάφορος του 0, ενώ ο αριθμητής θα ισούται με 0, αφού $(\overline{g}^k)^{p-1} = 1$. Άρα, προκύπτει και το δεύτερο αποτέλεσμα.

Συνεχίζοντας με την απόδειξη έχουμε ότι $J(\chi_\pi,\chi_\pi) \equiv 0 \pmod{\pi}$, αλλά $(1+i) \nmid J(\chi_\pi,\chi_\pi)$, διότι π primary και άρα $\pi \equiv 1 \pmod{2+2i} \Rightarrow (1+i)|(2+2i)|(\pi-1)$. Ισχύουν, επομένως, οι υποθέσεις του Λήμματος 2.3.2 για το $J(\chi_\pi,\chi_\pi)$ και άρα συμπεραίνουμε ότι υπάρχει μοναδική μονάδα u τέτοια ώστε $u \cdot J(\chi_\pi,\chi_\pi)$ να είναι primary. Εφόσον είναι μοναδική, όμως, από Πρόταση 2.5.2 την έχουμε βρει και είναι η $-\chi_\pi(-1)$. Αντίστοιχα, $(1+i) \nmid \pi$ και άρα, εφόσον το ίδιο π είναι primary, η μοναδική μονάδα θα είναι το 1. Καταλήγουμε ότι έχουμε ότι έχουμε δύο στοιχεία ισότιμα modπ, primary, ανάγωγα και με ίση Norm και είναι και τα δύο πάνω από τον ίδιο πρώτο αριθμό p. Άρα, είναι ίσα.

Θεώρημα 2.5.6:

$g(\chi_\pi)^4 = \pi^3\overline{\pi}$.

Απόδειξη:
Συνδυάζοντας τις Προτάσεις 2.5.3, 2.5.5 παίρνουμε $g(\chi_\pi)^4 = p \cdot \pi^2$.
Αλλά από Νόμο Ανάλυσης $p = \pi\overline{\pi}$ και προκύπτει το ζητούμενο.

-Στη συνέχεια, θα αποδείξουμε προτάσεις οι οποίες είναι ουσιαστικά διτετραγωνικοί νόμοι αντιστροφής για συγκεκριμένες κλάσεις στοιχείων. Η σύνθεση όλων αυτών των προτάσεων θα μας δώσει το συνολικό αποτέλεσμα.

Πρόταση 2.5.7:

Έστω $q > 0$ ένας πραγματικός ανάγωγος στο $\mathbb{Z}[i]$. Τότε $\chi_\pi(-q) = \chi_q(\pi)$.

Απόδειξη:
Αφού $q \equiv 3 \pmod 4$ έχουμε:

$$g(\chi_\pi)^q \equiv \sum_{j=1}^{p-1} \chi_\pi(j)^q \zeta^{qj} \pmod q \equiv \sum {\chi_\pi}^3(j)\zeta^{qj} \pmod q.$$

Ισχύει ${\chi_\pi}^3(j) = \frac{{\chi_\pi}^4(j)}{\chi_\pi(j)} = \overline{\chi}_\pi(j)$.

Αντικαθιστώντας αυτό στο τελευταίο άθροισμα έχουμε:

$$\sum_{j=1}^{p-1} \frac{\overline{\chi}_\pi(j)}{\overline{\chi}_\pi(q)} \zeta^{qj} \overline{\chi}_\pi(q) = \frac{1}{\overline{\chi}_\pi(q)} \sum_{j=1}^{p-1} \overline{\chi}_\pi(jq)\zeta^{qj} \equiv \chi_\pi(q) g(\overline{\chi}_\pi) \pmod q.$$

Συνολικά, $g(\chi_\pi)^q \equiv \chi_\pi(q) g(\overline{\chi}_\pi) \pmod q$.

Άρα, $(g(\chi_\pi)^4)^{(q+1)/4} = g(\chi_\pi)^{q+1} \equiv \chi_\pi(q) g(\chi_\pi) g(\overline{\chi}_\pi) \pmod q$.

Σύμφωνα με την Παρατήρηση της Πρότασης 2.2.2, έχουμε ότι: $g(\overline{\chi}_\pi) = \chi_\pi(-1)\overline{g(\chi_\pi)}$.
Εδώ, $g(\chi_\pi) g(\overline{\chi}_\pi) = g(\chi_\pi)\chi_\pi(-1)\overline{g(\chi_\pi)} = \chi_\pi(-1)|g(\chi_\pi)|^2 = \chi_\pi(-1)p = \chi_\pi(-1)\pi\overline{\pi} = \chi_\pi(-1)\pi\pi^q =$
$= \chi_\pi(-1)\pi^{q+1}$.
Από το αποτέλεσμα της Πρότασης 2.2.2, πήραμε $|g(\chi_\pi)|^2 = p$ και, επιπλέον, $\overline{\pi} \equiv \pi^q \pmod q$, γιατί $\pi^q = (a + bi)^q \equiv a^q + (bi)^q \equiv a^q + b^q i^q \equiv a + bi^3 = a - bi = \overline{\pi} \pmod q$.

Χρησιμοποιώντας την παραπάνω Πρόταση και το γεγονός ότι $\pi^q \equiv \overline{\pi} \pmod q$ καταλήγουμε ότι:

$$\pi^{[(q+3)(q+1)]/4} \equiv \chi_\pi(-1)\chi_\pi(q)\pi^{q+1} \pmod q \text{ ή } \pi^{(q^2-1)/4} \equiv \chi_\pi(-q) \pmod q.$$

Αλλά $N(q) = q^2$ για $q \equiv 3 \pmod 4$ και άρα $\chi_q(\pi) = \pi^{(q^2-1)/4}$. Άρα, $\chi_q(\pi) \equiv \chi_\pi(-q) \pmod q$. Αφού, όμως, και τα δύο μέλη είναι μονάδες του δακτυλίου $\mathbb{Z}[i]$, προκύπτει ότι δεν είναι μόνο ισότιμες αλλά και ίσες, πράγμα που ολοκληρώνει την απόδειξη.

Πρόταση 2.5.8:

Έστω q πρώτος με $q \equiv 1 \pmod 4$. Τότε $\chi_\pi(q) = \chi_q(\pi)$.

Απόδειξη:
Αφού $q \equiv 1 \pmod 4$, δουλεύοντας όπως πριν, έχουμε:

$g(\chi_\pi)^q \equiv \sum \chi_\pi(j)^q \zeta^{qj} \equiv \sum \chi_\pi(j)\zeta^{qj} \equiv \overline{\chi}_\pi(q) g(\chi_\pi) \pmod q$ όπου η τελευταία ισοδυναμία, όπως και πριν, ισχύει διότι:

$$\sum_{j=1}^{p-1} \frac{\chi_\pi(j)}{\chi_\pi(q)} \zeta^{qj} \chi_\pi(q) \equiv \frac{1}{\chi_\pi(q)} \sum_{j=1}^{p-1} \chi_\pi(jq)\zeta^{qj} \equiv \overline{\chi_\pi(q)} g(\chi_\pi) \pmod q.$$

Άρα, $g(\chi_\pi)^{q+3} \equiv \overline{\chi}_\pi(q) g(\chi_\pi)^4 \pmod q$ και εφαρμόζοντας την Πρόταση 2.5.6 έχουμε:

$$(\pi^3\overline{\pi})^{(q+3)/4} \equiv \overline{\chi}_\pi(q)\pi^3\overline{\pi} \pmod q.$$

Και τα δύο μέλη τις ισότητας ανήκουν στον $\mathbb{Z}[i]$ και $(q, \pi) = (q, \overline{\pi}) = 1$, άρα μπορούμε να απλοποιήσουμε τη σχέση: $(\pi^3)^{(q-1)/4}(\overline{\pi})^{(q-1)/4} \equiv \overline{\chi}_\pi(q) \pmod q$.

Αφού $q \in \mathbb{P}$, $q \equiv 1 \pmod 4$, ο q γράφεται: $q = \lambda\overline{\lambda}$ όπου $\lambda, \overline{\lambda}$ ανάγωγα στοιχεία στο $\mathbb{Z}[i]$.

Άρα, έχουμε ότι: $\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) \equiv \overline{\chi}_\pi(q) \pmod \lambda$, αφού $N(\lambda) = N(\overline{\lambda}) = q$.

Όπως και πριν, δε θα ισχύει μόνο η ισοτιμία αλλά και η ισότητα (βλ. τέλος απόδειξης της Πρότασης 2.5.7).

Άρα, $\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi}(q)$.

Αλλιώς, αυτό γράφεται $\overline{\chi_\lambda(\pi)}\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi}(q)$ (διότι $\pi^3 = \overline{\pi}$ και $N(\lambda) = N(\overline{\lambda})$) ή
$\chi_{\overline{\lambda}}(\overline{\pi})\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi}(q)$, που δίνει εξ' ορισμού $\chi_q(\overline{\pi}) = \overline{\chi}_\pi(q)$ και παίρνοντας συζυγίες στην τελευταία σχέση προκύπτει το ζητούμενο.

-Σε αυτό το σημείο αξίζει να παρατηρήσουμε ότι στην Πρόταση 2.5.7, το q δεν είναι ανάγωγο και ότι το αριστερό μέλος είναι το γενικευμένο σύμβολο διτετραγωνικού υπολοίπου!

Πρόταση 2.5.9:

Έστω α πραγματκός, δηλαδή $\alpha \in \mathbb{Z}$, με $\alpha \equiv 1 \pmod 4$ και λ primary, $(\lambda, a) = 1$. Τότε, $\chi_\alpha(\lambda) = \chi_\lambda(\alpha)$.

Απόδειξη:
Από Λήμμα 6.3, συμπεραίνουμε ότι εφόσον το α είναι primary μπορεί να γραφεί σαν γινόμενο primary αναγώγων. Συγκεκριμένα, υπάρχουν primary ανάγωγα $\pi_i,\ i = 1, .., r$ με $N(\pi_i) \equiv 1 \pmod 4$ και primary ανάγωγα $-q_j$, όπου $q_j \equiv 3 \pmod 4 \Rightarrow (-q_j \equiv 1 \pmod 4)$ τέτοια ώστε $\alpha = \pi_1...\pi_r(-q_1)...(-q_s)$.
Άρα, $\chi_\alpha(\lambda) = \chi_{\pi_1...\pi_r(-q_1)...(-q_s)}(\lambda) = \chi_{\pi_1}(\lambda)...\chi_{\pi_r}(\lambda)\chi_{-q_1}(\lambda)...\chi_{-q_s}(\lambda)$.

Εφόσον $(\alpha, \lambda) = 1$ δεν έχουμε πρόβλημα στο όρισμα των χαρακτήρων. Από το Λήμμα 2.3.3 και τις Προτάσεις 2.4.7, 2.5.7, 2.5.8: ισχύει η αντιστροφή και άρα έχουμε για το παραπάνω ότι είναι ίσο με:

$$\chi_\lambda(\pi_1)...\chi_\lambda(\pi_r)\chi_\lambda(-q_1)...\chi_\lambda(-q_s) = \chi_\lambda(\alpha).$$

Πρόταση 2.5.10:

Υποθέτουμε ότι έχουμε δύο σχετικά πρώτα και primary στοιχεία $\pi = a + bi,\ \lambda = c + di$.
Αν $(a, b) = 1$ και $(c, d) = 1$, τότε $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{a-1}{2}\frac{c-1}{2}}$.

Απόδειξη:
Με χρήση της γενικής υπόθεσης της παραγράφου και των υποθέσεων $(a, b) = 1$ και $(c, d) = 1$ της Πρότασης, έχουμε ότι $(a, \pi) = (b, \pi) = (c, \lambda) = (d, \lambda) = 1$.
Έχουμε $\lambda = c + di \equiv 0 \pmod \lambda \Rightarrow c \equiv -di \pmod \lambda$. Έτσι, προκύπτει $c\pi \equiv ca + bd \pmod \lambda$. Με όμοιο τρόπο, $a\lambda \equiv ac + bd \pmod \pi$. Από αυτά έπεται ότι $(ac + bd, \lambda) = (ac + bd, \pi) = 1$, γιατί εφόσον τα π, λ είναι ανάγωγα, αν ο μκδ δεν ήταν 1 θα ήταν π ή λ αντίστοιχα. Αλλά, αυτό δεν ισχύει φυσικά, γιατί τότε θα ήταν $\lambda|(ac+bd)|c\pi$, αλλά λ ανάγωγο και $(\lambda, c) = (\pi, \lambda) = 1$, άτοπο. Ανάλογα αποδεικνύεται και ότι $(ac + bd, \pi) = 1$.

Επιπλέον, $\chi_\lambda(c)\chi_\lambda(\pi) = \chi_\lambda(ac + bd)$ (1) και

$\chi_\pi(a)\chi_\pi(\lambda) = \chi_\pi(ac + bd)$ (2)

Παίρνοντας συζυγία στη (2) και πολλαπλασιάζοντας με την (1) έχουμε:
$\chi_\lambda(c)\chi_{\bar\pi}(a)\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\lambda\bar\pi}(ac + bd)$

Ισοδύναμα, $\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\bar\lambda}(c)\chi_\pi(a)\chi_{\lambda\bar\pi}(ac + bd)$ (3).

Υποθέτουμε ότι τα $a, c, ac+bd$ δεν είναι μονάδες. Οι 3 αυτοί αριθμοί είναι περιττοί λόγω ορισμού των π και λ ως primary στοιχεία. Δουλεύοντας, λοιπόν, μόνο με το δεξί μέλος της τελευταίας εξίσωσης, ορίζουμε για κάποιον περιττό ακέραιο n τη συνάρτηση πρόσημο $\epsilon(n) = (-1)^{(n-1)/2}$. Τότε ισχύει για κάθε τέτοιον n ότι $\epsilon(n)n \equiv 1 \pmod 4$. Επιπλέον, έχουμε $\epsilon(ac+bd) = \epsilon(a)\epsilon(c)$ αφού $bd \equiv 0 \pmod 4$ ($b \equiv 0$ ή $2 \pmod 4, d \equiv 0$ή $2 \pmod 4$).
Γράφοντας $\chi_\alpha(x) = \chi_\alpha(\epsilon(x))\chi_\alpha(\epsilon(x)x)$ για κάθε όρο του δεξιού μέλους της (3) (αφού $\epsilon(x)^2 = 1$ έχοντας επιλέξει x περιττό), παρατηρώντας ότι $\chi_\alpha(\epsilon(x)) = \chi_{\overline{\alpha}}(\epsilon(x))$ και χρησιμοποιώντας την Πρόταση 2.5.9 αφού πλέον έχουμε την ισοτιμία 1 mod4 λόγω του ότι $\epsilon(n)n \equiv 1 \pmod 4$, παίρνουμε για τους όρους αυτούς την αντίστοιχη αντιστροφή τους.

Άρα, $\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_c(\overline{\lambda})\chi_a(\pi)\chi_{ac+bd}(\lambda\overline{\pi})$ (4).

Τώρα για τους 3 τελευταίους όρους, χρησιμοποιώντας την Πρόταση 2.4.6, έχουμε τις σχέσεις:
$\chi_c(\overline{\lambda}) = \chi_c(c-di) = \chi_c(-di) = \chi_c(i)$
$\chi_a(\pi) = \chi_a(a+bi) = \chi_a(bi) = \chi_a(i)$
$\chi_{ac+bd}(\overline{\pi}\lambda) = \chi_{ac+bd}((ad-bc)i) = \chi_{ac+bd}(i)$

Άρα, έχουμε τη σχέση:
$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{(ac+bd)ac}(i) = (-1)^{((ac+bd)ac-1)/4} = (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}$. (βλ. Πρόταση 2.4.7), όπου η τελευταία ισότητα των εκθετών ισχύει λόγω ισοτιμίας mod2.
Ανάλογα αποδεικνύεται η Πρόταση στην περίπτωση που κάποιο από τα $a, c, ac+bd$ είναι μονάδα.

Απόδειξη του Διτετραγωνικού Νόμου Αντιστροφής:

Ο γενικός Νόμος Διτετραγωνικής Αντιστροφής έπεται εύκολα από την Πρόταση 2.5.10.
Γράφουμε $\pi = m(a+bi), \lambda = n(c+di)$, $(\pi, \lambda) = 1$, όπου πρέπει $m \equiv n \equiv 1 \pmod 4$ (διότι τα π, λ είναι primary), $(a,b) = 1, (c,d) = 1$. Από Πρόταση 2.5.9, $\chi_\pi(n) = \chi_n(\pi)$ και $\chi_\lambda(m) = \chi_m(\lambda)$. Επίσης, $\chi_m(n) = \chi_n(m)$ από Πρόταση 2.4.6. Τότε, αφού τα $a+bi,\ c+di$ είναι primary:

$$\chi_\lambda(\pi) = \chi_\lambda(m)\chi_\lambda(a+bi) =$$
$$= \chi_m(\lambda)\chi_n(a+bi)\chi_{c+di}(a+bi) =$$
$$= \chi_m(\lambda)\chi_{a+bi}(n)\chi_{a+bi}(c+di)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}} =$$
$$= \chi_\pi(\lambda)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}} =$$
$$= \chi_\pi(\lambda)(-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\lambda)-1}{4}}.$$

όπου η τελευταία ισότητα προκύπτει διότι $m \equiv n \equiv 1 \pmod 4$.
Ο Διτετραγωνικός Νόμος Αντιστροφής έχει αποδειχτεί!

2.6 Ο Τετραδικός χαρακτήρας του 2

Όπως στον τετραγωνικό νόμο αντιστροφής έχουμε έξτρα τη μελέτη των περιπτώσεων $\left(\frac{2}{p}\right)$ και $\left(\frac{-1}{p}\right)$, έτσι και εδώ υπολογίζουμε κατ΄ αρχήν το $\chi_\pi(1+i)$ και στη συνέχεια το $\chi_\pi(2)$, αφού $2 = (-i)\cdot(1+i)^2$.

Πρόταση 2.6.1:

Έστω p πρώτος, $p \equiv 1 \pmod 4$ ώστε ο p να γράφεται $p = \pi\overline{\pi}$, $\pi \in \mathbb{Z}[i]$.
Ισχύει ότι $\chi_p(1+i) = i^{\frac{(p-1)}{4}}$.

Απόδειξη:
Έχουμε $\chi_p(1+i) = \chi_\pi(1+i)\chi_{\overline{\pi}}(1+i) = \chi_\pi(1+i)\overline{\chi_\pi(1-i)} = \frac{\chi_\pi(1+i)}{\chi_\pi(1-i)} = \frac{\chi_\pi(i)\chi_\pi(1-i)}{\chi_\pi(1-i)} = \chi_\pi(i) = i^{\frac{p-1}{4}}$.

Στις ισότητες χρησιμοποιήσαμε ότι $(1-i)\cdot i = 1+i$, ενώ η τελευταία ισότητα προκύπτει ως συνέπεια του ορισμού του χ_π: $\chi_\pi(i) \equiv i^{\frac{p-1}{4}} \pmod\pi$, με τις κλάσεις $1, i, i^2, i^3 \pmod\pi$ να είναι διακριτές και άρα να έχουμε την ισότητα αντί της ισοτιμίας.

Πρόταση 2.6.2:

Έστω q θετικός πρώτος, $q \equiv 3 \pmod 4$. Ισχύει ότι $\chi_q(1+i) = i^{\frac{-q-1}{4}}$.

Απόδειξη:
Για την απόδειξη θα μας βοηθήσει, αρχικά, να αποδείξουμε ότι $(1+i)^{q-1} \equiv -i \pmod q$.

Ξεκινάμε γράφοντας το q στη μορφή $q = 4k+3, k \in \mathbb{N}$.
Έχουμε $(1+i)^2 = 1+2i+i^2 = 2i$ και άρα $(1+i)^{q-1} = (2i)^{\frac{q-1}{2}}$.
Αλλά, το πρώτο μέλος γράφεται $(1+i)^{4k+2} = (1+i)^{4k}(1+i)^2 = [(1+i)^2]^{2k}(1+i)^2 = 2i^{\frac{q-3}{2}}\cdot 2i = (2i)^{\frac{q-1}{2}}$.
Το πρόβλημα ανάγεται στο να υπολογίσουμε το $2^{\frac{q-1}{2}}$ και το $i^{\frac{q-1}{2}}$.

Ισχύει (βλ. Πρόταση 1.1.1 *a*)) ότι $2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \pmod q$.
Επίσης, $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = (-1)^{2k^2+3k+1} = (-1)^{k+1}$
και $i^{\frac{q-1}{2}} = i^{2k+1} = (-1)^k \cdot i$.
Συνολικά, λοιπόν, έχουμε ότι το γινόμενο δίνει $(-1)^{2k+1}\cdot i = (-1)\cdot i = -i$.
Άρα, όντως προκύπτει ότι $(1+i)^{q-1} \equiv -i \pmod q$.

Τώρα, εφόσον $q \equiv 3 \pmod 4$, ισχύει ότι $N(q) = q^2$.
Έχουμε $\chi_q(1+i) \equiv (1+i)^{\frac{q^2-1}{4}} \equiv (-i)^{\frac{q+1}{4}} \pmod q$.
Άρα, $\chi_q(1+i) \equiv (-i)^{\frac{-q-1}{4}} \pmod q$ (αφού $i^{-1} = -i$), με την ισότητα να προκύπτει βάσει του ίδιου επιχειρήματος με πριν.

Πρόταση 2.6.3:

Έστω $\pi = a + bi$ primary πρώτο στο $\mathbb{Z}[i]$, $b \neq 0$. Ισχύει ότι $a \equiv (-1)^{\frac{p-1}{4}} \pmod 4$, $p = N\pi$.

Απόδειξη:
Έχουμε την ανάλυση του p ως $p = \pi\overline{\pi} = a^2 + b^2 \equiv 1 \pmod 4$.

Διακρίνουμε δύο περιπτώσεις:

Πρώτη περίπτωση αν $a \equiv 1 \pmod 4$ και $b \equiv 0 \pmod 4$, όπου $a = 4A + 1$, $b = 4B$. Τότε:
$\frac{a^2+b^2-1}{4} = 4A^2 + 4B^2 + 2A$, δηλαδή άρτιος.
Άρα, $(-1)^{\frac{p-1}{4}} = (-1)^{\frac{a^2+b^2-1}{4}} = 1$ και $a \equiv 1 \pmod 4$, συνεπώς $a \equiv (-1)^{\frac{p-1}{4}}$.

Δεύτερη περίπτωση αν $a \equiv 3 \pmod 4$ και $b \equiv 2 \pmod 4$, όπου $a = 4A + 3, b = 4B + 2$. Τότε:
$a^2 + b^2 - 1 = 16A^2 + 24A + 9 + 16B^2 + 16B + 4 - 1 \equiv 4 \pmod 8 \Rightarrow \frac{a^2+b^2-1}{4} \equiv 1 \pmod 2$.
Άρα, $(-1)^{\frac{p-1}{4}} = (-1)^{\frac{a^2+b^2-1}{4}} = -1$ και $a \equiv -1 \pmod 4$, άρα και πάλι καταλήγουμε στο συμπέρασμα.

Παρατηρούμε ότι με τις παραπάνω υποθέσεις, το στοιχείο $a(-1)^{\frac{p-1}{4}}$ είναι primary, εφόσον είναι ισότιμο με 1 mod4. Με τις ίδιες υποθέσεις, λοιπόν, η ακόλουθη Πρόταση που θα αποδείξουμε εμπίπτει και εφαρμόζεται και για το στοιχείο αυτό.

Πρόταση 2.6.4:

Αν $a(-1)^{\frac{p-1}{4}}$ primary στοιχείο, τότε ισχύει ότι $\chi_\pi(a(-1)^{\frac{p-1}{4}}) = (-1)^{\frac{a^2-1}{8}}$.

Απόδειξη:
Παρατηρήσαμε και πριν ότι το στοιχείο $a(-1)^{\frac{p-1}{4}}$ είναι primary και επιπλέον, μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι το a δεν είναι μονάδα, γιατί ακόμα και αν $a = \pm 1$ ένας γρήγορος έλεγχος μας δίνει και πάλι το ζητούμενο.
Τώρα, αφού $a(-1)^{\frac{p-1}{4}} \equiv 1 \pmod 4$, η Πρόταση 2.5.9 μας δίνει:

$\chi_\pi(a(-1)^{\frac{p-1}{4}}) = \chi_{a(-1)^{\frac{p-1}{4}}}(\pi) = \chi_a(\pi) = \chi_a(a+bi) = \chi_a(bi) = \chi_a(b)\cdot\chi_a(i)$.

Αφού $(a,b)=1$, από Πρόταση 2.4.6 έχουμε $\chi_a(b)=1$ και τελικά, $\chi_\pi(a(-1)^{\frac{p-1}{4}}) = \chi_a(i)$.

Στη γενική περίπτωση διακρίνουμε δύο περιπτώσεις: την περίπτωση $a \equiv 1 \pmod 4$ και την περίπτωση $a \equiv -1 \pmod 4$.

Στην πρώτη περίπτωση εφαρμόζουμε την Πρόταση 2.4.7 και αποδεικνύουμε, επιπλέον, ότι $\chi_a(i) = (-1)^{\frac{a^2-1}{8}}$.
Συγκεκριμένα, $a = 4A+1$ και $(-1)^{\frac{a^2-1}{8}} = (-1)^{2A^2+A} = (-1)^A = (-1)^{\frac{a-1}{4}} = \chi_a(i)$.

Για την δεύτερη περίπτωση επαναλαμβάνουμε την ίδια ακριβώς διαδικασία θέτοντας $a = 4A-1$ και δουλεύοντας με το $\chi_{-a}(i)$, αφού ισχύει ότι $\chi_a(i) = \chi_{-a}(i)$.

Πρόταση 2.6.5:

Αν $\pi = a+bi$ ένα primary ανάγωγο στοιχείο με $(a,b)=1$, ισχύουν τα παρακάτω:
a) Αν $\pi \equiv 1 \pmod 4$, τότε $\chi_\pi(a) = i^{\frac{a-1}{2}}$.
b) Αν $\pi \equiv 3+2i \pmod 4$, τότε $\chi_\pi(a) = -i^{\frac{-a-1}{2}}$.

Απόδειξη:
a) Αφού $\pi \equiv 1 \pmod 4$, θα έχουμε $a \equiv 1 \pmod 4$ και $b \equiv 0 \pmod 4$, δηλαδή $a = 4A+1$, $b = 4B, A, B \in \mathbb{Z}$.

Από Πρόταση 2.4.7 θα ισχύει $\chi_\pi(i) = (-1)^{\frac{a-1}{4}} = (-1)^{\frac{4A+1-1}{4}} = (-1)^A$
και άρα $\chi_\pi(-1) = (-1)^{2A} = (-1)^{\frac{a-1}{2}}$.

Τώρα, από Πρόταση 2.6.4, με τις υποθέσεις να ισχύουν, έχουμε: $\chi_\pi(a(-1)^{\frac{p-1}{4}}) = (-1)^{\frac{a^2-1}{8}}$.

Συνδυάζοντας, έχουμε: $\chi_\pi(a)\cdot\chi_\pi(-1)^{\frac{p-1}{4}} = (-1)^{\frac{a^2-1}{8}} \Rightarrow (-1)^{\frac{p-1}{4}\cdot\frac{a-1}{2}}\chi_\pi(a) = (-1)^{\frac{a^2-1}{8}}$

$\Rightarrow \chi_\pi(a) = (-1)^{\frac{a^2-1}{8}}(-1)^{\frac{p-1}{4}\frac{a-1}{2}}$, όπου $N\pi = p = a^2+b^2$ και άρα:

$$(-1)^{\frac{p-1}{4}} = (-1)^{\frac{a^2+b^2-1}{4}} = (-1)^{\frac{a^2-1}{4}+\frac{b^2}{4}} = (-1)^{4A^2+2A+4B^2} = 1.$$

Άρα, συνολικά $\chi_\pi(a) = (-1)^{\frac{a^2-1}{8}} = (-1)^{2A^2+A} = (-1)^{A\cdot(2A+1)} = (-1)^A = (-1)^{\frac{a-1}{4}} = (i^2)^{\frac{a-1}{4}} = i^{\frac{a-1}{2}}$.

Άρα, για $\pi \equiv 1 \pmod 4$ ισχύει $\chi_\pi(a) = i^{\frac{a-1}{2}}$.

b) Για $\pi \equiv 3+2i \pmod 4$ έχουμε: $a = 4A+3, b = 4B+2, A, B \in \mathbb{Z}$.
Όπως και στο *a*) προκύπτει ότι $\chi_\pi(a) = (-1)^{\frac{a-1}{2}\cdot\frac{p-1}{4}}(-1)^{\frac{a^2-1}{8}}$.

Εδώ, $a^2+b^2-1 = 16A^2+24A+16B^2+16B+12 \equiv 4 \pmod 8$. Άρα, $\frac{a^2+b^2-1}{4} \equiv 1 \pmod 2$.
Επομένως, $(-1)^{\frac{p-1}{4}} = (-1)^{\frac{a^2+b^2-1}{4}} = -1$.
Ομοίως για το $\frac{a^2-1}{8}$ υπολογίζουμε ότι είναι ίσο με $2A^2+3A+1$
και άρα $(-1)^{\frac{a^2-1}{8}} = (-1)^{3A+1} = (-1)^{A+1} = (-1)^{\frac{a+1}{4}}$.

Τελικά, έχουμε: $\chi_\pi(a) = -(-1)^{\frac{a+1}{4}} = -i^{\frac{a+1}{4}}$.
Με έναν απλό υπολογισμό επαληθεύουμε ότι τα $\frac{a+1}{2}$ και $\frac{-a-1}{2}$ είναι ισότιμα mod4 και άρα έχουμε και τη διατύπωση της Πρότασης.

Πρόταση 2.6.6:

Αν $\pi = a+bi$ primary, ανάγωγο με $(a,b)=1$, τότε $\chi_\pi(a)\chi_\pi(1+i) = i^{\frac{3\cdot(a+b-1)}{4}}$.

Απόδειξη:
Αρχικά, ξεκινάμε την απόδειξη γενικεύοντας τις Προτάσεις 2.6.1 και 2.6.2 ως εξής:
Αν $n \equiv 1 \pmod 4,\ n \neq 1$, τότε $\chi_n(1+i) = i^{\frac{n-1}{4}}$. Έστω $n \in \mathbb{Z},\ n \equiv 1 \pmod 4,\ n \neq 1$.
Συγκεκριμένα, αν $p \equiv 1 \pmod 4$ έχουμε ακριβώς το συμπέρασμα της Πρότασης 2.6.1, ενώ αν $q \equiv 3 \pmod 4$, δηλαδή $-q \equiv 1 \pmod 4$, q πρώτος, τότε διατυπώνουμε την Πρόταση 2.6.2 ως: $\chi_{-q}(1+i) = \chi_q(1+i) = i^{\frac{-q-1}{4}}$.

Διακρίνουμε δύο περιπτώσεις:
-Αν $n>0$: $n = q_1q_2...q_kp_1...p_l$, όπου $q_i \equiv -1 \pmod 4$ και $p_i \equiv 1 \pmod 4$, τότε k είναι άρτιος.
-Αν $n<0$: $n = -q_1q_2...q_kp_1...p_l$ με k περιττό.
Και στις δύο πεεριπτώσεις: $n = (-q_1)(-q_2)...(-q_k)p_1...p_l$.
Οπότε, μπορούμε να γράψουμε $n = s_1s_2...s_N$, όπου $s_i = -q_i$, $1 \leq i \leq k$, $s_i = p_{i-k}$,
$k+i \leq i \leq k+l = N$, $s_i \equiv 1 \pmod 4$ και όπου $s_i \equiv 1 \pmod 4$, $1 \leq i \leq N$.

$\chi_n(1+i) = \chi_{-q_1}(1+i)\cdot ... \cdot \chi_{-q_k}(1+i)\cdot \chi_{p_1}(1+i)... \cdot \chi_{p_l}(1+i) = i^{\frac{-q_1-1}{4}} \cdot ... \cdot i^{\frac{-q_k-1}{4}} \cdot i^{\frac{p_1-1}{4}} \cdot ... \cdot i^{\frac{p_l-1}{4}} =$
$= i^{\frac{s_1-1}{4}} \cdot ... \cdot i^{\frac{s_N-1}{4}} = i^{\sum_{i=1}^N \frac{s_i-1}{4}} = i^{\frac{n-1}{4}}$.
Η τελευταία ισότητα προκύπτει άμεσα από το Λήμμα της Πρότασης 2.4.7.

Συμπεραίνουμε, λοιπόν, ότι αν $n \in \mathbb{Z}$, $n \equiv 1 \pmod 4$, $n \neq 1$, τότε: $\chi_n(1+i) = i^{\frac{n-1}{4}}$.

Έστω, τώρα, $\pi = a+bi$, $(a,b)=1$ primary, ανάγωγο.
Παρατηρούμε ότι $a(1+i) = a+b+i(a+bi)$, άρα $a(1+i) \equiv a+b \pmod \pi$.
Άρα, $\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b)$.
Τώρα, αφού $\pi = a+bi$ είναι primary, ανάγωγο ισχύει ότι $a+b \equiv 1 \pmod 4$.

-Αν $a+b=1$, τότε $\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b) = \chi_\pi(1) = 1 = i^{\frac{3(a+b-1)}{4}}$.

-Αν ισχύει η ισοτιμία, αλλά όχι η ισότητα, τότε εφαρμόζοντας την Πρόταση 2.5.9 έχουμε: $\chi_\pi(a+b) = \chi_{a+b}(\pi)$.
Τώρα, $b \equiv -a \pmod{(a+b)}$, άρα $\pi = a + bi \equiv a(1-i) \equiv -ia(1+i) \pmod{(a+b)}$.
Άρα, $\chi_{a+b}(\pi) = \chi_{a+b}(-1)\chi_{a+b}(a)\chi_{a+b}(1+i)$.

Από Πρόταση 2.4.7 για $a+b \equiv 1 \pmod 4$, έχουμε $\chi_{a+b}(i) = (-1)^{\frac{n-1}{4}}$ ή $\chi_{a+b}(-1) = (-1)^{\frac{n-1}{2}} = 1$.
Επιπλέον, αφού $(a,b) = 1 \Rightarrow (a+b, a) = 1$, από Πρόταση 2.4.6 προκύπτει ότι $\chi_{a+b}(a) = 1$.
Ακόμα, πάλι από Πρόταση 2.4.7 ισχύει: $\chi_{a+b}(i) = (-1)^{\frac{a+b-1}{4}}$.
Τέλος, από το πρώτο κομμάτι της απόδειξης έχουμε ότι $\chi_{a+b}(1+i) = i^{\frac{a+b-1}{4}}$, αφού $a+b \equiv 1 \pmod 4$.

Συνθέτοντας τα αποτελέσματα, το γινόμενο θα μας δώσει πράγματι ότι $\chi_{a+b}(\pi) = i^{\frac{3(a+b-1)}{4}}$, και κατά συνέπεια $\chi_\pi(a)\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}}$.

Πρόταση 2.6.7:

Αν π primary, ανάγωγο της μορφής $\pi = a + bi$, ισχύει ότι $\chi_\pi(1+i) = i^{\frac{(a-b-b^2-1)}{4}}$.

Απόδειξη:
Αρχικά, για την απόδειξη θα χρειαστούμε και θα αποδείξουμε ένα Λήμμα.

Λήμμα: Αν $\pi = a + bi$ primary, ανάγωγο, τότε $\chi_\pi(i) = i^{\frac{-a+1}{2}}$.

Απόδειξη:
Διακρίνουμε δύο περιπτώσεις:

-Αν $\pi = -q$, όπου $q \equiv 3 \pmod 4$, $q > 0$ πρώτος, τότε εξόρισμού ισχύει ότι:
$\chi_q(i) = i^{\frac{N(q)-1}{4}} = i^{\frac{q^2-1}{4}}$.
Αλλά, $-q = a = 4k+1$, $k \in \mathbb{Z}$. Αποδεικνύεται ότι $\frac{q^2-1}{4} \equiv \frac{a-1}{2} \pmod 4$.

Άρα, $\chi_{-q}(i) = \chi_q(i) = i^{\frac{q^2-1}{4}} = i^{\frac{a-1}{2}} = (-i)^{\frac{-a+1}{2}} = (-1)^{\frac{-a+1}{2}} \cdot (i)^{\frac{-a+1}{2}} = i^{\frac{-a+1}{2}}$.

-Αν, τώρα, $\pi = a + bi$ με $N\pi = p$, όπου $p \equiv 1 \pmod 4$ πραγματικός πρώτος, τότε:
$\chi_\pi(i) = i^{\frac{N\pi-1}{4}} = i^{\frac{p-1}{4}}$ και αφού π primary υπάρχουν 2 περιπτώσεις:

1) Αν $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, τότε θυμόμαστε ότι $\frac{p-1}{4} = \frac{a^2+b^2-1}{4}$ και αποδεικνύοντας ότι $\frac{p-1}{4} \equiv \frac{a-1}{2} \pmod 4$, έχουμε ότι: $\chi_\pi(i) = i^{\frac{p-1}{4}} = i^{\frac{a-1}{2}} = (-i)^{\frac{-a+1}{2}} = i^{\frac{-a+1}{2}}$.

2) Ομοίως αν $a \equiv 3 \pmod 4$, $b \equiv 2 \pmod 4$, με παρόμοιες πράξεις αποδεικνύουμε την

ισοτιμία $\frac{p-1}{4} \equiv \frac{-a+1}{2} \pmod 4$ και έχουμε άμεσα το ζητούμενο.

Άρα, η ισότητα $\chi_\pi(i) = (-1)^{\frac{-a+1}{4}}$ ισχύει για όλα τα primary πρώτα στοιχεία π.

Πίσω στην κανονική απόδειξη, έχουμε ότι $\pi = a + bi$ primary, ανάγωγο στοιχείο στο $\mathbb{Z}[i]$.

-Αν $b = 0$, τότε $\pi = a \in \mathbb{Z}$. Αφού το π είναι primary, $\pi = -q$, $q \equiv 3 \pmod 4$, q πραγματικός πρώτος τέτοιος ώστε $a = -q,\ b = 0$.

Από Πρόταση 2.6.1, έχουμε: $\chi_\pi(1+i) = \chi_{-q}(1+i) = i^{\frac{-q-1}{4}} = i^{(a-b-b^2-1)/4}$.

-Αν $b \neq 0$ και $(a,b) = 1$, από Πρόταση 2.6.6 έχουμε: $\chi_\pi(a)\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}}$.

Τώρα, αν $\pi \equiv 1 \pmod 4$, από Πρόταση 2.6.5 a) παίρνουμε $\chi_\pi(a) = i^{\frac{a-1}{2}}$.
Με παρόμοιους υπολογισμούς με πριν έχουμε, τελικά, $\chi_\pi(a)^{-1} = i^{\frac{a-1}{2}}$ και άρα $\chi_\pi(1+i) = i^{\frac{a+3b-1}{4}}$, το οποίο αποδεικνύουμε ότι είναι ισότιμο mod4 με το $\frac{a-b-b^2-1}{4}$.

Τέλος, αν $\pi \equiv 3 + 2i$, από το b) της Πρότασης 2.6.5 θα πάρουμε ότι $\chi_\pi(a) = -i^{\frac{-a-1}{2}}$, άρα $\chi_\pi(a)^{-1} = i^{\frac{a-3}{2}}$ και τελικά $\chi_\pi(1+i) = i^{\frac{5a+3b-9}{4}}$.
Ο εκθέτης αυτός θα βγει ισότιμος mod4 με τον εκθέτη της Πρότασης και, επομένως, καταλήγουμε να έχουμε το επιθυμητό αποτέλεσμα σε όλες τις δυνατές περιπτώσεις.

Ο τετραδικός χαρακτήρας του 2

Σκοπός μας είναι να υπολογίσουμε τον $\chi_\pi(2)$ για $\pi = a + bi$ primary πρώτο.

Έστω $p \equiv 1 \pmod 4$ τέτοιος ώστε $p = N(\pi)$.

Θα δείξουμε πρώτα ότι $\chi_\pi(2) = i^{\frac{ab}{2}}$.

Αφού $2 = i^3(1+i)^2$, συνδυαστικά οι Προτάσεις 2.6.7 και το Λήμμα της ίδιας Πρότασης μας δίνουν: $\chi_\pi(2) = \chi_\pi(i)^3\chi_\pi(1+i)^2 = i^{\frac{3(-a+1)}{2}} \cdot i^{\frac{a-b-b^2-1}{2}} = i^{1-a-(b+1)\frac{b}{2}}$.

Αφού το π είναι primary, ένας γρήγορος έλεγχος μας δίνει ότι $a \equiv b+1 \equiv -b+1 \pmod 4$.

Άρα, $1 - a - (b+1)\frac{b}{2} \equiv -b - (b+1)\frac{b}{2} \equiv \frac{b}{2}(-3-b) \equiv \frac{b}{2}(-b+1) \equiv \frac{ab}{2} \pmod 4$, και έχουμε το αποτέλεσμα.

-Θα δείξουμε, τώρα, ότι το p είναι της μορφής $p = A^2 + 64B^2$ αν και μόνο αν $p \equiv 1 \pmod 4$ και αν η ισοτιμία $x^4 \equiv 2 \pmod p$ έχει λύση για $x \in \mathbb{Z}$.

($\Rightarrow$) Αν $p = A^2 + 64B^2 = A^2 + (8B)^2$, τότε ο πρώτος αριθμός p γράφεται σαν άθροισμα δύο τετραγώνων και $p \neq 2$. Άρα, από βασική Θεωρία Αριθμών, $p \equiv 1 \pmod 4$.

Αφού $p = A^2 + 64B^2$, ο Α είναι περιττός ($A \equiv \pm 1 \pmod 4$).
Θέτουμε $b = 8B$ και $a = A$ αν $A \equiv 1 \pmod 4$ ή $a = -A$ αν $A \equiv -1 \pmod 4$.
Τότε, το $\pi = a + bi$ είναι τέτοιο ώστε $N(\pi) = a^2 + b^2 = p$, όπου $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$.
Άρα, το π είναι primary πρώτος και άρα από το πρώτο σκέλος ισχύει:

$$\chi_\pi(2) = i^{\frac{ab}{2}} = i^{\pm 4AB} = 1.$$

Επομένως, υπάρχει ένα $a \in \mathbb{Z}[i]$ τέτοιο ώστε $2 \equiv a^4 \pmod \pi$.
Αφού $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ είναι το σύνολο των κλάσεων των $0, 1, ..., p-1$, υπάρχει ένα $x \in \mathbb{Z}$ τέτοιο ώστε $x \equiv a \pmod \pi$ τέτοιο ώστε $2 \equiv x^4 \pmod \pi$.

Τότε, $p = N(\pi) | N(x^4 - 2) = (x^4 - 2)^2$ και άρα $p | (x^4 - 2)$. Με άλλα λόγια, $2 \equiv x^4 \pmod p$.

($\Leftarrow$) Υποθέτουμε, τώρα, ότι $p \equiv 1 \pmod 4$ και ότι το 2 είναι τετραδικό υπόλοιπο modp.
Αφού $p \equiv 1 \pmod 4$, τότε $p = \pi\overline{\pi}$, όπου $\pi = a + bi$ είναι ένα primary πρώτο στοιχείο.
Αφού $2 \equiv x^4 \pmod p$ για κάποιο $x \in \mathbb{Z}$, ισχύει και $2 \equiv x^4 \pmod \pi$ και άρα $\chi_\pi(2) = 1$.

Επιπλέον, $1 = \chi_\pi(2) = i^{\frac{ab}{2}}$.
Αφού το a είναι περιττό (π primary), θα πρέπει $8|b$, διότι ο χαρακτήρας μας έχει τάξη 4. Έτσι, προκύπτει η μορφή $p = A^2 + 64B^2$, όπου $A = a$, $B = \frac{b}{8}$ και καταλήγουμε στο συμπέρασμα.

3 Ο Κυβικός Νόμος Αντιστροφής

3.1 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 Norm του στοιχείου α μέσω του τύπου $N\alpha = \alpha\overline{\alpha} = a^2 - ab + b^2$, όπου $\overline{\alpha}$ το συζυγές του α. Γνωρίζουμε ότι $\mathbb{Z}[\omega]$ είναι δακτύλιος μονοσήμαντης ανάλυσης (εφόσον είναι και Ευκλείδεια περιοχή με απεικόνιση τη Norm). Αυτό που θα μας απασχολήσει, αρχικά, είναι η μελέτη των μονάδων και των πρώτων στοιχείων του δακτυλίου.

Πρόταση 3.1.1:

$\alpha \in \mathbb{Z}[\omega]$ είναι μονάδα αν και μόνο αν $N\alpha = 1$. Οι μονάδες στο $\mathbb{Z}[\omega]$ είναι οι: $1, -1, \omega, -\omega, \omega^2, -\omega^2$.

Απόδειξη:
Αν $N\alpha = 1 \Rightarrow \alpha\overline{\alpha} = 1$ που συνεπάγεται ότι το α είναι μονάδα αφού $\overline{\alpha} \in \mathbb{Z}[\omega]$.

Αν το α είναι μονάδα, υπάρχει ένα $\beta \in \mathbb{Z}[\omega]$ τέτοιος ώστε $\alpha\beta = 1$. Άρα, $N\alpha N\beta = 1$.
Αφού $N\alpha, N\beta$ είναι θετικοί ακέραιοι, παρατηρώντας τον γενικό τύπο της Norm,
έχουμε ότι $N\alpha = 1$.

Τώρα, υποθέτουμε ότι $\alpha = a + b\omega$ είναι μονάδα. Τότε, $1 = a^2 - ab + b^2$ ή $4 = (2a - b)^2 + 3b^2$.
Υπάρχουν δύο πιθανότητες:
a) $2a - b = \pm 1,\ b = \pm 1$
b) $2a - b = \pm 2,\ b = 0$.
Λύνοντας αυτά τα 6 ζεύγη εξισώσεων, καταλήγουμε στα αποτελέσματα $1,\ -1,\ \omega,\ -\omega,$
$-1 - \omega,\ 1 + \omega$. Αφού $\omega^2 + \omega + 1 = 0$ τα δύο τελευταία στοιχεία είναι τα $\omega^2,\ -\omega^2$.

Για να μελετήσουμε τους πρώτους στον δακτύλιο είναι σημαντικό να καταλάβουμε ότι οι πρώτοι στο $\mathbb{Z}$ δεν είναι απαραίτητα πρώτοι στον $\mathbb{Z}[\omega]$. Παραδείγματος χάρη
$7 = (3 + \omega) \cdot (2 - \omega)$. Γιάυτόν τον λόγο, θα αναφέρουμε πλέον τους πρώτους του $\mathbb{Z}$ με τον όρο ρητοί πρώτοι και τους πρώτους του $\mathbb{Z}[\omega]$ απλά πρώτους.

Πρόταση 3.1.2:

Αν το π είναι πρώτος του δακτυλίου, τότε υπάρχει ένας ρητός πρώτος p τέτοιος ώστε

$N\pi = p$ ή $N\pi = p^2$. Στην πρώτη περίπτωση το π δεν είναι συνεταιρικό με έναν ρητό πρώτο, ενώ στην δεύτερη περίπτωση το π είναι συνεταιρικό με το p.

Απόδειξη:
Έχουμε ότι $N\pi = n > 1$ ή $\pi\overline{\pi} = n$. Το n είναι γινόμενο ρητών πρώτων. Άρα, $\pi | p$ για κάποιον ρητό πρώτο p. Αν $p = \pi\gamma,\ \gamma \in \mathbb{Z}[\omega]$, τότε $N\pi N\gamma = Np = p^2$. Άρα, είτε $N\pi = p^2$ και $N\gamma = 1$ είτε $N\pi = p$.
Στην πρώτη περίπτωση, το γ είναι μονάδα και άρα το π είναι συνεταιρικό με το p. Στην δεύτερη περίπτωση, αν ήταν $\pi = uq$, όπου u μονάδα, τότε θα ήταν $p = N\pi = NuNq = q^2$, πράγμα που δεν έχει νόημα. Άρα, το π δεν είναι συνεταιρικό με κάποιον ρητό πρώτο.

Πρόταση 3.1.3:

Αν $\pi \in \mathbb{Z}[\omega]$ είναι τέτοιο ώστε $N\pi = p$, όπου p ρητός πρώτος, τότε το π είναι πρώτο στον $\mathbb{Z}[\omega]$.

Απόδειξη:
Αν το π δεν είναι πρώτος στον δακτύλιο, τότε θα μπορούσαμε να γράψουμε $\pi = m\gamma$ με $Nm,\ N\gamma > 1$. Τότε, $p = NmN\gamma$, που δεν μπορεί να αληθεύει, αφού ο p είναι πρώτος στο $\mathbb{Z}$. Άρα, το π είναι πρώτο στον δακτύλιο $\mathbb{Z}[\omega]$.

-Η παρακάτω πρόταση προσδιορίζει τους πρώτους στον $\mathbb{Z}[\omega]$.

Πρόταση 3.1.4:

Έστω p και q ρητοί πρώτοι. Αν $q \equiv 2 \pmod 3$, τότε ο q είναι πρώτος στον $\mathbb{Z}[\omega]$.
Αν $p \equiv 1 \pmod 3$, τότε $p = \pi\overline{\pi}$, όπου π είναι ένας πρώτος (ανάγωγο στοιχείο) του $\mathbb{Z}[\omega]$.
Τέλος, $3 = -\omega^2(1-\omega)^2$ και $1-\omega$ είναι πρώτος στον $\mathbb{Z}[\omega]$.

Απόδειξη:
Ας υποθέσουμε ότι ο p δεν είναι πρώτος στον $\mathbb{Z}[\omega]$. Τότε, $p = \pi\gamma$, με $N\pi,\ N\gamma > 1$.
Άρα, $p^2 = N\pi N\gamma$ και $N\pi = p$. Έστω $\pi = a + b\omega$. Τότε, $p = a^2 - ab + b^2$ ή $4p = (2a-b)^2 + 3b^2 \Rightarrow$ $p \equiv (2a-b)^2 \pmod 3$. Επειδή εξαιρούμε προς το παρόν το 3, έχουμε ότι $3 \nmid p$ και άρα $p \equiv 1 \pmod 3$, αφού το 1 είναι το μόνο μη μηδενικό τετράγωνο mod3.
Καταλήγουμε στο συμπέρασμα ότι αν ο ρητός πρώτος p δεν είναι πρώτος στον $\mathbb{Z}[\omega]$, τότε είναι αναγκαστικά $p \equiv 1 \pmod 3$.
Άμεση συνέπεια είναι ότι αν $p \equiv 2 \pmod 3$, τότε ο p είναι πρώτος στον $\mathbb{Z}[\omega]$.

Έστω τώρα πάλι $p \equiv 1 \pmod 3$. Από το Νόμο Τετραγωνικής Αντιστροφής θα έχουμε:

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

Επομένως, υπάρχει $a \in \mathbb{Z}$ τέτοιο ώστε $a^2 \equiv -3 \pmod p$ ή $pb = a^2 + 3$ για κάποιο $b \in \mathbb{Z}$.
Άρα, το p διαιρεί το $(a + \sqrt{-3}) \cdot (a - \sqrt{-3}) = (a + 1 + 2\omega) \cdot (a - 1 - 2\omega)$. Αν το p ήταν πρώτος στον $\mathbb{Z}[\omega]$ θα έπρεπε να διαιρεί κάποιον από τους παράγοντες, αλλά αυτό δεν μπορεί να συμβαίνει αφού αν διαιρούσε π.χ. τον πρώτο παράγοντα, θα έπρεπε να έχουμε $a + 1 + 2\omega = p \cdot (n + m\omega)$ για $n + m\omega \in \mathbb{Z}[\omega]$.
Θα είχαμε, δηλαδή, από αντιστοιχία ότι $2 = p \cdot m$, πράγμα άτοπο, αφού $p,\ m \in \mathbb{Z}$ και $p > 2$. Εντελώς ανάλογα, αποκλείουμε και την περίπτωση να διαιρεί τον δεύτερο παράγοντα. Άρα, καταλήγουμε στο ότι ο p δεν είναι πρώτος στον $\mathbb{Z}[\omega]$ και γράφεται ως $p = \pi \cdot \gamma$ με τα π και γ να μην είναι μονάδες. Παίρνοντας Norm έχουμε $p^2 = N\pi N\gamma$, οπότε πρέπει $p = N\pi = \pi\overline{\pi}$.

Για την τελευταία περίπτωση, τώρα, έχουμε ότι:
$x^3 - 1 = (x-1) \cdot (x-\omega) \cdot (x-\omega^2) \Rightarrow x^2 + x + 1 = (x-\omega) \cdot (x-\omega^2)$.
Θέτοντας $x = 1$ παίρνουμε $3 = (1-\omega) \cdot (1-\omega^2) = (1+\omega) \cdot (1-\omega)^2 = \omega^2 \cdot (1-\omega)^2$.
Παίρνοντας Norm έχουμε: $9 = N(1-\omega)^2 \Rightarrow 3 = N(1-\omega)$.
Άρα, το $1 - \omega$ είναι πρώτος στον δακτύλιο $\mathbb{Z}[\omega]$ (Πρόταση 3.1.3).

3.2 Ο κυβικός χαρακτήρας υπολοίπων

Πρόταση 3.2.1:

Έστω $\pi \in \mathbb{Z}[\omega]$ ένα πρώτο στοιχείο. Τότε, $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ είναι ένα πεπερασμένο σώμα με $N\pi$ στοιχεία.

Παρατήρηση: Έστω π ένα πρώτο στοιχείο. Τότε, η πολλαπλασιαστική ομάδα του $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ έχει τάξη $N\pi - 1$. Άρα, έχουμε μια αναλογία του Μικρού Θεωρήματος του Fermat.

Πρόταση 3.2.2:

Αν $\pi \nmid \alpha$, τότε $\alpha^{N\pi-1} \equiv 1 \pmod \pi$.

Παρατηρήσεις:
Αν η *Norm* του π είναι διαφορετική του 3 (που είναι η περίπτωση που εξετάζουμε ξεχωριστά κάθε φορά), τότε οι κλάσεις υπολοίπων $1,\ \omega,\ \omega^2$ είναι διακριτές στον $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$. Για να το δούμε αυτό, ας υποθέσουμε π.χ. ότι $\omega \equiv 1 \pmod{\pi}$. Τότε, $\pi|(1-\omega)$ και αφού όπως είδαμε $1-\omega$ είναι πρώτος, τα π και $1-\omega$ είναι συνεταιρικά στοιχεία. Άρα, $N\pi = N(1-\omega) = 3$, πράγμα άτοπο. Οι άλλες περιπτώσεις βγαίνουν παρόμοια.

Αφού $1,\ \omega,\ \omega^2$ είναι μια κυκλική ομάδα τάξης 3, έπεται ότι το 3 διαιρεί την τάξη της $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$, δηλαδή $3|(N\pi - 1)$. Αυτό μπορούμε να το δούμε διαφορετικά χρησιμοποιώντας την Πρόταση 3.1.4. Αν $\pi = q$ ένας ρητός πρώτος, τότε $N\pi = q^2 \equiv 1 \pmod{3}$. Αν το π είναι τέτοιο ώστε $N\pi = p$, τότε $p \equiv 1 \pmod{3}$.

Πρόταση 3.2.3

Έστω ένα πρώτο στοιχείο π τέτοιο ώστε $N\pi \neq 3$ και $\pi \nmid \alpha$. Τότε, υπάρχει μοναδικός ακέραιος $m = 0, 1, 2$ τέτοιος ώστε $\alpha^{\frac{N\pi-1}{3}} \equiv \omega^m \pmod{\pi}$.

Απόδειξη:
Γνωρίζουμε ότι το π διαιρεί το $\alpha^{N\pi-1} - 1$.

Έχουμε: $\alpha^{N\pi-1} - 1 = (\alpha^{\frac{N\pi-1}{3}} - 1) \cdot (\alpha^{\frac{N\pi-1}{3}} - \omega) \cdot (\alpha^{\frac{N\pi-1}{3}} - \omega^2)$.

Αφού το π είναι πρώτο, πρέπει να διαιρεί ένας από τους τρεις παράγοντες στα δεξιά. Από την προηγούμενη παρατήρηση θα διαιρεί ακριβώς έναν από τους παράγοντες, αφού αν διαιρούσε δύο παράγοντες θα διαιρούσε και τη διαφορά τους, πράγμα άτοπο (όπως το δείξαμε συγκεκριμένα στην περίπτωση $\pi|(1-\omega)$ με τις άλλες περιπτώσεις να αποδεικνύονται ανάλογα).

Έχουμε, λοιπόν, τον παρακάτω ορισμό:

Ορισμός:

Αν $N\pi \neq 3$, ο κυβικός χαρακτήρας του α modp δίνεται από:

a) $\left(\frac{\alpha}{\pi}\right)_3 = 0$ αν $\pi|\alpha$

b) $\alpha^{\frac{N\pi-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$ που ισούται με $1,\ \omega$ ή ω^2.

Πρόταση 3.2.4:

Ισχύουν οι ακόλουθες προτάσεις:

a) $\left(\frac{\alpha}{\pi}\right)_3 = 1$ αν και μόνο αν η ισοτιμία $x^3 \equiv \alpha \pmod{\pi}$ είναι επιλύσιμη, ή αλλιώς αν και μόνο αν α είναι κυβικό υπόλοιπο.

b) $\alpha^{\frac{N\pi-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$

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

d) Αν $\alpha \equiv \beta \pmod{\pi}$, τότε $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Για λόγους ευκολίας σε αυτό το κεφάλαιο θα συμβολίζουμε τον κυβικό χαρακτήρα

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

Πρόταση 3.2.5:

Έστω $\alpha \in \mathbb{Z}[\omega]$ και p πρώτος του $\mathbb{Z}[\omega]$. Ισχύουν οι παρακάτω προτάσεις:
a) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$

b) $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\alpha)$.

Απόδειξη:
a) $\chi_\pi(\alpha)$ είναι εξ΄ ορισμού $1, \omega$ ή ω^2 και καθένας από αυτούς τους αριθμούς στο τετράγωνο είναι ίσος με τον συζυγή του.

b) $\alpha^{\frac{N\pi-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi}$ και παίρνοντας συζυγίες θα έχουμε: $\overline{\alpha}^{\frac{N\pi-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$.
Αφού $N\overline{\pi} = N\pi$, έπεται ότι $\chi_{\overline{\pi}}(\overline{\alpha}) \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$ και άρα $\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\chi_\pi(\alpha)}$.

Πόρισμα 3.2.6:

$\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$ και $\chi_q(n) = 1$ αν το n ρητός ακέραιος τέτοιος ώστε $(n, q) = 1$, όπου q είναι πρώτος ($q \equiv 2 \pmod{3}$).

Απόδειξη:
Αφού $\overline{q} = q$, έχουμε $\chi_q(\overline{\alpha}) = \chi_{\overline{q}}(\overline{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$. Αυτό μας δίνει την πρώτη σχέση.

Αφού $\overline{n} = n$, έχουμε $\chi_q(n) = \overline{\chi_q(n)} = \chi_q(n)^2$. Αφού $\chi_q(n) \neq 0$, εφόσον $(n, q) = 1$, έπεται ότι $\chi_q(n) = 1$.

Παρατήρηση: Από το Πόρισμα συμπεραίνουμε ότι το n είναι κυβικό υπόλοιπο mod q. Άρα, αν $q_1 \neq q_2$ είναι δύο πρώτοι ισότιμοι με 2 mod3, τότε έχουμε τετριμμένα ότι $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$. Αυτή είναι μία ειδική περίπτωση του κυβικού νόμου αντιστροφής.

3.3 Primary πρώτοι

Για να διατυπώσουμε τον γενικό νόμο χρειαζόμαστε πάλι την ιδέα των primary πρώτων στοιχείων.

Ορισμός:

Αν π πρώτος στον $\mathbb{Z}[\omega]$, λέμε ότι το π είναι primary αν $\pi \equiv 2 \pmod 3$.
Αν $\pi = q$ είναι πραγματικός, δεν έχουμε κάτι καινούριο.
Αν $\pi = a + b\omega$ είναι μιγαδικός πρώτος, ο ορισμός είναι ισοδύναμος με $a \equiv 2 \pmod 3$ και $b \equiv 0 \pmod 3$.

-Χρειαζόμαστε κάποιο "primary" στοιχείο για να εξαλείψουμε το πρόβλημα ότι για κάθε μη μηδενικό στοιχείο του δακτυλίου έχουμε 6 συνεταρικά στοιχειά, τα οποία έχουν ανάλογη συμπεριφορά.

Πρόταση 3.3.1:

Έστω $N\pi = p \equiv 1 \pmod 3$. Από όλα τα συνεταιρικά στοιχεία του π ακριβώς ένα είναι primary.

Απόδειξη:
Γράφουμε $\pi = a + b\omega$. Οι συνεταιρικοί του π είναι οι: $\pi,\ \omega\pi,\ \omega^2\pi,\ -\pi,\ -\omega\pi,\ -\omega^2\pi$.
Τα στοιχεία αυτά είναι τα παρακάτω:
$a)\ a + b\omega$
$b)\ -b + (a - b)\omega$
$c)\ (b - a) - a\omega$

$d)\ -a-b\omega$
$e)\ b+(b-a)\omega$
$f)\ (a-b)+a\omega.$
Αφού $p=a^2-ab+b^2$, δεν μπορούν ταυτόχρονα τα a,b να διαιρούνται από 3 (γιατί $3\nmid p$). Εν τέλει, οι δυνατότητες που θα έχουμε για τα ζεύγη των (a,b) θα είναι:
$(a,b)\equiv(0,1),(0,2),(1,0),(1,1),(2,0),(2,2)$.
Σε κάθε μια από αυτές τις έξι πιθανές τιμές, ένας γρήγορος έλεγχος δείχνει ότι υπάρχει ακριβώς ένα συνεταιρικό στοιχείο του π το οποίο είναι $\equiv 2 \pmod 3$.

3.4 Ο Νόμος Κυβικής Αντιστροφής

Στόχος μας σε αυτήν την ενότητα είναι να αποδείξουμε το ακόλουθο σημαντικό Θεώρημα:

Θεώρημα 3.4.1: Ο Νόμος Κυβικής Αντιστροφής [[5] Κεφάλαιο 9 παράγραφος 4]

Έστω π_1,π_2 primary με $N\pi_1,N\pi_2\neq 3$ και $N\pi_1\neq N\pi_2$. Τότε $\chi_{\pi_1}(\pi_2)=\chi_{\pi_2}(\pi_1)$.

Παρατηρήσεις:
-Πριν δωθεί η απόδειξη του νόμου, είναι σημαντικό να γίνουν κάποιες παρατηρήσεις πάνω σε αυτόν.
1) Υπάρχουν τρεις περιπτώσεις που πρέπει να λάβουμε υπόψιν. Συγκεκριμένα, αν τα π_1,π_2 είναι και τα δύο πραγματικοί, αν είναι και τα δύο μιγαδικοί ή αν είναι ο ένας πραγματικός και ο άλλος μιγαδικός. Η πρώτη περίπτωση έχει μελετηθεί ήδη (Παρατήρηση Πορίσματος 3.2.6).
2) Ο κυβικός χαρακτήρας των μονάδων μπορεί να αντιμετωπιστεί ως ακολούθως:
Αφού $-1=(-1)^3$, έχουμε $\chi_\pi(-1)=1$ για όλους τους πρώτους π. Επίσης, από το b) της Πρότασης 3.2.4 έχουμε: $\chi_\pi(\omega)=\omega^{\frac{N\pi-1}{3}}$. Άρα, $\chi_\pi(\omega)=1,\ \omega$ ή ω^2 ανάλογα με το αν η Norm του π είναι 1,4 ή 7 modulo 9.
3) Ο πρώτος $1-\omega$ φαίνεται να έχει ιδιαίτερη δυσκολία. Αν είχαμε $N\pi\neq 3$ θα θέλαμε να υπολογίσουμε τον $\chi_\pi(1-\omega)$. Η περίπτωση αυτή θίγεται στο επόμενο Θεώρημα.

Θεώρημα 3.4.2:

Έστω $N\pi\neq 3$. Αν $\pi=q$ είναι πραγματικός, γράφουμε $q=3m-1$. Αν $\pi=a+b\omega$ είναι primary, γράφουμε $a=3m-1$. Τότε $\chi_\pi(1-\omega)=\omega^{2m}$.

Απόδειξη:
Δίνουμε μια απόδειξη για την περίπτωση ρητού πρώτου q.
Αφού $(1-\omega)^2 = -3\omega$, έχουμε $\chi_q(1-\omega)^2 = \chi_q(-3)\cdot\chi_q(\omega)$.
Από το Πόρισμα 3.2.6 ξέρουμε ότι $\chi_q(-3) = 1$. Ισχύει $\chi_q(\omega) = \omega^{(Nq-1)/3} = \omega^{(q^2-1)/3}$.
Άρα, συνολικά, $\chi_q(1-\omega)^2 = \omega^{q^2-1/3}$.
Υψώνοντας και τα δύο μέλη στο τετράγωνο προκύπτει ότι $\chi_q(1-\omega) = \omega^{(2/3)(q^2-1)}$.
Τώρα, $q^2-1 = 9m^2-6m$ και άρα $\frac{2}{3}(q^2-1) \equiv -4m \equiv 2m \pmod 3$. Η ισότητα έπεται.

Κυβικός Νόμος Αντιστροφής:

-Έστω π ένας μιγαδικός πρώτος τέτοιος ώστε $N\pi = p \equiv 1 \pmod 3$. Αφού $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ είναι πεπερασμένο σώμα χαρακτηριστικής p, περιέχει ένα αντίγραφο του $\mathbb{Z}/p\mathbb{Z}$.
Και τα δύο ($\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, $\mathbb{Z}/p\mathbb{Z}$) έχουν p στοιχεία. Άρα μπορούμε να ταυτίσουμε τα δύο σώματα.
Η ταύτιση αυτή μας επιτρέπει να θεωρήσουμε Gauss sums και Jacobi sums στον $\mathbb{Z}/p\mathbb{Z}$. Συγκεκριμένα, θεωρούμε τον κυβικό χαρακτήρα χ_π στον $\mathbb{Z}/p\mathbb{Z}$ και δουλεύουμε με τα Gauss sums $g_a(\chi_\pi)$ και Jacobi sums $J(\chi_\pi,\chi_\pi)$.

Αν χ κυβικός χαρακτήρας, έχουμε αποδείξει από Πόρισμα 2.2.8 και Πρόταση 2.2.9 ότι:
a) $g(\chi)^3 = pJ(\chi,\chi)$
b) Αν $J(\chi,\chi) = a+b\omega$, τότε $a \equiv -1 \pmod 3$ και $b \equiv 0 \pmod 3$.
Αφού $J(\chi,\chi)\overline{J(\chi,\chi)} = p$, από τη δεύτερη υπόθεση έχουμε ότι το $J(\chi,\chi)$ είναι primary πρώτο στον $\mathbb{Z}[\omega]$ με Norm p.

Υποθέτουμε ότι το π είναι primary.

Λήμμα 3.4.3:

Ισχύει: $J(\chi_\pi,\chi_\pi) = \pi$

Απόδειξη:
Έστω $J(\chi_\pi,\chi_\pi) = \pi'$.
Αφού $\pi\overline{\pi} = p = \pi'\overline{\pi'}$, έχουμε $\pi|\pi'$ ή $\pi|\overline{\pi'}$. Αφού όλοι οι πρώτοι που εμπλέκονται είναι primary, πρέπει να έχουμε $\pi = \pi'$ ή $\pi = \overline{\pi'}$. Θα θέλαμε να αποκλείσουμε τη δεύτερη πιθανότητα.
Από τους ορισμούς:
$J(\chi_\pi,\chi_\pi) = \sum_x \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_x x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \pmod\pi$, όπου το άθροισμα είναι πάνω από τα στοιχεία του $\mathbb{Z}/p\mathbb{Z}$.
Το πολυώνυμο $x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}}$ είναι βαθμού $\frac{2}{3}(p-1) < p-1$. Τώρα, από Πρόταση που έχουμε αποδείξει και παλαιότερα ισχύει ότι:

$1^k + 2^k + ... + (p-1)^k \equiv 0 \pmod{p}$ αν $(p-1) \nmid k$ και $-1 \pmod{\pi}$ αν $(p-1)|k$.

Στη δικιά μας περίπτωση $(p-1) \nmid (\frac{p-1}{3})$ και έχουμε $\sum_x x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \equiv 0 \pmod{p}$.
Αυτό δείχνει ότι $J(\chi_\pi,\chi_\pi) \equiv 0 \pmod{\pi}$, δηλαδή ότι $\pi|\pi'$ και άρα $\pi = \pi'$.

-Υπενθυμίζουμε ότι π είναι ένας μιγαδικός πρώτος του δακτυλίου $\mathbb{Z}[\omega]$ τέτοιος ώστε: $N\pi = p \equiv 1 \pmod{3}$.

Πόρισμα 3.4.4:

Ισχύει: $g(\chi_\pi)^3 = p\pi$.

Απόδειξη:
Από την Παρατήρηση *a*) και το Λήμμα 3.4.3, έπεται ότι $g(\chi_\pi)^3 = pJ(\chi_\pi,\chi_\pi) = p\pi$.

-Μπορούμε τώρα να αποδείξουμε τον κυβικό Νόμο Αντιστροφής.

Πρώτα θεωρούμε την περίπτωση όπου $\pi_1 = q \equiv 2 \pmod{3}$ και $\pi_2 = \pi$ με $N\pi = p$.
Υψώνοντας και τα δύο μέλη της $g(\chi_\pi)^3 = p\pi$ εις την $(q^2-1)/3$, παίρνουμε:

$$g(\chi_\pi)^{q^2-1} = (p\pi)^{(q^2-1)/3}.$$

Παίρνοντας ισοτιμίες modulo$q$ παρατηρούμε ότι $g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi) \pmod{q}$, αφού $\chi_q(p) = 1$ έχουμε:

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)g(\chi_\pi) \pmod{q} \quad (1)$$

Αναλύοντας, τώρα, το αριστερό μέλος παίρνουμε:

$$g(\chi_\pi)^{q^2} = (\sum \chi_\pi(t)\zeta^t)^{q^2} \equiv \sum \chi_\pi(t)^{q^2}\zeta^{q^2t} \pmod{q}.$$

Αφού $q^2 \equiv 1 \pmod{3}$ και $\chi_\pi(t)$ είναι μία κυβική ρίζα της μονάδας, έχουμε:

$$g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi) \pmod{q} \quad (2)$$

Από την Πρόταση 2.2.1 έχουμε: $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$.

Τώρα, συνδυάζοντας τις (1),(2) παίρνουμε:

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

Πολλαπλασιάζοντας και τα δύο μέλη με $\overline{g(\chi_\pi)}$ και αφού $g(\chi_\pi)\overline{g(\chi_\pi)} = p$, έχουμε:
$\chi_\pi(q)p \equiv \chi_q(\pi)p \pmod q \Rightarrow \chi_\pi(q) \equiv \chi_q(\pi) \pmod q$ (αφού $(p,q) = 1$)
και άρα $\chi_\pi(q) = \chi_q(\pi)$, (αφού είναι και τα δύο 3-ρίζες της μονάδας και άρα δεν είναι μόνο ισότιμες, αλλά θα είναι και ίσες).
Έχουμε, λοιπόν, τον Νόμο Αντιστροφής για την περίπτωση αυτή!
-Μένει να θεωρήσουμε την περίπτωση δύο μιγαδικών πρώτων π_1, π_2, όπου
$N\pi_1 = p_1 \equiv 1 \pmod 3$ και $N\pi_2 = p_2 \equiv 1 \pmod 3$. Αυτή η περίπτωση μπορεί να χειριστεί με παρόμοια τεχνική, αλλά με λίγο πιο δύσκολο τρόπο.
Έστω $\gamma_1 = \overline{\pi_1}$ και $\gamma_2 = \overline{\pi_2}$. Τότε, τα γ_1, γ_2 είναι primary και $p_1 = \pi_1\gamma_1$ και $p_2 = \pi_2\gamma_2$.
Ξεκινώντας από τη σχέση $g(\chi_{\gamma_1})^3 = p_1\gamma_1$, υψώνοντας εις την $(N\pi_2 - 1)/3 = (p_2 - 1)/3$ και παίρνοντας συζυγίες $mod\pi_2$ προκύπτει με τη μέθοδο που δουλέψαμε και πριν η σχέση:

$$\chi_{\gamma_1}(p_2^2) \equiv \chi_{\pi_2}(p_1\gamma_1) \ (3).$$

Συγκεκριμένα,συνδυάζοντας τις σχέσεις:

$g(\chi_{\gamma_1})^{(p_2-1)} = (p_1\gamma_1)^{(p_2-1)/3} \Rightarrow g(\chi_{\gamma_1})^{p_2-1} \equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}$

$\Rightarrow g(\chi_{\gamma_1}))^{p_2} \equiv \chi_{p_2}(\pi_1\gamma_1)g(\chi_{\gamma_1}) \pmod{\pi_2}$ (4)

$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}({p_2}^2)g(\chi_{\gamma_1}) \pmod{p_2}$ ή $g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \pmod{\pi_2}$ (5) (Πρόταση 2.2.1)

Συνδυάζοντας τις (4),(5) έχουμε:
$\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \pmod{\pi_2}$
$\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1})\overline{g(\chi_{\gamma_1})} \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1})\overline{g(\chi_{\gamma_1})} \pmod{\pi_2}$

$\chi_{\gamma_1}(p_2^2)p_1 \equiv \chi_{\pi_2}(p_1\gamma_1)p_1 \pmod{\pi_2}$

$\chi_{\gamma_1}(p_2^2) \equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}$

$\Rightarrow \chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1)$ $(*)$
(Έχουμε χρησιμοποιήσει ότι από Πρόταση 2.2.2 ισχύει ότι $|g(\chi_{\gamma_1})|^2 = p_1$.)

Ομοίως ξεκινώντας από την $g(\chi_{\pi_2})^3 = p_2\pi_2$, υψώνοντας εις την $(p_1 - 1)/3$ και παίρνοντας συζυγίες $mod\pi_1$ καταλήγουμε:

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\gamma_2) \ (**)$$

Χρειαζόμαστε, ακόμα, τη σχέση $\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2)$, το οποίο έπεται από την Πρόταση 3.2.5, αφού $\gamma_1 = \overline{\pi_1}$ και $\overline{p_2} = p_2$. Τώρα υπολογίζουμε:

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) = \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) \ (\text{από } *)$$

$$= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(p_2\pi_2)$$

$$= \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\gamma_1) \text{ (από **)}$$

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

Εξισώνοντας τον πρώτο με τον τελευταίο όρο και απλοποιώντας με $\chi_{\pi_2}(p_1\gamma_1)$ παίρνουμε, τελικά, το αποτέλεσμα:

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

3.5 Ο κυβικός χαρακτήρας του 2

Αυτό που πραγματευόμαστε σε αυτήν την ενότητα είναι να μελετήσουμε για ποια πρώτα στοιχεία π του $\mathbb{Z}[\omega]$ θα ισχύει ότι το 2 είναι κυβικό υπόλοιπο modπ.
Ξεκινάμε παρατηρώντας ότι η $x^3 \equiv 2 \pmod{\pi}$ είναι επιλύσιμη αν και μόνο αν $x^3 \equiv 2 \pmod{\pi'}$ για κάποιο π' συνεταιρικό του π.
Μπορούμε, άρα, να υποθέσουμε ότι το π είναι primary.

-Αν έχουμε $\pi = q$, όπου $q \equiv 2 \pmod 3$, δηλαδή αν ισχύει ότι το π είναι ένας ρητός πρώτος, τότε $\chi_q(2) = 1$ και άρα το 2 είναι ένα κυβικό υπόλοιπο για όλους τους πρώτους αυτής της μορφής. Αυτό προκύπτει ως μια απλή παρατήρηση του δεύτερου μέρους του Πορίσματος 3.2.6, εφόσον ισχύει ότι $(2, q) = 1$, υποθέτοντας εξ' αρχής ότι το q είναι διάφορο του 2.

-Υποθέτουμε, λοιπόν, από εδώ και πέρα ότι $\pi = a + b\omega$ είναι ένας primary μιγαδικός πρώτος. Από τον νόμο κυβικής αντιστροφής έχουμε $\chi_2(\pi) = \chi_\pi(2)$.

Η Norm του 2 είναι $2^2 = 4$.

$$\text{Άρα: } \pi = \pi^{\frac{4-1}{3}} \equiv \chi_2(\pi) \pmod 2.$$

Έπεται ότι $\chi_\pi(2) = 1$ αν και μόνο αν $\pi \equiv 1 \pmod 2$ και άρα έχουμε σαν συμπέρασμα την ακόλουθη Πρόταση.

Πρόταση 3.5.1:

Η ισοτιμία $x^3 \equiv 2 \pmod{\pi}$ είναι επιλύσιμη αν και μόνο αν $\pi \equiv 1 \pmod 2$, δηλαδή αν και μόνο αν $a \equiv 1 \pmod 2$ και $b \equiv 0 \pmod 2$.

-Η παραπάνω Πρόταση μπορεί να διατυπωθεί και με έναν διαφορετικό τρόπο:

Έστω π ένας μιγαδικός, primary, πρώτος και $p = N\pi = a^2 - ab + b^2$.
Τότε, $4p = (2a - b)^2 + 3b^2$, όπου θέτοντας $A = 2a - b$ και $B = \frac{b}{3}$, έχουμε ότι $4p = A^2 + 27B^2$.
Σύμφωνα με την Πρόταση 2.2.6 : Αν $p \equiv 1 \pmod 3$, τότε υπάρχουν ακέραιοι A, B τέτοιοι ώστε $4p = A^2 + 27B^2$, όπου τα $4p$, A, B είναι μοναδικά καθορισμένα μέχρι προσήμου.

Πρόταση 3.5.2:

Αν $p \equiv 1 \pmod 3$, τότε $x^3 \equiv 2 \pmod p$ είναι επιλύσιμη αν και μόνο αν υπάρχουν ακέραιοι C και D τέτοιοι ώστε $p = C^2 + 27D^2$.

Απόδειξη:
Αν $x^3 \equiv 2 \pmod p$ είναι επιλύσιμη, τότε και $x^3 \equiv 2 \pmod \pi$ και άρα $\pi \equiv 1 \pmod 2$ από την Πρόταση 3.5.1. Από την αναδιατύπωση της Πρότασης, έχουμε ακόμα ότι $4p = A^2 + 27B^2$, όπου $A = 2a - b$ και $B = \frac{b}{3}$.
Αφού το b είναι άρτιος ($b \equiv 0 \pmod 2$), παρατηρούμε από τους τύπους ότι και τα A, B είναι άρτια.
Έστω $D = \frac{B}{2}, C = \frac{A}{2}$. Τότε $p = C^2 + 27D^2$.

Αντίστροφα, αν υποθέσουμε ότι $p = C^2 + 27D^2$, τότε $4p = (2C)^2 + 27(2D)^2$.
Από μοναδικότητα: $B = \pm 2D$, άρα το B είναι άρτιο και από τους τύπους το ίδιο θα ισχύει και για το b.
Έπεται ότι $\pi = a + b\omega \equiv 1 \pmod 2$, διότι αν ήταν $\pi \equiv 0 \pmod 2$ θα είχαμε ότι το 2 διαιρεί το π πράγμα άτοπο αφού π πρώτος.
Λόγω της Πρότασης 3.5.1 έπεται ότι η $x^3 \equiv 2 \pmod \pi$ είναι επιλύσιμη.
Αφού $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ έχει $p = N\pi$ στοιχεία, υπάρχει ένας ακέραιος h για τον οποίο έχουμε $h^3 \equiv 2 \pmod \pi$. Αλλά, αν $\pi | (h^3 - 2)$, τότε $\overline{\pi} | (h^3 - 2)$ και άρα $\pi\overline{\pi} = p | (h^3 - 2)$.
Συνεπώς, $p | (h^3 - 2)$, δηλαδή η $x^3 \equiv 2 \pmod p$ έχει λύση.

4 Η σχέση του Stickelberger και ο Νόμος Αντιστροφής του Eisenstein

4.1 Στοιχεία Αλγεβρικής Θεωρίας Αριθμών

Παρακάτω αναφερόμαστε σε μερικά αποτελέσματα Αλγεβρικής Θεωρίας Αριθμών, χρήσιμα για την ανάπτυξη του τέταρτου Κεφαλαίου της εργασίας. Για τις αποδείξεις των Προτάσεων παραπέμπουμε στο [6].

Ορισμός:

-Ένας μιγαδικός αριθμός α λέγεται αλγεβρικός όταν είναι ρίζα μη-μηδενικού πολυωνύμου $f(x)$ με ρητούς συντελεστές.
-Ο αλγεβρικός αριθμός $\alpha \in \mathbb{C}$ λέγεται ακέραιος αλγεβρικός όταν είναι ρίζα μονικού πολυωνύμου με συντελεστές ακέραιους αριθμούς.
-Αλγεβρικό σώμα αριθμών λέγεται κάθε πεπερασμένη επέκταση $K/\mathbb{Q}$, $K \subseteq \mathbb{C}$.
-Το σύνολο των ακεραίων αλγεβρικών, έστω R, ενός αλγεβρικού σώματος αριθμών K, αποτελεί δακτύλιο (περιοχή) του Dedekind. Αυτό σημαίνει ιδιαίτερα ότι: Κάθε μη-μηδενικό, πρώτο ιδεώδες του R είναι maximal και ότι κάθε ιδεώδες $A \trianglelefteq R$, $A \neq < 0 >$ αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών. ([6] III.3.9 και III.3.14)
-Επίσης η περιοχή του Dedekind R των ακεραίων αλγεβρικών αριθμών ενός αλγεβρικού σώματος αριθμών K, ικανοποιεί τη συνθήκη ότι για κάθε ιδεώδες A του R ($A \neq < 0 >$), ο δακτύλιος πηλίκο R/A έχει πεπερασμένο πλήθος στοιχείων. ([6] III.4.5)

Ορισμός:

Norm του ιδεώδους A του R ($A \neq < 0 >$) ορίζεται η (πεπερασμένη) τάξη του δακτυλίου R/A και συμβολίζεται ως $N(A)$.

Πρόταση 4.1.1:

Η συνάρτηση Norm (στο σύνολο των ιδεωδών A του R, $A \neq < 0 >$) είναι πλήρως πολλαπλασιαστική, δηλαδή αν A,B ιδεώδη του R, ισχύει $N(A \cdot B) = N(A) \cdot N(B)$. ([6] V.1.5)

-Άμεση συνέπεια της Πρότασης είναι το παρακάτω Πόρισμα.

Πόρισμα 4.1.2:

Αν P πρώτο ιδεώδες του R, τότε $N(P) = p^f$ για κάποιο πρώτο αριθμό p και $f \in \mathbb{N}$.

Απόδειξη:
Η $N(P) = |\frac{R}{P}|$, αλλά R περιοχή του Dedekind και P πρώτο ιδεώδες. Συνεπώς, το ιδεώδες P είναι maximal και επομένως ο δακτύλιος R/P είναι πεπερασμένο σώμα.
Οπότε και $|\frac{R}{P}| = p^f$, για κάποια δύναμη ενός πρώτου αριθμού p.
Είναι φανερό ότι $f = [R/P : \mathbb{Z}/p\mathbb{Z}]$.

-Έστω τώρα $P = p\mathbb{Z}$ πρώτο ιδεώδες του $\mathbb{Z}$. Το ιδεώδες PR αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του R:

$$PR = Q_1^{e_1} Q_2^{e_2} ... Q_r^{e_r}.$$

Ο εκθέτης e_i του Q_i, $i = 1, 2, ..., r$ λέγεται δείκτης διακλάδωσης του Q_i υπεράνω του $P = p\mathbb{Z}$ και το $f_i = [R/Q_i : \mathbb{Z}/p\mathbb{Z}]$, $i = 1, 2, ..., r$ λέγεται βαθμός αδρανείας του Q_i υπεράνω του $P = p\mathbb{Z}$.

Ισχύει το παρακάτω Θεώρημα, γνωστό ως Νόμος Ανάλυσης.

Νόμος Ανάλυσης:

Έστω $K/\mathbb{Q}$ αλγεβρικό σώμα αριθμών, $P = p\mathbb{Z}$ ένα πρώτο ιδεώδες του $\mathbb{Z}$ και $PR = Q_1^{e_1} ... Q_r^{e_r}$ η μονοσήμαντη ανάλυση του PR σε γινόμενο πρώτων ιδεωδών του R.
Αν $[K : \mathbb{Q}] = n$, τότε ισχύει:

$$n = e_1 f_1 + ... + e_r f_r. \text{ ([6] } VI.3.4 \text{)}$$

Στην ειδική περίπτωση πλέον που η επέκταση $K/\mathbb{Q}$ είναι Galois με ομάδα Galois $G := Gal(K/\mathbb{Q})$, τότε αποδεικνύεται η παρακάτω Πρόταση.

Πρόταση 4.1.3:

Η ομάδα Galois δρα μεταβατικά στο σύνολο $\{Q_1, ..., Q_r\}$, δηλαδή για κάθε ζευγάρι πρώτων ιδεωδών Q_i, Q_j, $i, j \in \{1, ..., r\}$, $i \neq j$ υπάρχει $\sigma \in G$ τέτοιο ώστε $\sigma(Q_i) = Q_j$

Η Πρόταση αυτή ¨αναγκάζει¨ να συμβαίνουν τα παρακάτω:

$$e_1 = ... = e_r := e$$
$$\text{και } f_1 = ... = f_r := f. \text{ ([6] } VI.4.1 \text{)}$$

Και, επομένως, ισχύει η Πρόταση:

Πρόταση 4.1.4:

Έστω $K/\mathbb{Q}$ επέκταση Galois, $[K : \mathbb{Q}] = n$. Αν $P = p\mathbb{Z}$ πρώτο ιδεώδες του $\mathbb{Z}$, τότε το PR αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών του R και έχει τη μορφή:

$$PR = (Q_1...Q_r)^e,\ f = [R/Q_i : \mathbb{Z}/p\mathbb{Z}] \text{ για κάθε } i = 1, ..., r.$$

Επομένως, ισχύει $n = e \cdot r \cdot f$. ([6] $VI.4.2$)

Νόμος Ανάλυσης στα κυκλοτομικά σώματα:

Πρόταση 4.1.5: ([6] $VI.6.9$)

Όλοι οι πρώτοι αριθμοί p, $p \nmid n$ δεν διακλαδίζονται στο σώμα $L = \mathbb{Q}(\zeta_n)$.

Πρόταση 4.1.6: ([6] $VI.6.10$)

Έστω p πρώτος αριθμός, $p \nmid n$. Τότε είναι $e = 1$ και f είναι ο ελάχιστος φυσικός αριθμός τέτοιος ώστε $p^f \equiv 1 \pmod{n}$, δηλαδή η τάξη του p modn.

Πρόταση 4.1.7: ([6] $VI.6.13$)

Έστω p πρώτος αριθμός $n = p^k$, $k \geq 1$, $L = \mathbb{Q}(\zeta_{p^k})$. Τότε, ο δακτύλιος των ακεραίων αλγεβρικών του L είναι ο $R = \mathbb{Z}[\zeta_{p^k}]$ και ισχύει:

$$pR = Q^{\phi(n)} = Q^{\phi(p^k)},$$

όπου $Q =< 1 - \zeta_{p^k} >$.

Νόμος Ανάλυσης στα κυκλοτομικά σώματα: ([6] $VI.6.14$)

Έστω p πρώτος αριθμός, $n = p^k \cdot m$, $p \nmid m$, $k \geq 1$. Τότε, το ιδεώδες pR αναλύεται στο σώμα $L = \mathbb{Q}(\zeta_n)$ ως εξής:

$$pR = (Q_1...Q_r)^e$$

$N_{\frac{L}{\mathbb{Q}}}(Q_i) = p^f$, όπου $e = \phi(p^k)$, f είναι η τάξη του p στην ομάδα $(\mathbb{Z}/m\mathbb{Z})^*$ και $r = \frac{\phi(n)}{e \cdot f}$.

-Στη συνέχεια, θα αποδείξουμε δύο Προτάσεις ιδιαίτερα χρήσιμες στα επόμενα.

Πρόταση 4.1.8:

Έστω $K/\mathbb{Q}$ επέκταση Galois, με ομάδα Galois $G := Gal(K/\mathbb{Q})$ και A ιδεώδες του R, $A \neq < 0 >$. Ισχύει:

$$\prod_{\sigma \in G} \sigma(A) =< N(A) >.$$

Απόδειξη:
Παρατηρούμε ότι και τα δύο μέλη της ισότητας που θέλουμε να αποδείξουμε είναι πολλαπλασιαστικά. Αυτό, διότι οι σ είναι ομομορφισμοί σωμάτων, ενώ όπως αναφέραμε η Norm πρόκειται για μία πολλαπλασιαστική συνάρτηση. Άρα, λόγω πολλαπλασιαστικότητας, αρκεί να αποδείξουμε τη σχέση για κάποιο πρώτο ιδεώδες $P \subsetneq R$.

Έστω $Q_1, Q_2, ..., Q_r$ να είναι τα διακριτά πρώτα ιδεώδη στο σύνολο $\{\sigma(P) | \sigma \in G\}$.
Τότε, $|G| = r \cdot |G_Z(P)|$, όπου $G_Z(P) = \{\sigma \in G | \sigma(P) = P\}$ (Η $G_Z(P)$ είναι υποομάδα της G και λέγεται ομάδα ανάλυσης του Q ([6] $VII.2.1$). Πρόκειται για τον σταθεροποιητή της Θεωρίας Ομάδων).
Αφού $efr = n = [K : \mathbb{Q}] = |G|$ συνεπάγεται ότι $|G_Z(P)| = ef$.

Έχουμε, λοιπόν, ότι: $\prod_{\sigma \in G} \sigma(P) = (Q_1...Q_r)^{ef} = ((Q_1...Q_r)^e)^f =< p >^f =< p^f >$, διότι $pR =< p >= (Q_1...Q_r)^e$.

Αφού $N(P) = |R/P| = p^f$, αυτό ολοκληρώνει την απόδειξη.

Πρόταση 4.1.9: [[6] VI.4]

Έστω σ ένας $\mathbb{Q}$-αυτομορφισμός του σώματος K και Q πρώτο ιδεώδες του R που βρίσκεται πάνω από το πρώτο ιδεώδες P του $\mathbb{Z}$. Τότε:
1) Το $\sigma(Q)$ είναι πρώτο ιδεώδες του R
2) $P \subsetneq \sigma(P)$
3) $f(Q/P) = f(\sigma(Q)/P)$
4) $e(Q/P) = e(\sigma(Q)/P)$.

Ορισμός:

Έστω $K/\mathbb{Q}$ επέκταση αλγεβρικών σωμάτων αριθμών και $[K:\mathbb{Q}] = n$. Έστω $\alpha \in K$. Τότε: $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$, όπου σ_i ($i = 1, ..., n$) οι n εμφυτεύσεις του $K \subset \mathbb{C}$.

Πρόταση 4.1.10:

Έστω $K/\mathbb{Q}$ μία επέκταση Galois με ομάδα G. Έστω $\alpha \in R$ και $A =< \alpha >$ το κύριο ιδεώδες με γεννήτορα το α. Αν $N\alpha$ η Norm του α, τότε ισχύει ότι $N(A) = |N(\alpha)|$.

Απόδειξη:
$< N(A) >= \prod_{\sigma \in G} \sigma(A) = \prod_{\sigma \in G} \sigma(< \alpha >) = \prod_{\sigma \in G} < \sigma(\alpha) >=< \prod_{\sigma \in G} \sigma(\alpha) >=< N(\alpha) >$.
Τότε η $N(A)$ και η $N(\alpha)$ αναγκαστικά θα διαφέρουν κατά μία μονάδα (αφού έχουμε δύο ίσα κύρια ιδεώδη). Αφού είναι και τα δύο στο $\mathbb{Z}$ μπορούν να διαφέρουν μόνο ως προς το πρόσημο. Αλλά, αφού η $N(A)$ είναι εξ' ορισμού της, θετική ποσότητα, θα έχουμε $N(A) = |N(\alpha)|$.

- Η Πρόταση 4.1.7 ισχύει γενικότερα για κάθε επέκταση $K/\mathbb{Q}$ αλγεβρικού σώματος Κ. ([6] *V*.1.11)

4.2 Το Power Residue σύμβολο

Έστω m ένας θετικός ακέραιος και ας ορίσουμε ως D_m τον δακτύλιο των ακεραίων αλγεβρικών του κυκλοτομικού σώματος $\mathbb{Q}(\zeta_m)$. Έστω P ένα πρώτο ιδεώδες στον D_m που δεν περιέχει το m (δηλαδή το P δεν εμφανίζεται στην ανάλυση του $< m >$ σε γινόμενο πρώτων ιδεωδών). Επιπλέον, έστω $q = N(P) = |D_m/P|$.

Πρόταση 4.2.1:

Έστω p ένας ρητός πρώτος και $p \nmid m$. Έστω P ένα πρώτο ιδεώδες στον D_m που περιέχει το p. Τότε, τα σύμπλοκα των 1, ζ_m, $\zeta_m^2, ..., \zeta_m^{m-1}$ στον D_m/P είναι όλα διακριτά. Αν το f συνβολίζει τον βαθμό του P ($f = [D_m/P : \mathbb{Z}/p\mathbb{Z}]$) , τότε ισχύει ότι $p^f \equiv 1 \pmod{m}$.

Απόδειξη:
Αν $w \in D_m$, θα δηλώνουμε ως $\overline{w} = w + P$ το σύμπλοκό του στον D_m/P.

Διαιρούμε και τα δύο μέλη της $x^m - 1 = \prod_{i=0}^{m-1}(x - {\zeta_m}^i)$ με $(x-1)$.

Παίρνουμε: $1 + x + x^2 + ... + x^{m-1} = \prod_{i=1}^{m-1}(x - {\zeta_m}^i)$

Θέτουμε $x = 1$ σε συτήν την ισότητα και παίρνουμε: $m = \prod_{i=1}^{m-1}(1 - {\zeta_m}^i)$.
Άρα, $\overline{m} = \prod_{i=1}^{m-1}\overline{(1 - {\zeta_m}^i)}$. Τώρα, αφού $p \nmid m$, θα ισχύει ότι $\overline{m} \neq \overline{0}$.
Από αυτό συμπεραίνουμε ότι $\overline{\zeta_m}^i \neq \overline{1}$ για κάθε i, $1 \leq i \leq m-1$, και άρα $\overline{\zeta_m}^i \neq \overline{\zeta_m}^j$ για κάθε (i, j), $0 \leq i, j \leq m-1$, $i \neq j$.

Το σύνολο $\{\overline{\zeta_m}^i := {\zeta_m}^i + P \mid 0 \leq i \leq m-1\}$ αποτελεί πολλαπλασιαστική υποομάδα της $(\frac{D_m}{P})^*$ τάξης m. Όμως, η πολλαπλασιαστική ομάδα $|D_m/P|$ έχει τάξη $p^f - 1$. Επομένως, $m|(p^f - 1)$ και άρα $p^f \equiv 1 \pmod{m}$.

Πρόταση 4.2.2:

Έστω $\alpha \in D_m$, P ένα πρώτο ιδεώδες του D_m, $\alpha \notin P$ και $q = N(P) = |D_m P|$. Τότε υπάρχει ακέραιος i, μοναδικός mod m, τέτοιος ώστε:

$$\alpha^{\frac{(q-1)}{m}} \equiv \zeta_m^i \pmod{P}.$$

Απόδειξη:
Αφού η πολλαπλασιαστική ομάδα του σώματος D_m/P έχει $q-1$ στοιχεία, έχουμε ότι $\alpha^{q-1} \equiv 1 \pmod{P}$.

Έχουμε γενικά ότι: $x^m - 1 = \prod_{i=0}^{m-1}(x - \zeta_m^i)$

Συγκεκριμένα, εδώ για $x = \alpha^{\frac{q-1}{m}}$ (μπορούμε να το κάνουμε γιατί $\frac{q-1}{m} \in \mathbb{Z}$), έχουμε:

$$(\alpha^{\frac{q-1}{m}})^m - 1 = \prod_{i=0}^{m-1}(\alpha^{\frac{q-1}{m}} - \zeta_m^i) \equiv 0 \pmod{P}, \text{ αφού } a^{q-1} \equiv 1 \pmod{P}.$$

Άρα, $\prod_{i=0}^{m-1}(\alpha^{\frac{q-1}{m}} - \zeta_m^i) \equiv 0 \pmod{P}$ και αφού το P είναι πρώτο, υπάρχει i, $0 \leq i \leq m-1$ τέτοιο ώστε $\alpha^{\frac{q-1}{m}} \equiv \zeta_m^i \pmod{P}$. Αν $i \not\equiv j \pmod{m}$, τότε $\zeta_m^i \not\equiv \zeta_m^j \pmod{P}$ (βλ. Πρόταση 4.2.1).

Άρα, το i αυτό είναι μοναδικό modm.

Ορισμός:

Έστω $\alpha \in D_m$ και P πρώτο ιδεώδες του D_m που δεν περιέχει το m. Ορίζουμε το m-οστό Power Residue σύμβολο, $\left(\frac{\alpha}{P}\right)_m$, ως ακολούθως:

a) $\left(\frac{\alpha}{P}\right)_m = 0$, αν $\alpha \in P$

b) Αν $\alpha \notin P$, $\left(\frac{\alpha}{P}\right)_m$ είναι η μοναδική m-οστή ρίζα της μονάδας τέτοια ώστε:

$$\alpha^{(NP-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}.$$

Πρόταση 4.2.3:

a) $\left(\frac{\alpha}{P}\right)_m = 1$ αν και μόνο αν η ισοτιμία $x^m \equiv \alpha \pmod{P}$ είναι επιλύσιμη στον D_m.

b) Για όλα τα $\alpha \in D_m$, ισχύει $\alpha^{(NP-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}$.

c) Για κάθε $\alpha, \beta \in D_m$ ισχύει: $\left(\frac{\alpha\beta}{P}\right)_m = \left(\frac{\alpha}{P}\right)_m \cdot \left(\frac{\beta}{P}\right)_m$.

d) Αν $\alpha, \beta \in D_m$ και $\alpha \equiv \beta \pmod{P}$, τότε $\left(\frac{\alpha}{P}\right)_m = \left(\frac{\beta}{P}\right)_m$.

-Έχουμε ήδη αποδείξει την Πρόταση αυτή για $m = 2, 3, 4$ οπότε θα παραλείψουμε αυτή τη φορά την απόδειξη, καθώς είναι παρόμοια.

Πόρισμα 4.2.4:

Έστω P ένα πρώτο ιδεώδες του D_m που δεν περιέχει το m. Τότε:

$$\left(\frac{\zeta_m}{P}\right)_m = \zeta_m{}^{(NP-1)/m}.$$

Απόδειξη:
Από το *b*) της Πρότασης 4.2.3, τα δύο μέλη της παραπάνω σχέσης είναι ισότιμα modP. Αφού, όμως, και τα δύο μέλη είναι m-οστές ρίζες της μονάδας και $m \notin P$, έπεται από την Πρόταση 4.2.1 ότι είναι ίσα.

-Είναι σημαντικό να επεκτείνουμε τον ορισμό του $\left(\frac{\alpha}{P}\right)_m$ με τέτοιο τρόπο ώστε το $\left(\frac{\alpha}{\beta}\right)_m$ να έχει νόημα όταν το β είναι πρώτο προς το m. Αυτό γίνεται με τον ακόλουθο ορισμό.

Ορισμός:

Έστω $A \subsetneq D_m$ ένα ιδεώδες του D_m πρώτο προς το m. Έστω $A = P_1P_2...P_n$ η ανάλυση του A σε πρώτα ιδεώδη (όχι κατ΄ ανάγκη διαφορετικά μεταξύ τους).
Για $\alpha \in D_m$ ορίζουμε $\left(\frac{\alpha}{A}\right)_m := \prod_i \left(\frac{\alpha}{P_i}\right)_m$.
Αν $\beta \in D_m$ και β είναι πρώτο προς το m, ορίζουμε $\left(\frac{\alpha}{\beta}\right)_m := \left(\frac{\alpha}{<\beta>}\right)_m$.

Πρόταση 4.2.5:

Έστω A, B ιδεώδη πρώτα προς το $< m >$. Τότε ισχύουν:

a) Για κάθε $\alpha, \beta \in D_m$, πρώτα προς το m, ισχύει: $\left(\frac{\alpha\beta}{A}\right)_m = \left(\frac{\alpha}{A}\right)_m \cdot \left(\frac{\beta}{A}\right)_m$.

b) Για οποιαδήποτε ιδεώδη A,B, πρώτα προς το m, ισχύει: $\left(\frac{\alpha}{AB}\right)_m = \left(\frac{\alpha}{A}\right)_m \cdot \left(\frac{\alpha}{B}\right)_m$.

c) Αν α είναι πρώτος προς το A και $x^m \equiv \alpha \pmod{A}$ είναι επιλύσιμη στον D_m,
τότε $\left(\frac{\alpha}{A}\right)_m = 1$.

- Η απόδειξη είναι άμεση χρησιμοποιώντας την Πρόταση 4.2.3 και τον παραπάνω ορισμό.
Το αντίστροφο του *c*) δεν ισχύει εν γένει.

-Στη συνέχεια, θα χρειαστεί να δούμε πως συμπεριφέρεται το σύμβολο $\left(\frac{\alpha}{P}\right)_m$ ως προς τους αυτομορφισμούς της ομάδας Galois G της επέκτασης $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.

-Από εδώ και πέρα θα χρησιμοποιούμε εκθετικό συμβολισμό για τους αυτομορφισμούς.
-Αν $\sigma \in G$ και $\alpha \in \mathbb{Q}(\zeta_m)$ θα γράφουμε α^σ αντί για $\sigma(\alpha)$. Ομοίως και για ιδεώδες A θα γράφουμε A^σ αντί για $\sigma(A)$.

Πρόταση 4.2.6:

Έστω A ένα ιδεώδες πρώτο προς το m και $\sigma \in G = Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Τότε:

$$\left(\frac{\alpha}{A}\right)_m^\sigma = \left(\frac{\alpha^\sigma}{A^\sigma}\right)_m .$$

Απόδειξη:
Αφού και τα δύο μέλη της σχέσης είναι πολλαπλασιαστικά ως προς το ιδεώδες A, αρκεί

να αποδείξουμε τη σχέση για $A = P$ πρώτο ιδεώδες.

Από τον ορισμό έχουμε: $\alpha^{(NP-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}$.

Εφαρμόζοντας τον σ σε αυτή την ισοτιμία παίρνουμε:

$$(\alpha^\sigma)^{(NP-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m^\sigma \pmod{P^\sigma}.$$

Όμως, $NP = NP^\sigma = p^f$, αφού από Πρόταση 4.1.6 έχουμε ότι $f(\frac{P^\sigma}{p\mathbb{Z}}) = f(\frac{P}{p\mathbb{Z}})$ για τον πρώτο p που βρίσκεται κάτω από το P.

$$\text{Άρα, } (\alpha^\sigma)^{\frac{(NP^\sigma-1)}{m}} \equiv \left(\frac{\alpha}{P}\right)_m^\sigma \pmod{P^\sigma}.$$

$$\text{Αλλά, } (\alpha^\sigma)^{\frac{NP^\sigma-1}{m}} \equiv \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m \pmod{P^\sigma}.$$

Συμπεραίνουμε ότι $\left(\frac{\alpha^\sigma}{A^\sigma}\right)_m \equiv \left(\frac{\alpha}{P}\right)_m^\sigma \pmod{P^\sigma}$ και επειδή είναι και τα δύο ρίζες της μονάδας, έχουμε ότι $\left(\frac{\alpha^\sigma}{A^\sigma}\right)_m = \left(\frac{\alpha}{P}\right)_m^\sigma$.

-Από εδώ και πέρα θεωρούμε l έναν περιττό πρώτο αριθμό. Θυμίζουμε (Πρόταση 4.1.7) ότι στον D_l έχουμε $< l >=< 1-\zeta_l >^{l-1}$, όπου $< 1-\zeta_l >$ είναι πρώτο ιδεώδες βαθμού 1, δηλ. $[\frac{D_l}{<\lambda>} : \frac{\mathbb{Z}}{l\mathbb{Z}}] = 1$. Στόχος μας από δω και πέρα να καταλήξουμε στη διατύπωση του Νόμου Αντιστροφής του Eisenstein. Θα χρειαστούμε έναν σημαντικό ορισμό πρώτα. Πρόκειται για την έννοια του primary στοιχείου, όπως κάναμε και στα προηγούμενα Κεφάλαια.

Ορισμός:

Ένα μη μηδενικό στοιχείο α του D_l λέγεται primary αν δεν είναι μονάδα, είναι πρώτο προς το l και είναι ισότιμο με έναν ακέραιο $mod(1-\zeta_l)^2$.

-Υπενθυμίζουμε ότι στην περίπτωση για $l = 3$, απαιτούμε το α να είναι ισότιμο με $2 \pmod{(1-\zeta_3)}^2$.

Λήμμα 4.2.7:

Έστω $\alpha \in D_l$ και α πρώτο προς το l. Τότε υπάρχει ένας ακέραιος $c \in \mathbb{Z}$, μοναδικός modl, τέτοιος ώστε $\zeta_l^c \alpha$ να είναι primary.

Απόδειξη:
Έστω $\lambda = 1 - \zeta_l$.
Αφού το πρώτο ιδεώδες $< \lambda >$ είναι βαθμού 1, δηλαδή $[\frac{D_l}{<\lambda>} : \frac{\mathbb{Z}}{l\mathbb{Z}}] = 1$, θα ισχύει ότι τα σώματα αυτά ταυτίζονται και άρα κάθε στοιχείο του $\frac{D_l}{<\lambda>}$ θα μπορεί να αναπαρασταθεί από έναν ακέραιο modulo l. Άρα, και για το α υπάρχει ένας ακέραιος $d \in \mathbb{Z}$ τέτοιος ώστε $\alpha \equiv d \pmod{\lambda}$.
Τώρα, $\frac{\alpha - d}{\lambda} \in D_l$ και άρα πάλι υπάρχει ένα $b \in \mathbb{Z}$ τέτοιο ώστε:

$$\begin{gathered}\frac{\alpha-d}{\lambda} \equiv b \pmod{\lambda} \Rightarrow \\ \alpha - d \equiv b\lambda \pmod{\lambda^2} \Rightarrow \\ \alpha \equiv d + b\lambda \pmod{\lambda^2}.\end{gathered}$$

Αφού $\zeta_l = 1 - \lambda$ έχουμε $\zeta_l^c \equiv 1 - c\lambda \pmod{\lambda^2}$.

Συνδυάζοντας, έχουμε $\zeta_l^c \alpha \equiv (d + b\lambda) \cdot (1 - c\lambda) \pmod{\lambda^2}$.

Άρα, $\zeta_l^c \alpha \equiv d + b\lambda - dc\lambda - cb\lambda^2 \pmod{\lambda^2} \Rightarrow \zeta_l^c \alpha \equiv d + b\lambda - dc\lambda \pmod{\lambda^2} \Rightarrow$

$$\zeta_l^c \alpha \equiv d + (b - dc)\lambda \pmod{\lambda^2}.$$

Παρατηρούμε ότι ο ακέραιος d δεν διαιρείται από l, γιατί αν είχαμε ότι $l|d$ θα ίσχυε και ότι $\lambda|d$ και τελικά ότι $\lambda|\alpha$, πράγμα άτοπο διότι υποθέσαμε από την αρχή ότι το α είναι πρώτο προς το l. Άρα, η ισοτιμία μένει ως έχει και δεν ¨απλοποιείται¨. Επομένως, η ισοτιμία $dx \equiv b \pmod{\lambda}$ έχει μοναδική λύση, αφού $(d, \lambda) = 1$. Έστω c η λύση αυτή.
Τότε, $\zeta_l^c \alpha \equiv d \pmod{\lambda^2}$ και άρα το $\zeta_l^c \alpha$ είναι primary.

Ο Νόμος Αντιστροφής του Eisenstein:

Έστω l ένας περιττός πρώτος, $b \in \mathbb{Z}$ ένας ακέραιος πρώτος προς τον l και $\alpha \in D_l$ ένα primary στοιχείο. Υποθέτουμε ότι τα α, b είναι πρώτα μεταξύ τους. Τότε:

$$\left(\frac{\alpha}{b}\right)_l = \left(\frac{b}{\alpha}\right)_l.$$

4.3 Η σχέση του Stickelberger

Είχαμε ορίσει στο Κεφάλαιο 2.2 τα αθροίσματα Gauss μέσω του τύπου $g_a(\chi) = \sum_t \chi(t)\zeta^{at}$. Αν ονομάσουμε, τώρα, $\psi(t) := \zeta^{at}$, τότε το άθροισμα γίνεται $g_a = \sum_t \chi(t)\psi(t)$. Παρατηρούμε ότι ο] ψ είναι ένας προσθετικός χαρακτήρας, δηλαδή $\psi(t + s) = \zeta^{a(t+s)} = \zeta^{at} \cdot \zeta^{as} = \psi(t) \cdot \psi(s)$.

Στη γενική περίπτωση, τώρα, χρειαζόμαστε να γενικεύσουμε το κύριο αποτέλεσμα του Κεφαλαίου σε οποιοδήποτε πεπερασμένο σώμα F. Πρέπει να αντικαταστήσουμε, δηλαδή, τον προσθετικό χαρακτήρα $\psi(t) = \zeta_p^{at}$ που είχαμε στο σώμα $\mathbb{F}_p$ με κάποιο ανάλογό του στο $\mathbb{F}_q$ ($q = p^n$) και αυτό θα γίνει μέσω της συνάρτησης ίχνος.
Συγκεκριμένα, αν θέσουμε $F = \mathbb{F}_q$, για $\alpha \in F$ ορίζουμε ίχνος του α :
$tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + ... + \alpha^{p^{n-1}}$ (είναι το ίχνος του α στην επέκταση $\mathbb{F}_q/\mathbb{F}_p$).

Πρόταση 4.3.1:

Αν $\alpha, \beta \in F$ και $c \in \mathbb{Z}$, τότε:
a) $tr(\alpha) \in \mathbb{F}_p$
b) $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$
c) $tr(c\alpha) = c \cdot tr(\alpha)$
d) Η συνάρτηση tr απεικονίζει το F επί του $\mathbb{F}_p$.

Απόδειξη:
a) Έχουμε:

$$(\alpha + \alpha^p + ... + \alpha^{p^{n-1}})^p = \alpha^p + \alpha^{p^2} + ... + \alpha^{p^n}.$$

Αφού, $\alpha^{p^n} = \alpha^q = \alpha$, παρατηρούμε ότι $tr(\alpha)^p = tr(\alpha)$. Άρα, $tr(\alpha) \in \mathbb{F}_p$.

b) Ισχύει:

$$\begin{aligned} tr(\alpha + \beta) &= (\alpha + \beta) + (\alpha + \beta)^p + ... + (\alpha + \beta)^{p^{n-1}} \\ &= (\alpha + \beta) + (\alpha^p + \beta^p) + ... + (\alpha^{p^{n-1}} + \beta^{p^{n-1}}) \\ &= (\alpha + \alpha^p + ... + \alpha^{p^{n-1}}) + (\beta + \beta^p + ... + \beta^{p^{n-1}}) \\ &= tr(\alpha) + tr(\beta) \ . \end{aligned}$$

c) Έχουμε:

$$\begin{aligned} tr(c\alpha) &= c\alpha + c^p\alpha^p + ... + c^{p^{n-1}}\alpha^{p^{n-1}} \\ &= c(\alpha + \alpha^p + ... + \alpha^{p^{n-1}}) \\ &= c \cdot tr(\alpha). \end{aligned}$$

Έχουμε χρησιμοποιήσει το γεγονός ότι $c^p = c$, για κάθε $c \in \mathbb{F}_p$.

d) Το πολυώνυμο $x + x^p + ... + x^{p^{n-1}}$ έχει το πολύ p^{n-1} ρίζες στο F. Αφού το F έχει p^n στοιχεία, υπάρχει ένα $\alpha \in F$ τέτοιο ώστε $tr(\alpha) = c \neq 0$. Αν $b \in \mathbb{F}_p$, τότε χρησιμοποιώντας την ιδιότητα *c*) παίρνουμε ότι $tr((b/c)\alpha) = (b/c)tr(\alpha) = b$. Άρα, η συνάρτηση είναι επί.

Ορισμός:

Ο προσθετικός χαρακτήρας $\psi : \mathbb{F}_q \longrightarrow \mathbb{C}$ ορίζεται τώρα ως ξής:

$$\psi(\alpha) = \zeta_p^{tr(\alpha)}.$$

Πρόταση 4.3.2:

Η συνάρτηση ψ έχει τις παρακάτω ιδιότητες:
a) Για κάθε $\alpha, \beta \in \mathbb{F}_q$ ισχύει: $\psi(\alpha + \beta) = \psi(\alpha) \cdot \psi(\beta)$
b) Υπάρχει ένα $\alpha \in F$ τέτοιο ώστε $\psi(\alpha) \neq 1$
c) Ισχύει: $\sum_{\alpha \in F} \psi(\alpha) = 0$.

Απόδειξη:
a) $\psi(\alpha + \beta) = \zeta_p{}^{tr(\alpha+\beta)} = \zeta_p{}^{tr(\alpha)+tr(\beta)} = \zeta_p^{tr(\alpha)} \cdot \zeta_p{}^{tr(\beta)} = \psi(\alpha) \cdot \psi(\beta)$.

b) Η tr είναι επί συνάρτηση, άρα υπάρχει $\alpha \in F$, τέτοιο ώστε $tr(\alpha) = 1$. Τότε, $\psi(\alpha) = \zeta_p \neq 1$.

c) Έστω $S = \sum_{\alpha \in F} \psi(\alpha)$. Επιλέγουμε β τέτοιο ώστε $\psi(\beta) \neq 1$. Τότε, $\psi(\beta) \cdot S = \sum_{\alpha \in F} \psi(\beta)\psi(\alpha) =$
$= \sum_{\alpha \in F} \psi(\beta + \alpha) = S$.
Η τελευταία ισότητα προκύπτει, διότι τα $\alpha \in F$ και $\alpha + \beta \in F$ διατρέχουν και τα δύο ακριβώς όλα τα στοιχεία του σώματος F.
Έπεται ότι $S = 0$.

Πρόταση 4.3.3:

Έστω $\alpha, x, y \in F$. Τότε:

$$\frac{1}{q} \sum_{\alpha \in F} \psi(\alpha(x - y)) = \delta(x, y),$$

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

Απόδειξη:
Αν $x = y$, τότε $\sum_{\alpha \in F} \psi(\alpha(x - y)) = \sum_{\alpha \in F} \psi(0) = q$.

Αν $x \neq y$, τότε $x - y \neq 0$ και $\alpha(x - y)$ διατρέχει όλα τα στοιχεία της F όσο το α διατρέχει όλα τα στοιχεία της F. Άρα, $\sum_{\alpha \in F} \psi(\alpha(x - y)) = \sum_{\beta \in F} \psi(\beta) = 0$, από το *c*) της Πρότασης 4.3.2.

-Σε αυτό το Κεφάλαιο θα μελετήσουμε την ανάλυση του αθροίσματος Gauss σε πρώτα ιδεώδη στα κυκλοτομικά σώματα.

Έστω F ένα πεπερασμένο σώμα με $q = p^f$ στοιχεία, χ ένας πολλαπλασιαστικός χαρακτήρας τάξης m και ψ ένας προσθετικός χαρακτήρας. Τότε οι τιμές του χ είναι m-ρίζες της μονάδας και όπως ορίστηκε το ψ, οι τιμές του ψ είναι p-ρίζες της μονάδας.
Δηλαδή, έχουμε $\chi(t) \in \mathbb{Q}(\zeta_m)$, $\psi(t) \in \mathbb{Q}(\zeta_p)$. Συνεπώς, $g(\chi, \psi) = \sum_{t \in F} \chi(t)\psi(t) \in \mathbb{Q}(\zeta_m, \zeta_p)$.

Πριν ξεκινήσουμε, θα πρέπει να κάνουμε συγκεκριμένους τους χαρακτήρες $\chi,\ \psi$.

Έστω D_m ο δακτύλιος ακεραίων αλγεβρικών του $\mathbb{Q}(\zeta_m)$ και έστω $P \in D_m$ πρώτο ιδεώδες με $m \notin P$. Έστω p ο πρώτος που βρίσκεται κάτω από το P και, άρα, $N(P) = q = p^f$.
Τέλος, ας θέσουμε $F = D_m/P$. Από τον Νόμο Ανάλυσης στα κυκλοτομικά σώματα, έχουμε ότι $p^f \equiv 1 \pmod{m}$.

Ορίζουμε έναν πολλαπλασιαστικό χαρακτήρα χ_P στον F ως εξής:
Έστω $0 \neq t \in F$ και έστω $\gamma \in D_m$ να είναι τέτοιο ώστε $\overline{\gamma} = t$. Εδώ $\overline{\gamma}$ είναι η κλάση του γ $mod P$. Έστω:

$$\chi_P(t) = \left(\frac{\gamma}{P}\right)_m^{-1} = \overline{\left(\frac{\gamma}{P}\right)_m}.$$

Από την Πρόταση 4.2.3, ο $\chi_P(t)$ είναι καλά ορισμένος πολλαπλασιαστικός χαρακτήρας. Ο λόγος που ορίσαμε για χαρακτήρα τον αντίστροφο του Power Residue συμβόλου αντί του ίδιου του συμβόλου, θα φανεί στη συνέχεια σε κάποιες αποδείξεις.

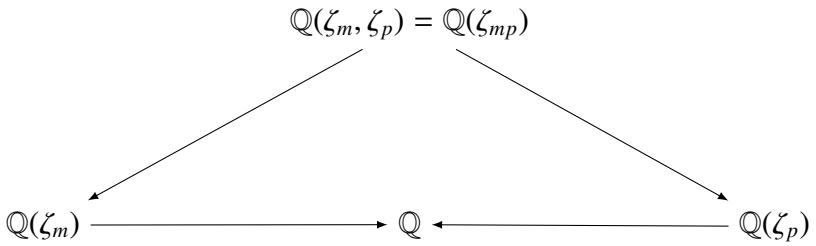
Θέτουμε για διευκόλυνση $g(P) = g(\chi_P, \psi)$ και $\Phi(P) = g(P)^m$.

Πρόταση 4.3.4:

Ισχύουν:
a) $g(P) \in \mathbb{Q}(\zeta_m, \zeta_p)$,
b) $|g(P)|^2 = q$,
και
c) $\Phi(P) \in \mathbb{Q}(\zeta_m)$.

Απόδειξη:
Το *a)* έχει ήδη συζητηθεί.
Το *b)* προκύπτει με όμοιο τρόπο όπως η Πρόταση 2.2.2 με τη διαφορά ότι εδώ το σώμα μας είναι το $\mathbb{F}_q$ αντί για το $\mathbb{F}_p$. Για το *c)* θα βασιστούμε στη Θεωρία Galois. Θεωρούμε το

παρακάτω διάγραμμα σωμάτων:



Η ομάδα Galois του $\mathbb{Q}(\zeta_{mp})/\mathbb{Q}$ δίνεται από τους αυτομορφισμούς σ_c, όπου $(c, pm) = 1$. Συγκεκριμένα, ο αυτομορφισμός αυτός είναι ο $\sigma_c : \zeta_{mp} \longrightarrow \zeta_{mp}^c$, όπου $(c, mp) = 1$.
Τώρα, ο σ_c αφήνει τα στοιχεία του $\mathbb{Q}(\zeta_m)$ σταθερά αν και μόνο αν $\sigma_c(\zeta_m) = \zeta_m$. Ας δούμε πότε συμβαίνει αυτό.
Μπορούμε να γράψουμε $\zeta_m = \zeta_{mp}^p$, οπότε το $\sigma_c(\zeta_m) = \zeta_m$ αλλιώς γράφεται $\sigma_c(\zeta_{mp}^p)$.
Έχουμε:

$$\sigma_c(\zeta_m) = \sigma_c(\zeta_{mp}^p) = [\sigma_c(\zeta_{mp})]^p = (\zeta_{mp}^c)^p$$

Και θέλουμε $\zeta_{mp}^{pc} = \zeta_m = \zeta_{mp}^p$. Για να ισχύει αυτό, πρέπει $pc \equiv p \pmod{mp}$ ή ισοδύναμα $c \equiv 1 \pmod{m}$, αφού $(p, m) = 1$.
Συγκεκριμένα, εδώ:
(i) Ο σ_c αφήνει τα στοιχεία του $\mathbb{Q}(\zeta_m)$ σταθερά αν και μόνο αν $c \equiv 1 \pmod{m}$
(ii) Ο σ_c αφήνει τα στοιχεία του $\mathbb{Q}(\zeta_p)$ σταθερά αν και μόνο αν $c \equiv 1 \pmod{p}$.

Για να δείξουμε ότι $\Phi(P) \in \mathbb{Q}(\zeta_m)$, αρκεί να δείξουμε, σύμφωνα με τα παραπάνω, ότι αν $c \equiv 1 \pmod{m}$, τότε $\Phi(P)^{\sigma_c} = \Phi(P)$.

Εφαρμόζουμε, λοιπόν, τον σ_c όταν $c \equiv 1 \pmod{m}$ αρχικά στο $g(P) = \sum_{t \in F} \chi_P(t)\psi(t)$.
Αφού, $\chi_P^{\sigma_c}(t) = \chi_P(t)$ (χ_P χαρακτήρας τάξης m) και $\psi(t)^{\sigma_c} = \psi(t)^c = \psi(ct)$, έχουμε:

$$g(P)^{\sigma_c} = \sum \chi_P(t)\psi(ct) = \chi_P(c)^{-1} g(P).$$

Για την τελευταία ισότητα θέσαμε $ct = t'$. Υψώνοντας τώρα και τα δύο μέλη εις την m, παίρνουμε το αποτέλεσμα ότι το $\Phi(P)$ μένει αμετάβλητο εφαρμόζοντας τον σ_c και άρα καταλήγουμε ότι $\Phi(P) \in \mathbb{Q}(\zeta_m)$.

-Προτού προχωρήσουμε στο να υπολογίσουμε την ανάλυση σε πρώτα ιδεώδη του $g(P)$ και του $\Phi(P)$ στη γενική μορφή, θα βοηθήσει σε αυτό το σημείο να ξαναθυμηθούμε πώς κάναμε το ίδιο για τις περιπτώσεις $m = 2, 3, 4$ που συζητήσαμε εκτενώς νωρίτερα.

-Για $m = 2$, το σώμα μας είναι το $\mathbb{Q}(\zeta_2) = \mathbb{Q}(\pm 1) = \mathbb{Q}$. Αν $p \in \mathbb{P}$, $P =< p >$ στο $\mathbb{Z}$. Έχουμε αποδείξει στην Πρόταση 1.4.4 ότι $g(P) = (-1)^{\frac{p-1}{2}} \cdot p$, δηλαδή έχουμε την μονοσήμαντη

ανάλυση του $g(P)$ σε γινόμενο πρώτων αριθμών.

-Για $m = 4$, το σώμα μας είναι το $\mathbb{Q}[i]$. Έχουμε αποδείξει στο Θεώρημα 2.5.6 ότι $g(\chi_\pi)^4 = \pi^3\overline{\pi}$. Έχουμε, δηλαδή, την μονοσήμαντη ανάλυση του $g(\chi_\pi)^4$ σε γινόμενο αναγώγων του $\mathbb{Z}[i]$.

-Για $m = 3$, το σώμα μας είναι το $\mathbb{Q}(\sqrt{-3})$. Έχουμε δείξει στο Πόρισμα 3.4.4 ότι $g(\chi_\pi)^3 = p\pi = \pi^2 \cdot \overline{\pi}$. Έχουμε, πάλι την ζητούμενη μονοσήμαντη ανάλυση του $g(\chi_\pi)^3$ σε γινόμενο αναγώγων του $\mathbb{Z}[\sqrt{-3}]$.

Σε όλες τις παραπάνω περιπτώσεις οι δακτύλιοι ακεραίων αλγεβρικών ήταν περιοχές μονοσήμαντης ανάλυσης και γι΄ αυτό υπήρχε μονοσήμαντη ανάλυση σε γινόμενο αναγώγων στοιχείων.
Βέβαια, στη γενική περίπτωση κάτι τέτοιο δεν ισχύει για οποιοδήποτε κυκλοτομικό σώμα $K = \mathbb{Q}(\zeta_l)$, $l \in \mathbb{P}$, $l \neq 2$.
Βέβαια, όπως έχουμε ξανααναφέρει ο δακτύλιος $D_l = \mathbb{Z}[\zeta_l]$ είναι περιοχή του Dedekind. Άρα, έχουμε μονοσήμαντη ανάλυση σε γινόμενο πρώτων ιδεωδών. Αυτή την ανάλυση αναζητάμε για το $< \Phi(P) >$.

Για να το πετύχουμε αυτό και για να γενικεύσουμε το μοτίβο, θα ορίσουμε κάποιες ¨συμβολικές δυνάμεις¨.
Έστω $K/\mathbb{Q}$ ένα αλγεβρικό σώμα αριθμών, Galois υπέρ του $\mathbb{Q}$ με ομάδα $G = Gal(K/\mathbb{Q})$. Η ομάδα G είναι πεπερασμένη.

Ορίζουμε τον δακτύλιο ομάδας $Z[G] = \{\sum_{\sigma\in G} a(\sigma)\sigma | a(\sigma) \in \mathbb{Z}\}$.

Αν $\alpha \in K$ ορίζουμε $\alpha^{\sum a(\sigma)\sigma} := \prod_\sigma \sigma(\alpha)^{a(\sigma)}$.

Αν το Α είναι ιδεώδες, ορίζουμε τη συμβολική δύναμη του με τον ίδιο τρόπο.

Ας εφαρμόσουμε τον ορισμό για τις περιπτώσεις που έχουμε μελετήσει ήδη. Για να είμαστε τυπικοί με τον ορισμό του χαρακτήρα που δώσαμε σε αυτό το Κεφάλαιο, παίρνοντας τον συζυγή χαρακτήρα αντί του κανονικού που παίρναμε ως τώρα, θα εργαστούμε με τις αντίστοιχες συζυγείς σχέσεις που είχαμε αποδείξει για το $g(P)$. Συγκεκριμένα, θεωρούμε ένα πρώτο ιδεώδες P βαθμού 1 (δηλ. $N(P) = p$, p πρώτος και $f = 1$). Οι δακτύλιοι $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ είναι Π.Κ.Ι. Άρα, $P =< \pi >$, όπου π πρώτο=ανάγωγο στοιχείο του $\mathbb{Z}[i]$ και $\mathbb{Z}[\omega]$ αντίστοιχα. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι το π είναι primary. Ο χαρακτήρας χ_P θα είναι $\chi_P = \chi^{-1}_{<\pi>} = \overline{\chi}_{<\pi>} = \overline{\chi}_\pi$. Το $g(\chi_P, \psi)$ δεν είχε ψ στις ειδικές περιπτώσεις. Έτσι, $g(P) = g(\chi_P) = g(\overline{\chi}_\pi)$. Επομένως, για την περίπτωση του $Z[i]$, $\Phi(P) = g(P)^4 = g(\overline{\chi}_\pi)^4 = \overline{\pi^3 \cdot \overline{\pi}} = \pi \cdot \overline{\pi}^3$ και ομοίως και για το $\mathbb{Z}[\omega]$.

-Για $m = 3$, έχουμε ότι $|\frac{\mathbb{Q}(\sqrt{-3})}{\mathbb{Q}}| = \phi(3) = 2$, άρα η ομάδα Galois έχει δύο αυτομορφισμούς. Από αυτούς, ο ένας θα είναι σίγουρα ο τετριμμένος αυτομομορφισμός και ο άλλος θα είναι μη-τετριμμένος και θα είναι η μιγαδική συζυγία. Έχουμε ότι σ_2 είναι ο μη-τετριμμένος αυτομορφισμός, οπότε εφόσον $\Phi(P) = \overline{\pi^2}\pi$ προκύπτει ότι $\Phi(P) = \pi^{\sigma_1+2\sigma_2} = \pi^{1\sigma_1^{-1}+2\sigma_2^{-1}}$.

-Ομοίως, για $m = 4$, έχουμε ότι $|\frac{\mathbb{Q}(\sqrt{-1})}{\mathbb{Q}}| = 2$. Έχουμε πάλι 2 αυτομορφισμούς και θέτοντας αυτή τη φορά με σ_3 τη μιγαδική συζυγία, εφόσον έχουμε $\Phi(P) = \overline{\pi^3}\pi$, παίρνουμε ότι $\Phi(P) = \pi^{\sigma_1+3\sigma_3} = \pi^{1\sigma_1^{-1}+3\sigma_3^{-1}}$.

Οι ειδικές αυτές περιπτώσεις γενικεύονται με το παρακάτω Θεώρημα, αφού φυσικά θεωρήσουμε την τιμή όχι του στοιχείου $\Phi(P)$, αλλά του κυρίου ιδεώδους που παράγεται από τον $\Phi(P)$ στον D_m.

Θεώρημα 4.3.5 (Η σχέση του Stickelberger) :

Έστω P πρώτο ιδεώδες στον D_m που δεν περιέχει το m. Τότε:

$$< \Phi(P) >= P^{\sum t\sigma_t^{-1}}.$$

Το άθροισμα είναι πάνω από όλα τα t, $1 \leq t \leq m$ που είναι σχετικά πρώτα προς το m.

4.4 Απόδειξη της σχέσης του Stickelberger

Θα χωρίσουμε την απόδειξη σε 4 βήματα.

Βήμα 1- Στοιχειώδες Βήμα

Λήμμα 4.4.1:

Έστω $p > 1$ ένας θετικός ακέραιος. Κάθε θετικός ακέραιος μπορεί να γραφεί μοναδικά στη μορφή $\sum_{i=0}^{n} a_i p^i$, όπου $0 \leq a_i < p$.

Απόδειξη:
Έστω a ένας θετικός ακέραιος. Υπάρχει πάντα μοναδικός μη αρνητικός ακέραιος n τέτοιος ώστε $p^n \leq a < p^{n+1}$. Από τον Ευκλείδειο Αλγόριθμο, έχουμε $a = a_n p^n + r$, όπου $0 \leq r < p^n$. Ο αριθμός a_n είναι μικρότερος από p, γιατί αν ήταν μεγαλύτερος θα είχαμε ότι $a \geq p^{n+1}$, άτοπο. Εφαρμόζουμε την ίδια διαδικασία για το r κ.ο.κ. Μετά από πεπερασμένο αριθμό βημάτων, θα έχουμε την επιθυμητή μορφή γραφής για το α.

Για την μοναδικότητα: Έστω ότι δεν υπάρχει μοναδική γραφή και, δηλαδή, έχουμε $\sum a_i p^i = \sum b_i p^i$, όπου $0 \leq a_i, b_i < p$. Τότε, το p διαιρεί το $a_0 - b_0$. Αφού, όμως, $|a_o - b_o| < p$, έχουμε $a_0 = b_0$. Αφαιρώντας το a_0 και από τα δύο μέλη, διαιρώντας με p και επαναλαμβάνοντας την διαδικασία, παίρνουμε ότι $a_1 = b_1$. Μετά από πεπερασμένο αριθμό βημάτων, καταλήγουμε ότι $a_i = b_i$ για κάθε i και άρα, η γραφή αυτή είναι μοναδική.

Ορισμός:

Έστω $q = p^f$. Αν $0 \leq a < q - 1$, γράφουμε $a = \sum_{i=0}^{f-1} a_i p^i$ με $0 \leq a_i < p$ και ορίζουμε $S(a) = \sum_{i=0}^{f-1} a_i$.
Για τυχαίο θετικό ακέραιο α ορίζουμε $S(a) = S(r)$, όπου $a \equiv r \pmod{q-1}$ και $0 \leq r < q - 1$.

Ορισμός:

Για πραγματικό αριθμό u ορίζουμε $\{u\}$ ως το $u - [u]$, όπου $[u]$ είναι ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του u. Ο αριθμός $\{u\}$ ανήκει στο διάστημα $[0,1)$ και ονομάζεται κλασματικό μέρος του u.

Λήμμα 4.4.2:

Για κάθε ακέραιο αριθμό a, ισχύει: $S(a) = (p-1)\sum_{i=0}^{f-1} \{\frac{p^i a}{(q-1)}\}$.

Απόδειξη:
Παρατηρούμε ότι και τα δύο μέλη παραμένουν αμετάβλητα αν προστεθεί ένα πολλαπλάσιο του $q-1$ στο a. Γι΄ αυτόν τον λόγο μπορούμε, χωρίς βλάβη της γενικότητας, να υποθέσουμε ότι $1 \leq a < q - 1$.

Γράφουμε $a = a_0 + a_1 p + \ldots + a_{f-1} p^{f-1}$, όπου $0 \leq a_i < p$. Αφού $p^f = q \equiv 1 \pmod{(q-1)}$, έχουμε:

$a = a_0 + a_1 p + ... + a_{f-1} p^{f-1}$,
$pa \equiv a_{f-1} + a_0 + ... + a_{f-2} p^{f-1} \pmod{(q-1)}$,
$p^2 a \equiv a_{f-2} + a_{f-1} p + ... + a_{f-3} p^{f-1} \pmod{(q-1)}$
και συνεχίζουμε ανάλογα για τις υπόλοιπες δυνάμεις...

Τα δεξιά μέλη των ισοτιμιών και της ισότητας είναι όλα μικρότερα από $q-1$. Επομένως, το $\{\frac{p^i a}{q-1}\}$ ισούται με την i-οστή ισοτιμία διαιρεμένη με $q-1$.
Άρα,

$$\sum_{i=0}^{f-1} \{\frac{p^i a}{q-1}\} = \frac{1}{q-1} S(a)(1 + p + ... + p^{f-1}) = \frac{1}{q-1} S(a) \frac{q-1}{p-1} = \frac{S(a)}{p-1}.$$

Λήμμα 4.4.3:

Για κάθε a ακέραιο, ισχύει: $\sum_{a=1}^{q-2} S(a) = \frac{f(p-1)(q-2)}{2}$.

Απόδειξη:
Γράφουμε $a = a_0 + a_1 p + ... + a_{f-1} p^{f-1}$, με $0 \le a_i < p$.

Παρατηρούμε, ακόμα, ότι $q - 1 = (p-1) + (p-1)p + ... + (p-1)p^{f-1}$, διότι οι ενδιάμεσοι όροι αλληλοαναιρούνται και μένει μόνο ο πρώτος και ο τελευταίος όρος.

Έπεται, λοιπόν, ότι $q - 1 - a = (p - 1 - a_0) + (p - 1 - a_1)p + ... + (p - 1 - a_{f-1})p^{f-1}$.

Άρα, προκύπτει ότι $S(a) + S(q - 1 - a) = f(p-1)$.

Αθροίζουμε την σχέση για α από 1 έως $q-2$ και παίρνουμε:
$S(1) + S(q-2) + S(2) + S(q-3) + ... + S(q-2) + S(1)$.
Παρατηρούμε ότι κάθε όρος εμφανίζεται δύο φορές και, άρα, είναι σαν να έχουμε δύο φορές το $S(a)$.

Τελικά, παίρνουμε: $2S(a) = \sum_{a=1}^{q-2} f(p-1) = f(p-1)(q-2)$.

Βήμα 2

-Το άθροισμα Gauss g(P), όπως προαναφέραμε είναι ένα στοιχείο του $\mathbb{Q}(\zeta_m, \zeta_p)$. Η απόδειξη της σχέσης του Stickelberger που θα δώσουμε, προαπαιτεί ότι εργαζόμαστε στο μεγαλύτερο σώμα $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$. Αυτό έχει το πλεονέκτημα ότι μπορούμε να χρησιμοποιούμε ελεύθερα τις $(q-1)-$ρίζες της μονάδας.

Το ακόλουθο διάγραμμα θα είναι χρήσιμο για τα επόμενα επιχειρήματα.

$$\begin{array}{ccccc}
S & \subset & D_{(q-1)p} & \to & D_{(q-1)p}/S \\
\cup & & \cup & & \cup \\
Q & \subset & D_{q-1} & \to & D_{q-1}/Q \\
\cup & & \cup & & \cup \\
P & \subset & D_m & \to & D_m/P \\
\cup & & \cup & & \cup \\
p & \subset & \mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z}
\end{array}$$

Στο παραπάνω διάγραμμα τα S, Q, P είναι πρώτα ιδεώδη για τους αντίστοιχους δακτυλίους ακεραίων αλγεβρικών. Θυμόμαστε από προηγούμενη παράγραφο ότι $p \nmid m$, f είναι η τάξη του p modulo m, τέτοια ώστε $p^f \equiv 1 \pmod{m}$ και $q = p^f$. Επιπλέον, για αυτήν την παράγραφο, έχουμε $\lambda_p = 1 - \zeta_p$.

Ορισμός:

Ορίζουμε τάξη (*ord*) ενός ακέραιου ιδεώδους A κάποιου αλγεβρικού σώματος αριθμών ως προς πρώτο ιδεώδες P, τον εκθέτη του P που εμφανίζεται στη μονοσήμαντη ανάλυση του A σε γινόμενο πρώτων ιδεωδών. Δηλαδή, αν $A = P^a B$, $P \nmid B$, τότε συμβολίζουμε $ord_P A = a$. Αν το P δεν ανήκει στην ανάλυση αυτή, τότε $ord_P A = 0$. Συχνά, η τάξη του A ως προς P λέγεται και P-αδική εκτίμηση του A.

Ιδιότητες του ord:
(*i*) $ord_P P = 1$
(*ii*) Αν P_1, P_2 πρώτα ιδεώδη του αντίστοιχου D, $P_1 \neq P_2$, τότε $ord_{P_1} P_2 = 0$ και $ord_{P_2} P_1 = 0$.
(*iii*) Αν A, B ακέραια ιδεώδη του D και P πρώτο ιδεώδες του D, τότε αν $A = P^a \cdot \Gamma$, $P \nmid \Gamma$ και $B = P^\beta \cdot \Delta$, $P \nmid \Delta$, ισχύει ότι $ord_P(A \cdot B) = ord_P(A) + ord_P(B)$.

Λήμμα 4.4.4:

(1) $ord_S(pD_{(q-1)p}) = p - 1$.
(2) $ord_S(\lambda_p) = 1$.
(3) $ord_S(P) = p - 1$.

Απόδειξη:
Εδώ έχουμε πάρει ένα πρώτο ιδεώδες, το S, του $D_{p(q-1)}$, πάνω από τον πρώτο αριθμό p. Τα Q, P είναι $Q = S \cap D_{q-1}$ και $P = Q \cap D_m$.
Εφαρμόζοντας τον Νόμο Ανάλυσης στο $\mathbb{Q}(\zeta_{p(q-1)})$ (εδώ αν γράψουμε $q - 1 = m'$, $p \nmid m'$), ο νόμος ανάλυσης μας δίνει ότι $e(S/p\mathbb{Z}) = \phi(p) = p - 1$.
Άρα, $ord_S(pD_{p(q-1)}) = p - 1$ και έχουμε το (1).
Για το (2), αν θεωρήσουμε τον πύργο σωμάτων:

$$\begin{array}{ccccc} S & \subset & D_{(q-1)p} & \to & D_{(q-1)p}/S \\ \cup & & \cup & & \cup \\ <\lambda_p> & \subset & D_p & \to & D_p/<\lambda_p> \\ \cup & & \cup & & \cup \\ p & \subset & \mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \end{array}$$

τότε γνωρίζουμε ότι $e(\frac{S}{<\lambda_p>}) \cdot e(\frac{<\lambda_p>}{p\mathbb{Z}}) = e(\frac{S}{p\mathbb{Z}}) = p - 1$.
Αλλά, επίσης, είναι γνωστό ότι $e(\frac{<\lambda_p>}{p\mathbb{Z}}) = p - 1$ (Πρόταση 4.1.7). Άρα, $e(\frac{S}{<\lambda_p>}) = 1$, ή ισοδύναμα $ord_S(<\lambda_p>) = 1$. Εδώ $<\lambda_p> = \lambda_p \cdot D_{q-1}$, το κύριο ιδεώδες που παράγεται από το λ_p στον δακτύλιο D_{q-1}.

Για το (3), αφού $p \nmid m$, ο νόμος ανάλυσης μας δίνει ότι $e(\frac{P}{p\mathbb{Z}}) = 1$ (Πρόταση 4.1.6).
Αλλά, $e(\frac{S}{p\mathbb{Z}}) = p - 1 = e(\frac{S}{P}) \cdot e(\frac{P}{p\mathbb{Z}}) \Rightarrow e(\frac{S}{P}) = p - 1$. Ισοδύναμα, $ord_S(P) = p - 1$.

Λήμμα 4.4.5:

Ισχύει: $D_m/P \approx D_{q-1}/Q$.

Απόδειξη:
Υπάρχει ένας φυσικός μονομορφισμός του σώματος D_m/P στο σώμα D_{q-1}/Q. Για να δείξουμε ότι ο μονομορφισμός είναι ισομορφισμός αρκεί να δείξουμε ότι τα δύο σώματα έχουν το ίδιο πλήθος στοιχείων.
Ο μονομορφισμός αυτός είναι ο $\psi : D_m/P \hookrightarrow D_{q-1}/Q$ που στέλνει ένα στοιχείο $\alpha + P$ στο $\alpha + Q$. Το πλήθος των στοιχείων του D_m/P είναι, όπως έχουμε δει, p^f, όπου f ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $p^f \equiv 1 \pmod m$. Αντίστοιχα, για το D_{q-1}/Q θα έχουμε $p^{f'}$ στοιχεία, όπου, τώρα, f' θα είναι ο ελάχιστος θετικός ακέραιος ώστε $p^{f'} \equiv 1 \pmod{(q-1)}$. Αλλά, αφού $q = p^f$, έχουμε ότι $p^f - 1 = q - 1$ και, άρα, $p^f \equiv 1 \pmod{(q-1)}$. Συμπεραίνουμε, λοιπόν, ότι $f = f'$ και, επομένως, τα δύο σώματα έχουν το ίδιο πλήθος στοιχείων.

Βήμα 3

-Θυμίζουμε ότι τα 1, ζ_{q-1}, $\zeta_{q-1}^2, .., \zeta_{q-1}^{q-2}$ έχουν διακεκριμένες εικόνες στον δακτύλιο πηλίκο D_{q-1}/Q. Ο ακόλουθος ορισμός προσομοιάζει τον ορισμό του m-αδικού Power Residue συμβόλου.

Ορισμός:

Αν $\alpha \in D_{q-1}$, ορίζουμε:
a) $\left(\frac{\alpha}{Q}\right) = 0$ αν $\alpha \in Q$.
b) Αν $\alpha \notin Q$, $\left(\frac{\alpha}{Q}\right)$ είναι η μοναδική $(q-1)$-ρίζα της μονάδας τέτοια ώστε $\alpha \equiv \left(\frac{\alpha}{Q}\right) \pmod Q$.

-Παρατηρούμε εύκολα ότι για κάθε $\alpha, \beta \in D_{q-1}$ ισχύει: $\left(\frac{\alpha\beta}{Q}\right) = \left(\frac{\alpha}{Q}\right) \cdot \left(\frac{\beta}{Q}\right)$ και αν ισχύει $\alpha \equiv \beta \pmod Q$ συνεπάγεται ότι $\left(\frac{\alpha}{Q}\right) = \left(\frac{\beta}{Q}\right)$.

Λήμμα 4.4.6:

Αν $\alpha \in D_m$, τότε $\left(\frac{\alpha}{Q}\right)^{\frac{q-1}{m}} = \left(\frac{\alpha}{P}\right)_m$.

Απόδειξη:
Ισχύει ότι το $\left(\frac{\alpha}{Q}\right)$ είναι μία $(q-1)$-ρίζα της μονάδας. Όμως, το $\alpha \in D_m$ και άρα
$\alpha \equiv \left(\frac{\alpha}{P}\right)_m \pmod{P}$.
Αυτό, διότι $\alpha \in D_m \Rightarrow \alpha \equiv \left(\frac{\alpha}{Q}\right)^{\frac{q-1}{m}} \pmod{D_m \cap Q}$ και $D_m \cap Q = P$.

Συνολικά, $\left(\frac{\alpha}{Q}\right)^{\frac{q-1}{m}} \equiv \left(\frac{\alpha}{P}\right) \pmod{P}$.

Και τα δύο είναι m-ρίζες της μονάδας διακριτές mod P και άρα δεν είναι μόνο ισότιμα αλλά και ίσα.

-Θα ορίσουμε, τώρα, τον πολλαπλασιαστικό χαρακτήρα στον D_{q-1}/Q ως εξής:

$$\omega(t) = \left(\frac{\gamma}{Q}\right), \text{ όπου } \gamma \in D_{q-1} \text{ είναι τέτοιο ώστε } \overline{\gamma} = t \ (\ \overline{\gamma} = \gamma + Q \ ).$$

Ο χαρακτήρας αυτός είναι εύκολο να δούμε ότι είναι ένας καλά ορισμένος πολλαπλασιαστικός χαρακτήρας.

Λήμμα 4.4.7:

Ισχύει: $\omega(\overline{\zeta}^i_{q-1}) = \zeta^i_{q-1}$.

Απόδειξη:
Εδώ παίρνουμε $\gamma = \zeta^i_{q-1} \in D_{q-1}$. Η κλάση του γ είναι $\overline{\gamma} = \zeta^i_{q-1} \pmod{Q}$.
Άρα, $\omega(t) = \omega(\overline{\gamma}) = \omega(\overline{\zeta}^i_{q-1}) = \left(\frac{\zeta^i_{q-1}}{Q}\right)$, όπου $\left(\frac{\zeta^i_{q-1}}{Q}\right)$ η μοναδική δύναμη της ζ_{q-1} τέτοια ώστε $\zeta^i_{q-1} \equiv \left(\frac{\zeta^i_{q-1}}{Q}\right) \pmod{Q}$.
Για τον ίδιο λόγο με το Προηγούμενο Λήμμα, προκύπτει τελικά η ισότητα.

Ορισμός:

Έστω a ένας μη-αρνητικός ακέραιος. Ορίζουμε $g_a := (\omega^{-a}, \psi)$.

-Παρατηρούμε ότι το $g(P)$ που μελετήθηκε στην προηγούμενη παράγραφο είναι ίσο με το g_a για $a = \frac{q-1}{m}$.

Θεώρημα 4.4.8:

Ισχύει: $ord_S g_a = S(a)$, όπου $1 \leq a < q$.

Απόδειξη:
Θα κάνουμε την απόδειξη επαγωγικά. Σε πρώτο βήμα θα αποδείξουμε το Θεώρημα για $a = 1$.

Για $a = 1$, θα αποδείξουμε ότι $ord_S(g_1) = S(1) = 1$.
Θυμίζουμε ότι $F = \mathbb{F}_{q-1}$ και ότι ο πολλαπλασιαστικός χαρακτήρας ω έχει τάξη $(q-1)$.

Έχουμε $g_1 = g(\omega^{-1}, \psi) = \sum_{t \in \mathbb{F}_{q-1}} \omega(t)^{-1} \zeta_p^{tr(t)}$.
Θα προσπαθήσουμε να γράψουμε το g_1 ως δυνάμεις του ζ_{q-1}. Τα στοιχεία του ίχνους $tr(\overline{\zeta}_{q-1}^{i})$ ανήκουν στο σώμα $\mathbb{F}_p$ ($tr: \mathbb{F}_q \longrightarrow \mathbb{F}_p$), δηλαδή είναι κλάσεις mod p.
Μπορούμε, επομένως, για κάθε i να επιλέξουμε έναν θετικό ακέραιο m_i τέτοιο ώστε:

$$m_i \equiv tr(\overline{\zeta}_{q-1}^{i}) \pmod{p},\ i = 1, 2, ..., q-2 \ (1).$$

Γνωρίζουμε ότι $\lambda_p := 1 - \zeta_p$, δηλαδή $\zeta_p = 1 - \lambda_p$.

Από Λήμμα 4.4.7 έχουμε ότι $\omega(\overline{\zeta}_q^{i}) = \zeta_q^{i}$. Μέσω της (1) η σχέση για το g_1 γίνεται:

$$g_1 = \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (1 - \lambda_p)^{m_i}.$$

Τώρα, από το σχήμα σελ.78, 79 προκύπτει ότι $S| < \lambda_p >$, δηλαδή $\lambda_p \in S$ και άρα $\lambda_p^2 \in S^2$ (2).

Εφαρμόζοντας τον διωνυμικό τύπο στην δύναμη $(1 - \lambda_p)^{m_i}$, έχουμε:

$$(1 - \lambda_p)^{m_i} \equiv 1 - m_i \lambda_p \pmod{S^2} \ (3).$$

Επομένως, το g_1 γράφεται:

$$g_1 \equiv \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} - \sum_{i=0}^{q-2} m_i \zeta_{q-1}^{-i} \lambda_p \pmod{S^2} \ (4).$$

Αλλά, $m_i \lambda_p \equiv tr(\overline{\zeta}_{q-1}^{i}) \lambda_p \equiv (\zeta_{q-1}^{i} + \zeta_{q-1}^{p \cdot i} + ... + \zeta_{q-1}^{p^{f-1} \cdot i}) \lambda_p \pmod{S^2}$, οπότε η (4) γράφεται:

$$g_1 \equiv \sum_{i=0}^{q-2} \zeta_{q-1}^{i} - \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (\zeta_{q-1}^{i} + \zeta_{q-1}^{p \cdot i} + ... + \zeta_{q-1}^{p^{f-1} \cdot i}) \lambda_p \pmod{S^2}.$$

Το πρώτο άθροισμα, ως γνωστόν, είναι μηδέν.

Επιπλέον, όλα τα αθροίσματα $\sum_{i=0}^{q-2} \zeta_{q-1}^{(p^j - 1) \cdot i}$, $j = 1, 2, ..., f-1$ είναι μηδέν, με το μόνο που μένει να είναι το άθροισμα για $j = 0$ που δίνει την τιμή $q-1$ (γιατί είναι μηδέν βλ. τη σειρά στην απόδειξη της Πρότασης 2.5.5).
Συνολικά, λοιπόν, έχουμε ότι $g_1 \equiv -(q-1) \lambda_p \pmod{S^2}$.

Πάλι από τον πύργο σελ. 78, 79 έχουμε ότι $p \equiv 0 \pmod{S}$ και επιπλέον $q = p^f$, $f \geq 2$ (αλλιώς θα ήταν $q = p$). Άρα, $S|p \Rightarrow S^2|p^2|p^f = q$.

Τελικά, η σχέση γίνεται $g_1 \equiv \lambda_p \pmod{S^2}$.
Από Λήμμα 4.4.4 (2) έχουμε ότι $S|g_1$, αφού $S| < \lambda_p >$. Όμως, το $S^2 \nmid g_1$, γιατί αν το διαρούσε, θα είχαμε ότι $S^2| < \lambda_p >$, πράγμα άτοπο αφού $ord_S(\lambda_p) = 1$.

Συμπεραίνουμε ότι $S|g_1$ αλλά $S^2 \nmid g_1$ και άρα $ord_S(g_1) = 1$, όπως θέλαμε να δείξουμε.

Συνεχίζουμε την επαγωγή μας ορίζοντας $\hat{s}(a) = ord_S g_a$.
Θα μελετήσουμε κάποιες, χρήσιμες στα επόμενα, ιδιότητες της συνάρτησης $\hat{s}(a)$.

(i) $\hat{s}(a+b) \leq \hat{s}(a) + \hat{s}(b)$, $1 \leq a, b, a+b < q-1$.

Από Θεώρημα 2.2.3 d) έχουμε $g_a g_b = J(\omega^{-a}, \omega^{-b}) g_{a+b}$. Παίρνουμε και στα δύο μέλη ord_S και χρησιμοποιώντας την τρίτη ιδιότητα του ord παίρνουμε το αποτέλεσμα.

(ii) $\hat{s}(a+b) \equiv \hat{s}(a) + \hat{s}(b) \pmod{p-1}$.

Θυμόμαστε ότι $J(\omega^{-a}, \omega^{-b}) \in \mathbb{Q}(\zeta_{q-1})$ και μάλιστα είναι ακέραιος αλγεβρικός, δηλαδή ανήκει στο D_{q-1}. Από το γεγονός ότι $QD_{(q-1)p} = S^{p-1}$ έπεται ότι $(p-1)|ord_S(J(\omega^{-a}, \omega^{-b}))$, λόγω της πολλαπλασιαστικότητας του ord. Το αποτέλεσμα είναι και πάλι συνέπεια της σχέσης $g_a g_b = J(\omega^{-a}, \omega^{-b}) g_{a+b}$.

(iii) $\hat{s}(pa) = \hat{s}(a)$.

Παρατηρούμε ότι $g_{pa} = \sum \omega(t)^{-pa} \psi(t) = \sum \omega(t^p)^{-a} \psi(t^p)$.
Αυτό, διότι με μια απλή εφαρμογή του ορισμού του ίχνους: $tr(t^p) = tr(t)$.
Τώρα ο $t \hookrightarrow t^p$ είναι ένας αυτομορφιμός του F. Συμπεραίνουμε ότι $g_{pa} = g_a$ και άρα $\hat{s}(pa) = \hat{s}(a)$.

Στο πρώτο μέρος της απόδειξης βρήκαμε ότι $\hat{s}(1) = 1$. Χρησιμοποιώντας τα $i), ii)$ θα δείξουμε ότι $\hat{s}(a) = a$, $1 \leq a < p$.

Ξεκινάμε παρατηρώντας ότι από (i) παίρνουμε: $\hat{s}(2) \leq \hat{s}(1) + \hat{s}(1) = 2$.
Από τη (ii) ,τώρα, $\hat{s}(2) \equiv \hat{s}(1) + \hat{s}(1) \pmod{p-1} \Rightarrow \hat{s}(2) \equiv 2 \pmod{p-1}$.
Αλλά, $\hat{s}(2) \leq 2$, άρα $\hat{s}(2) = 2$.

Συνεχίζουμε εντελώς ανάλογα επαγωγικά για $a = 3, 4, ..., p-1$ και αποδεικνύεται ότι $\hat{s}(a) = a$, για κάθε a, $1 \leq a < p$.
Τώρα, παίρνουμε ένα a, $1 \leq a < q-1$ και το γράφουμε στη μορφή που γνωρίζουμε ήδη,

δηλαδή $a = a_o + a_1 p + ... + a_{f-1} p^{f-1}$, $0 \le a_i < p$.

Έχουμε: $\hat{s}(a) = \hat{s}(\sum_{j=0}^{f-1} a_j p^j) \overset{(i)}{\le} \sum_{j=0}^{f-1} \hat{s}(a_j p^j) \overset{(iii)}{=} \sum_{j=0}^{f-1} \hat{s}(a_j) = \sum_{j=0}^{f-1} a_j = S(a)$.

Αποδείξαμε μέχρι στιγμής ότι $\hat{s}(a) \le S(a)$, για κάθε a, $1 \le a < q-1$.

Για να αποδείξουμε το Θεώρημα αρκεί, βάσει του Λήμματος 4.4.3, να δείξουμε ότι $\sum_{a=1}^{q-2} \hat{s}(a) = \frac{f(p-1)(q-2)}{2}$, διότι σε συνδυασμό με το ότι $\hat{s}(a) \le S(a)$ θα μας δώσει το ζητούμενο.
Γενικά, για τα Gauss Sums, έχουμε τη σχέση $g(\chi^{-1}) = \chi(-1)\overline{g(\chi)}$.

Άρα, $g_a g_{q-1-a} = g(\omega^{-a}) g(\omega^{a-(q-1)})$, αλλά ω είναι $(q-1)$-ρίζα της μονάδας.
Επομένως, $g_a g_{q-1-a} = g(\omega^{-a}) g(\omega^a) = \omega(-1)^a \overline{g(\omega^a)} g(\omega^a) = \omega(-1)^a \cdot |g(\omega^a)| = \omega(-1)^a \cdot q = \omega(-1)^a \cdot p^f$.

Γνωρίζουμε από το Λήμμα 4.4.4 ότι $ord_S(p) = p-1$.

Λόγω του ότι το $\omega(-1)^a$ είναι μονάδα, παίρνουμε:
$ord_S(< g_a g_{q-1-a} >) = ord_S[(pD_{q-1})^f] \Rightarrow ord_S(< g_a >) + ord_S(< g_{q-1-a} >) = f \cdot ord_S(pD_{q-1}) \Rightarrow \hat{s}(a) + \hat{s}(q-1-a) = f \cdot (p-1)$.

Αθροίζοντας και τα δύο μέλη για α από 1 έως $q-2$, με επιχείρημα ίδιο με την άθροιση για το $S(a)$, παίρνουμε: $2\sum_{a=1}^{q-2} \hat{s}(a) = f(p-1)(q-2)$.
Αυτό ολοκληρώνει την απόδειξη του Θεωρήματος.

Βήμα 4

Πόρισμα 4.4.9:

$ord_P(< \Phi(P) >) = \frac{m}{p-1} S(\frac{q-1}{m})$.

Απόδειξη:
Ισχύει ότι: $(p-1) ord_P(< \Phi(P) >) = ord_S(< \Phi(P) >)$.

Αυτό, διότι από το (3) του Λήμματος 4.4.4, έχουμε $ord_S(P) = p-1$ και επιπλέον, ισχύει η ισότητα $ord_S(< \Phi(P) >) = ord_S(P) ord_P(< \Phi(P) >)$.

Τώρα, $ord_S(< \Phi(P) >) = m \cdot ord_S(< g(P) >)$, αφού $\Phi(P) = g(P)^m$.

Από Θεώρημα 4.4.8, $ord_S(g_a) = S(a)$, και επειδή το $g(P)$ ισούται με g_a για $a = \frac{q-1}{m}$, έχουμε ότι $ord_S(< g(P) >) = S(\frac{q-1}{m})$.

Συνολικά, έχουμε $mS(\frac{q-1}{m}) = (p-1) \cdot ord_P(< \Phi(P) >) \Rightarrow ord_P(< \Phi(P) >) = \frac{m}{p-1} S(\frac{q-1}{m})$.

-Το Πόρισμα δίνει το πρώτο βήμα για την πλήρη ανάλυση σε πρώτα ιδεώδη του $\Phi(P)$. Συνεχίζουμε παρατηρώντας ότι τα μόνα πρώτα ιδεώδη του D_m στην ανάλυση του $< \Phi(P) >$ είναι αυτά που περιέχουν τον πρώτο p. Αυτό προκύπτει από τα b) και c) της Πρότασης 4.3.4 που δίνουν:

$$|\Phi(P)|^2 = q^m = p^{fm}.$$

Εδώ, $N(P) = p^f$. και επομένως, μόνο αυτός ο πρώτος p που διαιρεί την Norm θα εμφανίζεται στην ανάλυση του P, οπότε ισχύει η υπόθεσή μας.
Αν P' είναι κάποιο άλλο πρώτο ιδεώδες στον D_m που περιέχει τον p, τότε υπάρχει αυτομορφισμός σ_t στο $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ τέτοιος ώστε $P' = P^{\sigma_t^{-1}}$ (Πρόταση 4.1.3). Για $1 \leq t < m$ και $(t, m) = 1$, ορίζουμε $P_t = P^{\sigma_t^{-1}}$.

Λήμμα 4.4.10:

Για το P_t που ορίσαμε πριν, ισχύει: $ord_{P_t}(< \Phi(P) >) = \frac{m}{p-1} S(\frac{t \cdot (q-1)}{m})$.

Απόδειξη:
Ισχύει ότι $ord_(P_t(< \Phi(P) >) = ord_P(< \Phi(P)^{\sigma_t} >)$, γιατί $ord_{P_t}(< \Phi(P) >) = ord_{P^{\sigma_t^{-1}}}(< \Phi(P) >) =$
$= ord_P(< \Phi(P)^{\sigma_t} >)$.

Επιλέγουμε έναν ακέραιο t' τέτοιο ώστε $t' \equiv t \pmod m$ και $t' \equiv 1 \pmod p$ (υπάρχει επειδή $(p, m) = 1$). Τότε:

$$g(P)^{\sigma_{t'}} = (\sum_{r \in F} \chi_P(r)\psi(r))^{\sigma_{t'}} = \sum_{r \in F} \chi_P(r)^t \psi(r),$$

διότι $\chi_P(r)^{t'} \equiv \chi_P(r)^t \pmod m$ και $\psi(rt') \equiv \psi(r) \pmod p$.

Άρα, έχουμε ότι $\Phi(P)^{\sigma_t} = (\sum_{r \in F} \chi_P(r)^t \psi(r))^m$.

Το δεξί μέλος της παραπάνω ισότητας είναι ίσο με g_a^m, όπου $a = \frac{t \cdot (q-1)}{m}$.

Με αιτιολόγηση ίδια με το Πόρισμα 4.4.9 για διαφορετικό a, προκύπτει το αποτέλεσμα του Λήμματος.

-Μπορούμε, τώρα, να καταλήξουμε στην απόδειξη του Θεωρήματος 4.3.5, δηλαδή της σχέσης του Stickelberger.

Απόδειξη της σχέσης του Stickelberger

Έχουμε: p πρώτος, $p \nmid m$, f ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $p^f \equiv 1 \pmod{m}$ και $pD_m = (P_1P_2...P_r)^e$, όπου κάθε P_i έχει βαθμό f και $r = \phi(m)/f$.

Θέτοντας P να είναι ένα εκ των P_i, ορίζουμε, όπως και παλιότερα,
$G_Z(P) = \{\sigma \in G | \sigma(P) = P\}$. Τότε, ισχύει ότι η $G_Z(P)$ είναι μία κυκλική ομάδα με γεννήτορά της το σ_p ([5] Πόρισμα Θεωρήματος 2 Chapter 13), τάξης f.
Αυτό σημαίνει ότι $[G : G_Z(P)] = r$ (βλ. Πρόταση 4.1.8) και αν γράψουμε την G ως ένωση (ξένων μεταξύ τους) συμπλόκων, έχουμε: $G = \bigsqcup_{i=1}^{r} \sigma_{t_i} G_Z(P)$.
Αυτό μας εξασφαλίζει ότι για κάθε $\sigma \in G$ υπάρχει ένα t_i, $i = 1, 2, ..., r$ και ένα j, $j = 0, 1, ..., f-1$, τέτοια ώστε $\sigma = \sigma_{t_i}\sigma_p^j$.
Δηλαδή, τα $\sigma_{t_i} \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = G$ είναι αυτά που μας δίνουν τις διαφορετικές εικόνες του P, δηλαδή $\sigma_{t_i}(P) = P_i$.
Αντί να δουλέψουμε με τα σ_{t_i}, $i = 1, 2, ..., r$, θα πάρουμε των σύνολο των t_i. Θα περάσουμε στην ομάδα μονάδων του δακτυλίου $\mathbb{Z}/m\mathbb{Z}$, $(\mathbb{Z}/m\mathbb{Z})^*$. Άρα, για τους δείκτες των στοιχείων της ομάδας Galois, δηλαδή για τα t, $(t, m) = 1$, μπορούμε να γράψουμε $t \equiv t_i \cdot p^j \pmod{m}$, για μοναδικό ζεύγος (i, j), $1 \le i \le r$ και $0 \le j < f$ (αφού $p^f \equiv 1 \pmod{m}$).

Συνολικά, αν $1 \le t < m$, $(t, m) = 1$, τότε $t \equiv t_i \cdot p^j \pmod{m}$ για μοναδικό ζεύγος (i, j), $0 \le j < f$, $1 \le i \le r$.

-Από το Λήμμα 4.4.10, έχουμε ότι η ανάλυση του $\Phi(P)$ σε πρώτα ιδεώδη δίνεται από: $P^{\gamma'}$, όπου:

$$\gamma' = \frac{m}{p-1} \sum_{i=1}^{r} S\left(t_i \cdot \frac{q-1}{m}\right)\sigma_{t_i}^{-1}.$$

Χρησιμοποιώντας το Λήμμα 4.4.2 και παρατηρώντας ότι $S\left(\frac{t_i \cdot (q-1)}{m}\right) = (p-1)\sum_{i=0}^{f-1}\{\frac{p^j t_i}{m}\}$ παίρνουμε:

$$\gamma' = m \sum_i \left(\sum_j \{\frac{p^j t_i}{m}\}\right)\sigma_{t_i}^{-1}.$$

Αφού, $\sigma_p(P) = P$ (έτσι ορίστηκε), έπεται ότι και $\sigma_{p^j}(P) = P$, για κάθε $j = 0, 1, ..., f-1$. Αφού το σ_P αφήνει σταθερό το P, μπορούμε να προσθέσουμε στους όρους του γ' το $\sigma_{p^j}^{-1}$. Επομένως, το $\gamma = m \sum_{i=1}^{r} \sum_{j=0}^{f-1} \{\frac{p^j t_i}{m}\}\sigma_{t_i}^{-1}\sigma_{p^j}^{-1}$, θα έχει την ίδια επίδραση που έχει το γ'.

$$\gamma = m \sum_i \sum_j \{\frac{p^j t_i}{m}\}\sigma_{t_i}^{-1}\sigma_{p^j}^{-1}$$

$$= m \sum_{t \bmod m} \{\frac{t}{m}\}\sigma_t^{-1}$$

$$=\sum t\sigma_t^{-1}, \quad \text{όπου } 1 \le t < m,\ (t,m) = 1.$$

Αυτό ολοκληρώνει και την απόδειξη.

-Η σχέση του Stickelberger πλέον γράφεται:

$$< \Phi(P) >= P^{m\theta}, \text{ όπου } \quad \theta = \sum_{tmodm}\{\tfrac{t}{m}\}\sigma_t^{-1},\ (t,m) = 1$$

Το στοιχείο $\theta \in \mathbb{Q}[G]$ λέγεται στοιχείο του Stickelberger.

4.5 Η απόδειξη του Νόμου Αντιστροφής του Eisenstein

Θεώρημα Μονάδων του Dirichlet ([6] Θεώρημα $IX.2.1$)
Έστω K αλγεβρικό σώμα αριθμών,

$$[K : \mathbb{Q}] = n = r_1 + 2r_2,$$

ταυτότητας $[r_1, r_2]$, όπου r_1 το πλήθος των πραγματικών και r_2 το πλήθος των μιγαδικών εμφυτεύσεων του K και διακρίνουσας $D_{K/\mathbb{Q}}$. Η ομάδα των μονάδων του σώματος K είναι πεπερασμένα παραγόμενη αβελιανή ομάδα βαθμού $r_1 + r_2 - 1$. Αναλυτικά, ο R_K περιέχει πολλαπλασιαστικά ανεξάρτητες μονάδες $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ άπειρης τάξης ώστε

$$E(R_K) \cong E(R_K)_{\text{torsion}} \otimes \langle\varepsilon_1\rangle \otimes \langle\varepsilon_2\rangle \otimes \cdots \otimes \langle\varepsilon_r\rangle.$$

Το σύνολο $E(R_K)_{\text{torsion}}$ είναι το σύνολο των ριζών της μονάδας που ανήκουν στο K και είναι κυκλική ομάδα τάξης διαιρέτη του $2|D_{K/\mathbb{Q}}|$.

-Πολλαπλασιαστικά ανεξάρτητες μονάδες σημαίνει ότι αν $\varepsilon_1^{m_1} \cdot \varepsilon_2^{m_2} \ldots \cdot \varepsilon_r^{m_r} = 1$, με $m_i \in \mathbb{Z}$, τότε $m_1 = m_2 = \ldots = m_r = 0$.

-Στην ειδική περίπτωση, τώρα, κυκλοτομικού σώματος, ισχύει το ακόλουθο:

Λήμμα 4.5.1:

Οι μοναδικές ρίζες της μονάδας του κυκλοτομικού σώματος $K = \mathbb{Q}(\zeta_m)$, $(m \in \mathbb{N},\ m \ge 2)$ είναι το σύνολο $\{\pm\zeta_m^i |\ i = 1, 2, \ldots, m\}$.

Παρατήρηση: Θα αποδείξουμε το Λήμμα μόνο για την περίπτωση που $m = l$, l πρώτος, διαφορετικός του 2. Ο λόγος που θα το κάνουμε αυτό είναι διότι αυτό χρειαζόμαστε για τα επόμενα.

Έστω $\zeta_n \in \mathbb{Q}(\zeta_l)$, για κάποιο φυσικό αριθμό n.
Διακρίνουμε διάφορες περιπτώσεις:

Πρώτη περίπτωση:
Έστω $n \equiv 0 \pmod 4$, $n = 4k$, $k \in \mathbb{Z}$, άρα και το $\zeta_{4k}^k = i \in \mathbb{Q}(\zeta_l)$, δηλαδή το $\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_l)$.

Υπενθυμίζουμε το Θεώρημα της Διακρίνουσας ([6] Θεώρημα X.2.4) :
Έστω $K/\mathbb{Q}$ επέκταση αλγεβρικών σωμάτων αριθμών και R ο δακτύλιος των ακεραίων αλγεβρικών του K. Έστω p ένας πρώτος αριθμός. Τότε:
(Το p διακλαδίζεται στην $K/\mathbb{Q}$) $\Leftrightarrow$ (Το p διαιρεί την διακρίνουσα $D_{K/\mathbb{Q}}$ του σώματος K).

Εδώ, η διακρίνουσα του $\mathbb{Q}(i)$ είναι -4. Επομένως, το 2 διακλαδίζεται στην επέκταση $\mathbb{Q}(i)/\mathbb{Q}$.

Η διακρίνουσα του $\mathbb{Q}(\zeta_l)$ είναι $D_{\mathbb{Q}(\zeta_l)/\mathbb{Q}} = (-1)^{\frac{l-1}{2}} \cdot l^{l-2}$. ([6] Θεώρημα IV.7.1)

Επομένως, το 2 δεν διακλαδίζεται στο K, αφού ο μόνος πρώτος που διακλαδίζεται είναι το l και υποθέσαμε ότι $l \neq 2$.

Όμως, αυτό είναι άτοπο, αφού ο δείκτης διακλαδώσεως του 2 στην $\mathbb{Q}(i)/\mathbb{Q}$ διαιρεί τον δείκτη διακλαδώσεως του 2 στην $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ (λόγω της πολλαπλασιαστικότητας των δεικτών διακλάδωσης για τον πύργο σωμάτων $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_l)$).

Επομένως, αν $\zeta_n \in \mathbb{Q}(\zeta_l)$, τότε κατ΄ ανάγκη $n \not\equiv 0 \pmod 4$.

Δεύτερη περίπτωση:
Έστω ότι το n διαιρείται με 2, δηλαδή $n \equiv 2 \pmod 4$, οπότε $n = 2 \cdot n_0$, όπου n_0 περιττός.

Το σύνολο $\{\zeta_n^j\} = \{\zeta_n, \zeta_n^2, ..., \zeta_n^{\frac{n}{2}} = \zeta_n^{n_0}, \zeta_n^{n_0+1}, ..., \zeta_n^{2n_0} = 1\} = \{\pm\zeta_{n_0}, \pm\zeta_{n_0}^2, ..., \pm\zeta_{n_0}^{n_0} = \pm 1\}$.

Εξηγούμε γιατί ισχύει η παραπάνω ισότητα: Το $n_0 | n$, άρα $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{n_0}) \subseteq \mathbb{Q}(\zeta_n)$. Όμως, $\phi(n) = \phi(2 \cdot n_0) = \phi(2) \cdot \phi(n_0) = \phi(n_0)$. Δηλαδή, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{n_0}) : \mathbb{Q}]$ και επομένως $\mathbb{Q}(\zeta_{n_0}) = \mathbb{Q}(\zeta_n)$.
Αρκεί να το αποδείξουμε για περιττό n για να ολοκληρωθεί η απόδειξη της Δεύτερης περίπτωσης. Ας το μελετήσουμε στην Τρίτη περίπτωση.

Τρίτη περίπτωση:
Υποθέτουμε ότι ο n είναι περιττός ≥ 3. Θα υπάρχει ένας περιττός πρώτος διαιρέτης του n,

έστω p.
Το $\zeta_n \in \mathbb{Q}(\zeta_l)$ και αν $n = p \cdot k$, $k \in \mathbb{Z}$, το $\zeta_n^k \in \mathbb{Q}(\zeta_l)$ και η τάξη του ζ_n^k είναι p, δηλαδή $\zeta_p = \zeta_n^k \in \mathbb{Q}(\zeta_l)$.
Έχουμε τον πύργο σωμάτων $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_l)$ και εφαρμόζουμε την ίδια διαδικασία με πριν.
Το l είναι ο μοναδικός πρώτος που διακλαδίζεται στο $\mathbb{Q}(\zeta_l)$. Το p διακλαδίζεται στο $\mathbb{Q}(\zeta_p)$, άρα διακλαδίζεται και στο $\mathbb{Q}(\zeta_l)$. Άρα, $p = l$ και άρα κατ΄ ανάγκη $n = l^a$, $a \in \mathbb{N}$. Ο βαθμός της επέκτασης $[\mathbb{Q}(\zeta_{l^a}) : \mathbb{Q}] = \phi(l^a) = l^{a-1} \cdot (l-1)$.

Επίσης, $[\mathbb{Q}(\zeta_l) : \mathbb{Q}] = l - 1$.
Άρα, $l^{a-1} \cdot (l-1) | (l-1) \Rightarrow a = 1$.

Και πάλι οι μοναδικές ρίζες του $\mathbb{Q}(\zeta_l)$ είναι $\{\pm\zeta_l^j | \ j = 1, 2, ..., l\}$, δηλαδή η απόδειξη του Λήμματος.

Παρατηρήσεις:
1) Για την πλήρη απόδειξη του Λήμματος, για κάθε $m \in \mathbb{N}$ ($m > 1$) παραπέμπουμε στο [[7] σελ. 212] από την απόδειξη του οποίου προκύπτει ότι πάντοτε το $-\zeta_m$ είναι γεννήτορας της (κυκλικής) ομάδας των ριζών της μονάδας του $\mathbb{Q}(\zeta_m)$, όπου ζ_m πρωταρχική m-ρίζα της μονάδας.

2) Επίσης, παραπέμπουμε στο άρθρο του Keth Conrad, Cyclotomic Extensions, Thm. 3.5:
Έστω m, n θετικοί ακέραιοι.
(1) Το πλήθος των ριζών της μονάδας στο $\mathbb{Q}(\zeta_m)$ είναι $lcm(2, m)$.
(2) Αν $m \neq n$, τότε $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ αν και μόνο αν $\{m, n\} = \{k, 2k\}$ για κάποιον περιττό k.

Λήμμα 4.5.2:

Έστω $K/\mathbb{Q}$ επέκταση ενός αλγεβρικού σώματος αριθμών K υπέρ το $\mathbb{Q}$ και έστω $n = [K : \mathbb{Q}]$. Άρα, υπάρχουν ακριβώς n διαφορετικοί μεταξύ τους μονομορφισμοί του K στο $\mathbb{C}$, έστω $\sigma_1, \sigma_2, ..., \sigma_n$. Αν το $\alpha \in R_K$ (τον δακτύλιο των ακεραίων αλγεβρικών του K) τέτοιο ώστε $|\alpha^{\sigma_i}| \leq 1$ για κάθε $i = 1, 2, ..., n$, τότε το α είναι ρίζα της μονάδας.

Απόδειξη:
Το α είναι ακέραιος αλγεβρικός. Επομένως, για το ανάγωγο πολυώνυμο του α υπέρ το $\mathbb{Q}$, έχουμε $p(X) \in \mathbb{Z}[X]$. Έστω $f(X)$ το χαρακτηριστικό πολυώνυμο του α. Το $f(X)$ είναι δύναμη του αναγώγου, άρα και αυτό με ακέραιους συντελεστές, και έχει ως ρίζες του ακριβώς το σύνολο $\{\alpha^{\sigma_i} | \ i = 1, ..., n\}$, δηλαδή $f(X) = \prod_{i=1}^{n}(X - \alpha^{\sigma_i}) \in \mathbb{Z}[x]$.

Άρα, ο συντελεστής του ενδιάμεσου όρου X^m του πολυωνύμου $f(X)$ θα είναι όλα τα $\binom{n}{m}$

δυνατά αθροίσματα όλων των δυνατών γινομένων των $\{\alpha^{\sigma_i} |\ i = 1, ..., n\}$ ανά m. Δηλαδή, οι συντελεστές είναι συμμετρικές συναρτήσεις των $\sigma_1(\alpha), \sigma_2(\alpha), ..., \sigma_n(\alpha)$.
Επομένως, ο συντελεστής του X^m φράσσεται από το $\binom{n}{m}$, από το οποίο συνεπάγεται ότι υπάρχουν πεπερασμένου πλήθους ακέραιοι συντελεστές σε κάθε όρο του πολυωνύμου.
Συνεπώς, υπάρχουν πεπερασμένου πλήθους τέτοια πολυώνυμα $f(x)$ βαθμού n.
Όταν το α επαληθεύει την υπόθεση του Λήμματος, το ίδιο ισχύει και για οποιαδήποτε δύναμη του α. ($\sigma_i(\alpha^m) \leq 1$ για κάθε $i = 1, 2, ..., n$ και κάθε $m \in \mathbb{N}$, αφού ισχύει $\sigma_i(\alpha) \leq 1$)

Πεπερασμένου πλήθους πολυώνυμα (βαθμού n) έχουν πεπερασμένου πλήθους ρίζες.
Επομένως, κάποιες δυνάμεις του α θα είναι ίσες. Έστω $\alpha^k = \alpha^m$, $k, m \in \mathbb{N}$, $k \neq m$.
Χωρίς βλάβη της γενικότητας, έστω $k > m$. Τότε $\alpha^{k-m} = 1$ και άρα το α είναι μία ρίζα της μονάδας.
-Το επόμενο βήμα είναι να ορίσουμε το Φ(A) για ένα τυχαίο ιδεώδες του D_m, $m \notin A$ και να μελετήσουμε τις ιδιότητες αυτής της συνάρτησης. Συγκεκριμένα, θα είναι σημαντικό στα επόμενα να ορίσουμε το Φ σε κύρια ιδεώδη.

Ορισμός:

Έστω $A \subset D_m$ ένα ιδεώδες και υποθέτουμε ότι $m \notin A$. Έστω $A = P_1...P_n$ η ανάλυση του A σε γινόμενο πρώτων ιδεωδών (όχι κατ' ανάγκη διαφορετικών). Ορίζουμε:

$$\Phi(A) := \Phi(P_1)...\Phi(P_n).$$

Πρόταση 4.5.3:

Έστω $A, B \subset D_m$ ιδεώδη πρώτα προς το m και $\alpha \in D_m$ ένα στοιχείο πρώτο προς το m. Θυμόμαστε ότι $\gamma = \sum_t t\sigma_t^{-1}$, $1 \leq t < m$ και $(t, m) = 1$. Τότε:
a) $\Phi(A) \cdot \Phi(B) = \Phi(A \cdot B)$
b) $|\Phi(A)|^2 = (N(A))^m$
c) $< \Phi(A) >= A^\gamma$
d) $\Phi(< \alpha >) = \epsilon(\alpha)\alpha^\gamma$, όπου $\epsilon(\alpha)$ είναι μονάδα στον D_m.

Απόδειξη:
Το *a*) είναι προφανές από τον ορισμό.
Για το *b*), εφόσον και τα δύο μέλη είναι πολλαπλασιαστικά ως προς το A, μπορούμε να υποθέσουμε ότι το A είναι ένα πρώτο ιδεώδες P. Σε αυτήν την περίπτωση $|\Phi(P)|^2 = |g(P)|^{2 \cdot m} = (N(P))^m$ (Πρόταση 4.3.4 *b*)).
Για το *c*), και τα δύο μέλη είναι πολλαπλασιαστικά ως προς A, οπότε ξανά μπορούμε να υποθέσουμε ότι το A είναι ένα πρώτο ιδεώδες P. Το αποτέλεσμα είναι, βασικά, η σχέση

του Stickelberger. (Θεώρημα 4.3.5)
Για το d) εφαρμόζουμε την c) για $A =< \alpha >$ και έχουμε:

$$< \Phi(< \alpha >) >=< \alpha >^{\gamma}=< \alpha^{\gamma} >$$

Άρα, τα $< \Phi(< \alpha >) >$ και $< \alpha^{\gamma} >$ είναι δύο ίσα, κύρια ιδεώδη και άρα αναγκαστικά διαφέρουν κατά μία μονάδα του D_m που εξαρτάται προφανώς από το α, έστω $\epsilon(\alpha)$, δηλαδή $\Phi(< \alpha >) = \epsilon(\alpha)\alpha^{\gamma}$.

Λήμμα 4.5.4:

Έστω $A \subset D_m$ ένα ιδεώδες πρώτο προς το m και έστω σ ένας αυτομορφισμός του $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Τότε:

$$\Phi(A)^{\sigma} = \Phi(A^{\sigma}).$$

Απόδειξη:
Ξεκινάμε γράφοντας το $g(P)$ στη μορφή:

$$g(P) = \sum \left(\frac{\alpha}{P}\right)_m^{-1} \zeta_p^{tr(\overline{\alpha})},$$

όπου το άθροισμα είναι πάνω ένα σύνολο αντιπροσώπων των συμπλόκων του δακτυλίου D_m/P.

Έστω $\hat{\sigma}$ ένας αυτομορφισμός του $\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q}$, ο οποίος περιορίζεται σε σ στον $\mathbb{Q}(\zeta_m)$ και στην ταυτότητα στον $\mathbb{Q}(\zeta_p)$ (βλ. Απόδειξη Λήμματος 4.4.10.).

Εφαρμόζουμε στο $g(P)$ τον αυτομορφισμό $\hat{\sigma}$ και έχουμε:

$$g(P)^{\hat{\sigma}} = \sum \left(\frac{\alpha^{\sigma}}{P^{\sigma}}\right)_m^{-1} \zeta_p^{tr(\overline{\alpha})}.$$

Για την παραπάνω ισότητα κάναμε χρήση της Πρότασης 4.2.6.
Αφού, $tr(\overline{\alpha}) \in \mathbb{Z}/p\mathbb{Z}$, έχουμε $tr(\alpha) = tr(\overline{\alpha}^{\sigma})$ και έπεται ότι $g(P)^{\hat{\sigma}} = g(P^{\sigma})$. Υψώνοντας και τα δύο μέλη εις την m-οστή δύναμη παίρνουμε το αποτέλεσμα $\Phi(P)^{\sigma} = \Phi(P^{\sigma})$ για πρώτο ιδεώδες P. Από την πολλαπλασιαστικότητα του Α, το αποτέλεσμα προκύπτει να ισχύει για κάθε ιδεώδες.

Λήμμα 4.5.5:

Για κάθε $\alpha \in D_m$, $|\alpha^{\gamma}|^2 = |N\alpha|^m$.

Απόδειξη:
Ο αυτομορφισμός σ_{-1} είναι η μιγαδική συζυγία στο σώμα $\mathbb{Q}(\zeta_m)$, αφού στέλνει το ζ_m στο $\zeta_m^{-1} = \overline{\zeta_m}$.

$$\text{Άρα, } \ |\alpha^\gamma|^2 = \alpha^\gamma \overline{\alpha^\gamma} = \alpha^\gamma (\alpha^\gamma)^{\sigma_{-1}} = \alpha^{\gamma(1+\sigma_{-1})}.$$

Τώρα, $\sigma_{-1}\gamma = \sigma_{-1} \sum t\sigma_t^{-1} = \sum t\sigma_{-t}^{-1}$.

Προφανώς, αφού ζ_m έχει τάξη m, θα ισχύει $\sigma_{m-t} = \sigma_{-t}$ και επομένως $\gamma = \sum (m-t)\sigma_{m-t}^{-1}$.

Έχουμε:

$$(1+\sigma_{-1})\gamma = \sum_t t\sigma_{-t}^{-1} + \sum (m-t)\sigma_{m-t}^{-1} = \sum_t m\sigma_{m-t}^{-1} = m\sum_t \sigma_{m-t}^{-1} = m\sum \sigma_{-t}^{-1}$$

Από την άλλη, $N\alpha = \prod \alpha^{\sigma_{-t}^{-1}} = \alpha^{\sum \sigma_{-t}^{-1}}$ και το αποτέλεσμα έπεται.

Πρόταση 4.5.6:

Έστω $\alpha \in D_m$, α πρώτο προς το m. Ισχύει ότι $\Phi(\alpha) = \epsilon(\alpha)\alpha^\gamma$, όπου $\epsilon(\alpha) = \pm\zeta_m^i$ για κάποιο i.

Απόδειξη:
Βάσει του d) της Πρότασης 4.5.3 είναι αρκετό να αποδείξουμε τη μορφή που θα έχει το $\epsilon(\alpha)$.
Έχουμε $|\Phi(A)|^2 = (N < \alpha >)^m$, πάλι από Πρόταση 4.5.3 και $|\alpha^\gamma|^2 = |N\alpha|^m$ από το προηγούμενο Λήμμα. Επίσης $N(< \alpha >) = |N\alpha|$ από Πρόταση 4.1.10.
Συνδυάζοντάς τα όλα αυτά, παίρνουμε ότι $|\epsilon(\alpha)|^2 = 1 \Rightarrow |\epsilon(\alpha)| = 1$.

Κάνοντας χρήση του Λήμματος 4.5.4, έχουμε: $|\epsilon(\alpha)^\sigma| = 1$ για κάθε $\sigma \in G$.
Βάσει αυτού, από το Λήμμα 4.5.2 παίρνουμε ότι η $\epsilon(\alpha)$ είναι μία ρίζα της μονάδας. Τέλος, αφού $\epsilon(\alpha) \in \mathbb{Q}(\zeta_m)$ και το $\epsilon(\alpha)$ είναι μία ρίζα της μονάδας, θα είναι $\epsilon(\alpha) = \pm\zeta_m^i$, από Λήμμα 4.5.1.

-Είμαστε, πλέον, σε θέση να ξεκινήσουμε την απόδειξη του Νόμου Αντιστροφής του Eisenstein. Το μοτίβο της απόδειξης θα πρέπει να μας είναι αρκετά οικείο από τις αποδείξεις του τετραγωνικού, κυβικού και διτετραγωνικού νόμου αντιστροφής.

Πρόταση 4.5.7:

Έστω $P, P^{'} \in D_m$, πρώτα προς το m. Υποθέτουμε ότι $NP, NP^{'}$ είναι σχετικά πρώτα στοιχεία. Τότε:

$$\left(\frac{\Phi(P)}{P'}\right)_m = \left(\frac{NP'}{P}\right)_m .$$

Απόδειξη:

Έστω $q^{'} = p^{'f^{'}} = NP^{'}$. Θυμόμαστε ότι $q^{'} \equiv 1 \pmod m$.
Οι ακόλουθες ισοτιμίες είναι $mod p^{'}$ στον D_m.

$g(P)^{q^{'}} \equiv \sum \chi_P(t)^{q^{'}} \psi(t)^{q^{'}} \equiv \sum \chi_P(t)\psi(q^{'}t) = \frac{1}{\chi_P(q^{'})} \sum \chi_P(q^{'}t)\psi(q^{'}t) \equiv \left(\frac{q^{'}}{P}\right)_m g(P) \pmod{P^{'}}$.

Από την άλλη, $g(P)^{q^{'}-1} = \Phi(P)^{\frac{q^{'}-1}{m}} \equiv \left(\frac{\Phi(P)}{P'}\right)_m \pmod{P^{'}}$.

Συνολικά, $\left(\frac{\Phi(P)}{P'}\right)_m \equiv \left(\frac{NP'}{P}\right)_m \pmod{P^{'}}$.

Αφού $m \notin P$, τα δύο μέλη της ισοτιμίας θα είναι και ίσα.

Πόρισμα 4.5.8:

Έστω A,B $\subset D_m$ δύο ιδεώδη πρώτα προς το m και NA, NB είναι στοιχεία σχετικά πρώτα μεταξύ τους. Τότε:

$$\left(\frac{NB}{A}\right)_m = \left(\frac{\Phi(A)}{B}\right)_m .$$

Απόδειξη:
Το Πόρισμα προκύπτει άμεσα από την προηγούμενη Πρόταση λόγω της πολλαπλασιαστικότητας των συναρτήσεων Φ και Norm.

Πόρισμα 4.5.9:

Έστω A,B να είναι τέτοια ώστε να πληρούνται οι ίδες υποθέσεις με του Πορίσματος 4.5.8. Επίσης, υποθέτουμε ότι $A =< \alpha >$ ένα κύριο ιδεώδες. Τότε:

$$\left(\frac{\epsilon(\alpha)}{B}\right)_m \cdot \left(\frac{\alpha}{NB}\right)_m = \left(\frac{NB}{\alpha}\right)_m .$$

Απόδειξη:
Αρχικά:

$$\left(\frac{\Phi(\alpha)}{B}\right)_m = \left(\frac{\epsilon(\alpha)}{B}\right)_m \cdot \left(\frac{\alpha^\gamma}{B}\right)_m$$

Παρατηρούμε ότι: $\left(\frac{\alpha^{t\sigma_t^{-1}}}{B}\right)_m = \left(\frac{\alpha^{\sigma_t^{-1}}}{B}\right)_m^t = \left(\frac{\alpha^{\sigma_t^{-1}}}{B}\right)_m^{\sigma_t} = \left(\frac{\alpha}{B^{\sigma_t}}\right)_m$.

Η τελευταία ισότητα προκύπτει λόγω της Πρότασης 4.2.6.
Άρα:

$$\left(\frac{\alpha^\gamma}{B}\right)_m = \prod_t \left(\frac{\alpha^{t\sigma_t^{-1}}}{B}\right)_m = \prod_t \left(\frac{\alpha}{B^{\sigma_t}}\right)_m = \left(\frac{\alpha}{\prod_t B^{\sigma_t}}\right)_m = \left(\frac{\alpha}{NB}\right)_m.$$

Για να πάρουμε την τελευταία ισότητα έχουμε χρησιμοποιήσει την Πρόταση 4.1.8.

-Από εδώ και πέρα θα υποθέσουμε ότι $m = l$, όπου l είναι ένας περιττός πρώτος.

Λήμμα 4.5.10:

Αν $A \subset D_l$ είναι ένα ιδεώδες πρώτο προς το l, τότε $\Phi(A) \equiv \pm 1 \pmod{l}$.

Απόδειξη:
Αρκεί να δείξουμε ότι $\Phi(P) \equiv -1 \pmod{l}$, όπου $P \subset D_l$ είναι πρώτο ιδεώδες πρώτο προς το l. Έχουμε:

$$\Phi(P) = g(P)^l \equiv \sum_t \chi_p(t)^l \psi(t)^l \pmod{l} \equiv \sum_{t\neq 0} \psi(lt) \equiv -1 \pmod{l}.$$

Η τελευταία ισοτιμία προκύπτει από το γεγονός ότι $l \longrightarrow \psi(lt)$ είναι ένας μη τετριμμένος προσθετικός χαρακτήρας στον D_l/P και άρα το άθροισμα πάνω από όλες τις τιμές του t είναι μηδέν. Εδώ, από το άθροισμα εξαιρείται η τιμή 0, άρα το συνολικό αποτέλεσμα θα είναι $-\psi(0) = -1$.

Θυμόμαστε σε αυτό το σημείο ότι το $\alpha \in D_l$ είναι primary αν το α είναι πρώτο προς το l και $\alpha \equiv x \pmod{(1-\zeta_l)^2}$, για κάποιο $x \in \mathbb{Z}$.

Λήμμα 4.5.11:

Αν $\alpha \in D_l$ είναι primary, τότε $\epsilon(\alpha) = \pm 1$.

Απόδειξη:
Αφού $(1 - \zeta_l)$ είναι το μοναδικό πρώτο στοιχείο πάνω από το l στον D_l, έχουμε ότι $\sigma(< 1 - \zeta_l >) =< 1 - \zeta_l >$, για κάθε $\sigma \in G$.
Αυτό, διότι γνωρίζουμε ότι αν πάρουμε ένα πρώτο ιδεώδες P του $\mathbb{Q}(\zeta_l)$ και δράσουμε με οποιοδήποτε στοιχείο της ομάδας Galois, τότε $\sigma(P)$ είναι επίσης πρώτο και εμφανίζεται στην ανάλυση του P σε γινόμενο πρώτων ιδεωδών στον D_l. (βλ. Πρόταση 4.1.9 *a*))
Εδώ, όμως, έχουμε ένα μοναδικό πρώτο ιδεώδες, άρα αναγκαστικά ο αυτομορφισμός θα το στέλνει πάλι στον εαυτό του.

Επιπλέον, $< 1 - \zeta_l >^{\gamma} = \prod_{t=1}^{l-1} [\sigma_t^{-1}(< 1 - \zeta_l >)]^t \subset < 1 - \zeta_l >$ (όπου $\gamma = \sum_t t\sigma_t^{-1}$).

Τώρα, αφού $\Phi(< \alpha >) = \epsilon(\alpha)\alpha^{\gamma}$ από Πρόταση 4.5.3 *d*) και $\Phi(< \alpha >) \equiv \pm 1 \pmod{l}$ από Λήμμα 4.5.10, συμπεραίνουμε ότι $\epsilon(\alpha)\alpha^{\gamma} \equiv \pm 1 \pmod{l}$.

Επιπλέον, αφού α primary, έχουμε ότι $\alpha \equiv x \pmod{< 1 - \zeta_l >^2}$. Παρατηρούμε ότι:

$$\alpha^{\gamma} \equiv x^{\gamma} \equiv x^{1+2+\ldots+(l-1)} \pmod{< 1 - \zeta_l >^2}$$

Η παραπάνω ισοτιμία ισχύει, διότι, αρχικά, το t διατρέχει όλα τα στοιχεία του F_l που είναι πρώτα προς το l, δηλαδή τα $1, 2, \ldots, l-1$, και επιπλέον $x \in \mathbb{Z} \subseteq \mathbb{Q}$, με την ομάδα Galois να αφήνει τα στοιχεία του $\mathbb{Q}$ αναλλοίωτα.

Τώρα, από Fermat έχουμε: $x^{(l-1)/2} \equiv \pm 1 \pmod{l}$. (Εφόσον α primary και α πρώτο προς το l, θα έχουμε και ότι το x είναι πρώτο προς το l και άρα εφαρμόζεται το Fermat.)

Άρα, $\alpha^{\gamma} \equiv (-1)^l \equiv \pm 1 \pmod{< 1 - \zeta_l >^2}$.

Έπεται από το τελευταίο ότι $\epsilon(\alpha) \equiv \pm 1 \pmod{< 1 - \zeta_l >^2}$. Από την Πρόταση 4.5.6 γνωρίζουμε ότι $\epsilon(\alpha) = \pm\zeta_l^i$. Προκύπτει ότι $\zeta_l^i \equiv \pm 1 \pmod{< 1 - \zeta_l >^2}$.

Για να ολοκληρώσουμε την απόδειξη αρκεί να δείξουμε ότι $l | i$. Αυτό είναι προφανές από το Λήμμα 4.2.7, εφόσον το ίδιο το α είναι primary και άρα το $\zeta_l^i\alpha$ που θα είναι primary είναι το ίδιο το α και άρα $i \equiv 0 \pmod{l}$.

Ας δούμε όμως και έναν δεύτερο τρόπο. Έχουμε: $\zeta_l^i \equiv \pm 1 \pmod{< 1 - \zeta_l >^2}$. Γράφοντας $\zeta_l = 1 - (1 - \zeta_l)$ παίρνουμε: $\zeta_l^i \equiv 1 - i(1 - \zeta_l) \equiv \pm 1 \pmod{< 1 - \zeta_l >^2}$.

Αν ίσχυε το μείον στην ισοτιμία, θα είχαμε $(1-\zeta_l)^2|(2-i(1-\zeta_l))$ και άρα $mod(1-\zeta_l)$ θα παίρναμε ότι $(1-\zeta_l)|2$, πράγμα άτοπο. Αντιθέτως, για το συν, αφαιρώντας και από τα δύο μέλη το 1 παίρνουμε $(1-\zeta_l)|i$ και άρα $l|i$, όπως θέλαμε να δειξουμε.

Πρόταση 4.5.12:

Αν $\alpha \in D_l$ είναι primary, B ένα ιδεώδες πρώτο προς τον l και NB είναι πρώτη προς το α, τότε:

$$\left(\frac{\alpha}{NB}\right)_l = \left(\frac{NB}{\alpha}\right)_l.$$

Απόδειξη:
Από το Πόρισμα 4.5.9 αρκεί να δείξουμε ότι $\left(\frac{\epsilon(\alpha)}{B}\right)_l = 1$. Αφού το α είναι primary από το παραπάνω Λήμμα παίρνουμε: $\epsilon(\alpha) = \pm 1$.

Τώρα, αν P κάποιο πρώτο ιδεώδες, από Πόρισμα 4.2.4 έχουμε: $\left(\frac{\pm 1}{P}\right)_l = (\pm 1)^{\frac{NP-1}{l}}$. Αλλά, η Norm ενός πρώτου ιδεώδους είναι μία δύναμη κατάλληλου πρώτου p, έστω p^f. Συνολικά, $p^f - 1$ είναι άρτιος και άρα $(p^f-1)/l$ είναι άρτιος. Τελικά, $\left(\frac{\pm 1}{P}\right) = 1$ και από πολλαπλασιαστικότητα του συμβόλου προκύπτει η υπόθεση για τυχαίο ιδεώδες $B \in D_l$.

Απόδειξη Νόμου Αντιστροφής του Eisenstein

-Για το τελευταίο βήμα της απόδειξης, έστω $p \in \mathbb{Z}$ ένας πρώτος, διαφορετικός του l και p πρώτος προς το $\alpha \in D_l$. Έστω P ένα πρώτο ιδεώδες στον D_l που περιέχει το p. Τότε $NP = p^f$. Στην Πρόταση που αποδείξαμε μόλις, αντικαθιστώντας όπου B το P παίρνουμε το αποτέλεσμα:

$$\left(\frac{\alpha}{p}\right)_l^f = \left(\frac{p}{\alpha}\right)_l^f.$$

Αφού $f|(l-1) = [\mathbb{Q}(\zeta_l) : \mathbb{Q}]$, συμπεραίνουμε ότι $(f, l) = 1$.
Άρα:

$$\left(\frac{\alpha}{p}\right)_l = \left(\frac{p}{\alpha}\right)_l.$$

Αυτό διότι αν $\left(\frac{\alpha}{p}\right)_l = \zeta_l^i$ και $\left(\frac{p}{\alpha}\right)_l = \zeta_l^j$, έχουμε ότι $\zeta_l^{fi} = \zeta_l^{fj} \Rightarrow \zeta_l^{f(i-j)} = 1$. Όμως, ζ_l είναι μία πρωταρχική l-ρίζα του 1 και άρα πρέπει $l|f(i-j)$. Τα l και f είναι πρώτα μεταξύ τους και άρα καταλήγουμε ότι $l|(i-j)$, $0 \le i, j < l$. Συμπεραίνουμε ότι $i = j$ και επομένως προκύπτει η ισότητα.
Από αυτό και λόγω της πολλαπλασιαστικότητας, συμπεραίνουμε ότι $\left(\frac{\alpha}{b}\right)_l = \left(\frac{b}{\alpha}\right)_l$ για όλα τα $b \in \mathbb{Z}$ πρώτα προς το l και προς το α, δεδομένου ότι α είναι primary.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Ι.Α Αντωνιάδης, Α.Κοντογεώργης, Θεωρία Αριθμών και Εφαρμογές, KALLIPOS, https://https://repository.kallipos.gr/handle/11419/107

[2] F.Lemmermyer, Reciprocity Laws, From Euler to Eisenstein, Springer-Verlag, 2000

[3] Βικιπαίδεια για ιστορικά στοιχεία

[4] F.Lemmermyer, Introduction to Number Theory, Notes 2000

[5] A Classical Introduction to Modern Number Theory Second Edition, Ireland and Rosen, Springer-Verlag New York 1990 (Το βιβλίο στο οποίο βασιστήκαμε περισσότερο για την εργασία)

[6] Ι.Α Αντωνιάδης, Α.Κοντογεώργης, Αλγεβρική Θεωρία Αριθμών, KALLIPOS, https://repository.kallipos.gr/handle/11419/8007

[7] A.Frölich, M.J Taylor Algebraic Number Theory, CUP Cambridge 1991