Gauss και Αριθμητική

Εμμανουήλ Γ. Τσακνάκης

Μεταπτυχιακή Εργασία

Επιβλέπων Καθηγητής κ. Γιάννης Α. Αντωνιάδης

Τμήμα Μαθηματικών

Πανεπιστημίου Κρήτης

Δεκέμβριος 2007

Η μεταπτυχιακή αυτή εργασία πραγματοποιήθηκε στο Τμήμα Μαθηματικών του Πανεπιστημίου Κρήτης, στα πλαίσια του Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών με τίτλο "Μαθηματικά και οι Εφαρμογές τους", στην κατεύθυνση "Μαθηματικά για την Εκπαίδευση" και κατατέθηκε τον Δεκέμβριο του 2007.

Την επιτροπή αξιολόγησης αποτέλεσαν οι κύριοι:

Γιάννης Α. Αντωνιάδης (επιβλέπων καθηγητής)

Χρήστος Κουρουνιώτης

Νίκος Τζανάκης

Πρόλογος

Ένας από τους μεγαλύτερους και παραγωγικότερους μαθηματικούς που υπήρξαν ποτέ είναι αδιαμφισβήτητα ο Carl Friedrich Gauss (1777-1855). Η εργασία αυτή έγινε με στόχο να γνωρίσει ο αναγνώστης τον Gauss μέσα από το μαθηματικό του έργο. Είναι φυσικά αδύνατο να καταπιαστεί κανείς με όλες τις περιοχές που ασχολήθηκε ο ιδιοφυής μαθηματικός σε μία μόνο εργασία, αλλά πιστεύω ότι έχει γίνει μια καλή επιλογή για το έργο του στη θεωρία αριθμών και την άλγεβρα.

Θα δούμε λοιπόν τα αποτελέσματα του Gauss για τα κατασκευάσιμα κανονικά n-γωνα (δουλεύοντας 30 χρόνια πριν τον Galois συνέδεσε τα ενδιάμεσα σώματα της κυκλοτομικής επέκτασης $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ με τις υποομάδες της $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, κατασκευάζοντας το κανονικό 17-γωνο και αποδεικνύοντας ότι αν p πρώτος του Fermat, τότε το κανονικό p-γωνο κατασκευάζεται με κανόνα και διαβήτη), για τον τετραγωνικό νόμο αντιστροφής (ο Gauss ήταν ο πρώτος που απέδειξε τον τετραγωνικό νόμο αντιστροφής, δίνοντας συνολικά οκτώ αποδείξεις) και για το θεώρημα των πολύγωνων αριθμών (απέδειξε την ισχύ του θεωρήματος για την περίπτωση των τρίγωνων αριθμών), την ιστορία των προβλημάτων αυτών, αλλά και την εξέλιξη τους μετά τον Gauss.

Το εντυπωσιακό είναι ότι όλες του οι ανακαλύψεις που θα δούμε έγιναν το έτος 1796, όταν ο Gauss ήταν μόλις 19 ετών, χαρακτηρίζοντας το σαν μία από τις παραγωγικότερες περιόδους της ζωής του.

Μία από τις πρώτες παρατηρήσεις που μπορεί να κάνει κανείς είναι ότι απουσιάζει από την εργασία το Θεμελιώδες Θεώρημα της Άλγεβρας, ένα από τα σημαντικότερα αποτελέσματα του Gauss. Αυτό έχει ως αιτία την κυκλοφορία του βιβλίου "Το θεμελιώδες Θεώρημα της Άλγεβρας" (G. Rosenberger και F. Benjamin, εκδόσεις Leader Books) και μία δική μας αναφορά στο θεώρημα δε θα πρόσφερε κάτι νέο στην Ελληνική βιβλιογραφία.

Τέλος θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κ. Γιάννη Α. Αντωνιάδη που χωρίς την πολύτιμη βοήθεια και καθοδήγηση του δε θα είχε γίνει αυτή η εργασία, καθώς και την οικογένεια μου για τη στήριξη της όλα αυτά τα χρόνια.

Εμμανουήλ Γ. Τσακνάκης

Περιεχόμενα

Κεφάλαιο 1

Κατασκευάσιμα κανονικά n-γωνα

1.1 Εισαγωγή

Όταν ο Gauss άφησε το κολλέγιο Carolinum τον Οκτώβριο του 1795 για να σπουδάσει στο Πανεπιστήμιο του $Göttingen$ είχε το δίλημμα για το αν θα συνέχιζε τις σπουδές του στα μαθηματικά ή στην άλλη του μεγάλη αγάπη, τις γλώσσες. Μια ανακάλυψή του όμως έμελε να χαράξει την πορεία του σα μεγάλου μαθηματικού. Σε ηλικία μόλις 19 ετών (30 Μαρτίου 1796) ο Gauss κατασκεύασε το κανονικό 17-γωνο (η απόδειξη βρίσκεται στο Disquisitiones Arithmiticae, κεφάλαιο 7, άρθρο 365, το οποίο αν και ολοκληρώθηκε το 1798, όταν ο Gauss ήταν 21 ετών, δημοσιεύθηκε το 1801, δείτε [9]).

Ο Gauss ήταν πολύ περήφανος για αυτή του την ανακάλυψη (αναφέρει μάλιστα ότι από την εποχή του Ευκλείδη ήταν γνωστή η κατασκευή του ισοπλεύρου τριγώνου καθώς και του κανονικού πενταγώνου, αλλά καμία πρόοδος δε σημειώθηκε για 2000 χρόνια) και εξέφρασε την επιθυμία η επιτάφια πλάκα του να έχει χαραγμένο το κανονικό 17-γωνο. Η επιθυμία του δεν πραγματοποιήθηκε, αφού ο γλύπτης το αρνήθηκε λέγοντας ότι θα μοιάζει περισσότερο με κύκλο.

Εδώ θα πρέπει να σημειώσουμε ότι η ανακάλυψη του Gauss είναι πολύ σημαντική για έναν ακόμα λόγο. Για πρώτη φορά χρησιμοποιήθηκε μια τεχνική που αργότερα έγινε από τις πιο χρήσιμες στην ιστορία των μαθηματικών, η μεταφορά δηλαδή ενός προβλήματος από μία περιοχή σε μια άλλη. Στη συγκεκριμένη περίπτωση έχουμε τη μεταφορά ενός προβλήματος της γεωμετρίας στην άλγεβρα.

Ο Gauss απέδειξε επίσης ότι το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη όταν $n = 2^r p_1 ... p_s$, όπου οι p_i να είναι διαφορετικοί πρώτοι της μορφής

$2^{2^n}+1$. Ο Gauss ήταν βέβαιος για την ισχύ του αντιστρόφου, δεν κατάφερε όμως να το αποδείξει. Την απόδειξη έδωσε ο Pierre Wantzel (1814-1848) το 1837.

Οι πρώτοι της μορφής $F_n = 2^{2^n}+1$ ονομάζονται πρώτοι του Fermat. Ο Fermat διατύπωσε τον ισχυρισμό ότι όλοι οι αριθμοί της μορφής αυτής είναι πρώτοι, εικασία που κατέρριψε ο Euler δείχνοντας ότι ο 641 διαιρεί τον $F_5 = 2^{2^5}+1$. Λόγω του αποτελέσματος του Euler, λίγο ενδιαφέρον δόθηκε στη συνέχεια για τους πρώτους του Fermat, μέχρι ο Gauss να δείξει τη σχέση τους με την κατασκευασιμότητα των κανονικών n-γώνων.

Μέχρι σήμερα δεν έχει βρεθεί άλλος πρώτος του Fermat μετά τον F_4. Δηλαδή οι $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ και $F_4 = 65537$ είναι οι μόνοι γνωστοί πρώτοι του Fermat. Μέχρι τις 2 Ιουνίου 2007 είχε αποδειχθεί ότι για $n = 5, 6, 7, ..., 32, 36, ..., 39, 42, 43$ και για άλλες 196 τιμές του n με $43 < n \leq 2478782$ οι F_n είναι σύνθετοι, συνολικά 230 αριθμοί.

Θα δούμε στη συνέχεια ότι αν το κανονικό m-γωνο και το κανονικό n-γωνο είναι κατασκευάσιμα και (m,n)=1, τότε και το κανονικό mn-γωνο καθώς και το κανονικό 2n-γωνο είναι κατασκευάσιμα. Επομένως το πρόβλημα της κατασκευασιμότητας των κανονικών n-γώνων ανάγεται στο πρόβλημα της κατασκευής του κανονικού p-γώνου, όπου p πρώτος του Fermat.

Το ισόπλευρο τρίγωνο καθώς και το κανονικό 5-γωνο κατασκευάστηκαν από τον Ευκλείδη (Στοιχεία, 300 π.Χ., βιβλίο 4, προτάσεις 11,15), το τελευταίο κατασκευάστηκε και από τον Πτολεμαίο (Almagest, 150 μ.Χ.). Το κανονικό 17-γωνο κατασκευάστηκε από τον Gauss (δόθηκε το μήκος $cos\frac{2\pi}{17}$ σε κατασκευάσιμη έκφραση) και ακολούθησε μια γεωμετρική απόδειξη από τον Johannes Erchinger. Ο R. J. Richelot το 1832 κατασκευάζει το κανονικό 257-γωνο (βιβλιο-γραφία [17]) και ο J. Hermes το 1894 δουλεύοντας για δέκα χρόνια κατασκευάζει, σε μία εργασία 200 σελίδων, το κανονικό 65537-γωνο (δείτε [11]). Ο Coxeter (δείτε [4]) αναφέρει ότι μετά τη λήξη του Δευτέρου Παγκοσμίου Πολέμου τα γραπτά του μεταφέρθηκαν στο Μαθηματικό Ινστιτούτο του $Göttingen$, όπου και βρίσκονται μέχρι σήμερα.

Στο κεφάλαιο αυτό θα δούμε τις κατασκευές του ισοπλεύρου τριγώνου και του κανονικού πενταγώνου, όπως αυτές έγιναν από τον Ευκλείδη. Στη συνέχεια θα δούμε την κατασκευή του κανονικού 17-γώνου από τον Gauss με χρήση των περιόδων και μια γεωμετρική κατασκευή του Richmond (1893). Τέλος θα μελετήσουμε τους κύκλους Carlyle, πως μπορούμε με τη βοήθεια τους να κατασκευάσουμε γεωμετρικά τις ρίζες δευτεροβάθμιων πολυωνύμων και πως από αυτό μπορούμε να κατασκευάσουμε όλα τα κανονικά n-γωνα για n=3,5,17,257 και 65537 με ομοιόμορφο τρόπο.

Ξεκινώντας, θα δούμε πρώτα την ικανή και αναγκαία συνθήκη για να είναι ένα κανονικό n-γωνο κατασκευάσιμο. Κάποια θεωρήματα από τη θεωρία ομάδων και τη

θεωρία Galois που είναι απαραίτητα για τις αποδείξεις βρίσκονται στο παράρτημα.

1.2 Κατασκευασιμότητα κανονικού n-γώνου

Κατασκευές με κανόνα και διαβήτη:

Έστω $P \subseteq \mathbb{R}^2$. Θεωρούμε τις ακόλουθες δύο κατασκευές:

1. Κατασκευή ευθείας γραμμής, ορισμένης από δύο σημεία του P.

2. Κατασκευή κύκλου με κέντρο σημείο του P και ακτίνα ίση με την απόσταση δύο σημείων του P.

Λέμε ότι ένα σημείο του επιπέδου είναι άμεσα κατασκευάσιμο (με κανόνα και διαβήτη) από το P, αν είναι σημείο τομής δύο ευθειών ή μιας ευθείας και ενός κύκλου ή δύο κύκλων που προκύπτουν από τις κατασκευές 1,2.

Θα λέμε ότι ένα σημείο $r \in \mathbb{R}^2$ του επιπέδου είναι κατασκευάσιμο (με κανόνα και διαβήτη) από το P, αν υπάρχει πεπερασμένο πλήθος σημείων $r_1, ..., r_n$ έτσι ώστε:

-Το r_1 να είναι άμεσα κατασκευάσιμο από το P.

-Το r_i, με $i = 2, ..., n$ να είναι άμεσα κατασκευάσιμο από το $P \cup \{r_1, ..., r_{i-1}\}$.

-$r_n = r$.

Σε κάθε βήμα της κατασκευής θεωρούμε το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες των σημείων που έχουν κατασκευαστεί.

Έστω K_0 το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες του P.

Αν το $r_i = (x_i, y_i)$, ορίζουμε επαγωγικά το σώμα K_i, $K_i = K_{i-1}(x_i, y_i)$, $i = 1, ..., n$.

$$K_0 \subseteq K_1 \subseteq ... \subseteq K_n \subseteq \mathbb{R}$$

Λήμμα 1.2.1:

Τα x_i,$y_i \in K_i$ (με τον παραπάνω συμβολισμό) είναι ρίζες ενός τετραγωνικού πολυωνύμου με συντελεστές από το σώμα K_{i-1}.

Απόδειξη:

Για την κατασκευή του $r_i = (x_i, y_i)$ έχουμε τρεις περιπτώσεις, να είναι τομή δύο ευθειών ή κύκλων ή τομή ευθείας με κύκλο. Θα εξετάσουμε μόνο την τρίτη περίπτωση. Οι άλλες δύο περιπτώσεις διαπραγματεύονται ανάλογα.

Έστω ότι η ευθεία διέρχεται από τα σημεία $A = (p, q)$ και $B = (r, s)$ με $p, q, r, s \in K_{i-1}$ και ο κύκλος έχει ακτίνα ω και κέντρο $C = (t, u)$, με $t, u, \omega^2 \in K_{i-1}$

(Το ω εν γένει δεν ανήκει στο K_{i-1}, όμως αφού το ω είναι η απόσταση δύο σημείων του K_{i-1}, έστω των $G(a,b)$ και $D(c,d)$, θα έχουμε ότι $\omega^2 = (a-c)^2+(b-d)^2 \in K_{i-1}$)

Η εξίσωση της ευθείας AB είναι $\frac{x-p}{r-p} = \frac{y-q}{s-q}$ και η εξίσωση του κύκλου με κέντρο C και ακτίνα ω, είναι $(x-t)^2+(y-u)^2 = \omega^2$. Τελικά $(x-t)^2+(\frac{s-q}{r-p}(x-p)+q)^2 = \omega^2$, άρα το x είναι ρίζα τετραγωνικού πολυωνύμου με συντελεστές από το K_{i-1}.

Ομοίως αποδεικνύεται για το y.

□

Θεώρημα 1.2.2:

Αν το $r = (x,y)$ είναι κατασκευάσιμο από ένα $P \subseteq \mathbb{R}^2$ και K_0 το υπόσωμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες του P, τότε οι βαθμοί $[K_0(x) : K_0]$ και $[K_0(y) : K_0]$ είναι δυνάμεις του 2.

Απόδειξη:

Από το λήμμα 1.2.1 έχουμε $[K_{i-1}(x_i) : K_{i-1}]$=1 ή 2 και όμοια $[K_{i-1}(y_i) : K_{i-1}]$=1 ή 2, (αφού όπως είδαμε τα x_i και y_i είναι ρίζες ενός δευτεροβάθμιου πολυωνύμου με συντελεστές από το K_{i-1}, άρα το ανάγωγο πολυώνυμό τους στο K_{i-1} θα είναι βαθμού 1 ή 2), τότε

$$[K_i : K_{i-1}] = [K_{i-1}(x_i,y_i) : K_{i-1}] = [K_{i-1}(x_i,y_i) : K_{i-1}(x_i)]\cdot[K_{i-1}(x_i) : K_{i-1}] = 1, 2 \text{ ή } 4$$

(αφού $[K_{i-1}(x_i,y_i) : K_{i-1}(x_i)]$=2, αν $y_i \notin K_{i-1}(x_i)$, ενώ είναι 1 αν $y_i \in K_{i-1}(x_i)$).

Άρα ο βαθμός $[K_i : K_{i-1}]$ είναι δύναμη του 2. Επαγωγικά αποδεικνύεται ότι $[K_n : K_0]$ είναι δύναμη του 2 και επειδή $[K_n : K_0] = [K_n : K_0(x)] \cdot [K_0(x) : K_0]$ συνεπάγεται ότι $[K_0(x) : K_0]$ είναι δύναμη του 2. Αντίστοιχα, το $[K_0(y) : K_0]$ είναι δύναμη του 2.

□

Λήμμα 1.2.3:

Έστω $P \subseteq \mathbb{R}^2$ με (0,0),(1,0)$\in P$. Αν οι συντεταγμένες του (x,y) ανήκουν στο σώμα που παράγουν οι συντεταγμένες των σημείων του P, τότε το (x,y) κατασκευάζεται από το P.

(Το αντίστροφο εν γένει δεν ισχύει, θα δούμε αργότερα ότι αν το (x, y) κατασκευάζεται από το P μπορεί τα x, y να ανήκουν σε μια επέκταση του σώματος βαθμού δύναμη του 2).

Σε όσα ακολουθούν θεωρείται γνωστό ότι είναι δυνατόν, με κανόνα και διαβήτη να γίνουν τα παρακάτω:

$i)$ Μπορούμε να κατασκευάσουμε ευθεία ε_1, κάθετη σε δοσμένη ευθεία ε_2, που να διέρχεται από δοθέν σημείο $A \in \varepsilon_2$.

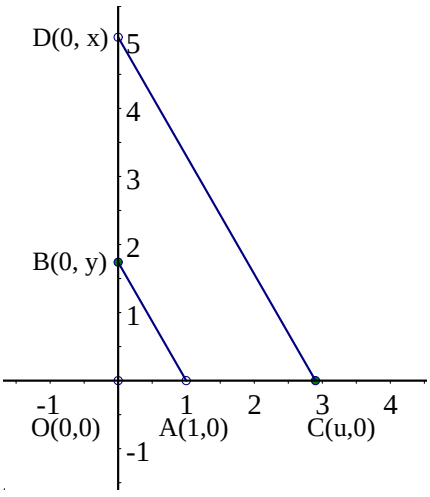
$ii)$ Μπορούμε να κατασκευάσουμε ευθεία ε_1, κάθετη σε δοσμένη ευθεία ε_2, που να διέρχεται από δοθέν σημείο $A \notin \varepsilon_2$.

$iii)$Μπορούμε να κατασκευάσουμε ευθεία ε_1, παράλληλη σε δοσμένη ευθεία ε_2, που να διέρχεται από δοθέν σημείο $A \notin \varepsilon_2$.

Απόδειξη (Λήμματος 1.2.3):

Καταρχήν λόγω των $i)$ και $ii)$ και αφού (0,0),(1,0)$\in P$, από το (x, y) εύκολα κατασκευάζουμε τα $(0, x)$, $(0, y)$ και αντίστροφα.

Αρκεί λοιπόν να δείξουμε ότι δοσμένων των $(0, x)$, $(0, y)$ μπορούμε να κατασκευάσουμε τα $(0, x + y), (0, x - y), (0, xy)$ και $(0, \frac{x}{y}), y \neq 0$. (δηλαδή από τα σημεία $(x, y) \in P$ μπορούμε να κατασκευάσουμε όλα τα σημεία που οι συντεταγμένες τους ανήκουν στο σώμα που παράγεται από τα x και y). Τα πρώτα δύο προκύπτουν αμέσως από την κατασκευή κύκλου ακτίνας y και κέντρου x. Για την κατασκευή του $\frac{x}{y}$, ενώνουμε τα $B(0, y)$ και $A(1, 0)$ και από το $iii)$ φέρνουμε ευθεία παράλληλη προς το ευθύγραμμο τμήμα ΑΒ που να διέρχεται από το $(0, x)$. (Υποθέτουμε ότι $x \neq y$, αν $x = y$ τότε έχουμε το $(0, 1)$, τετριμμένο).



Τα τρίγωνα ΟΑΒ και OCD είναι όμοια, άρα $\frac{u}{x} = \frac{1}{y} \Rightarrow u = \frac{x}{y}$.

Για το xy κάνουμε την παραπάνω διαδικασία θέτοντας όπου x το 1 και κατασκευάζουμε το $\frac{1}{y}$ και μετά την επαναλαμβάνουμε θέτοντας όπου y το $\frac{1}{y}$.

□

Λήμμα 1.2.4:

Έστω $K(a)/K$ επέκταση σωμάτων, με $[K(a) : K] = 2$, όπου $K(a) \subseteq \mathbb{R}$. Τότε κάθε $(z, t) \in \mathbb{R}^2$ με $z, t \in K(a)$ κατασκευάζεται από (πεπερασμένο) σύνολο σημείων, με συντεταγμένες από το K.

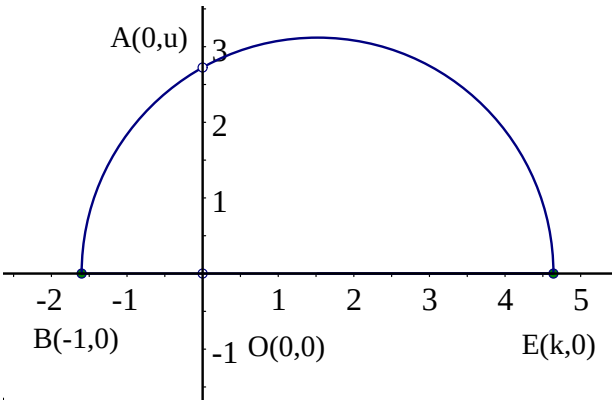
Απόδειξη:

Έχουμε $[K(a) : K] = 2$, άρα το ανάγωγο πολυώνυμο $f(x)$ του a πάνω από το K, (θα το συμβολίζουμε με $Irr(a, K)$), θα είναι δευτέρου βαθμού, δηλαδή $f(x) = x^2 + px + q,\ q, p \in K$.

Άρα $a = \frac{-p \pm \sqrt{p^2-4q}}{2}$, όπου $p^2 - 4q \geq 0$, αφού $K(a) \subseteq \mathbb{R}$.

Αφού για κάθε $z, t \in K(a)$ έχουμε $z, t = x + ay$ (η {1,a} είναι βάση της $K(a)/K$) με $x, y \in K$ και $p, q, p^2 - 4q \in K$, αρκεί να δείξουμε την κατασκευασιμότητα του a ή ισοδύναμα του $(0, \sqrt{k})$ για κάθε $k \in K$ με $k > 0$.

Κατασκευάζουμε τους άξονες (με τον κανόνα φέρνουμε τον άξονα των x, επειδή το 1 είναι στοιχείο του K μπορούμε να αριθμήσουμε, στη συνέχεια, από το (i), μπορούμε να φέρουμε κάθετη στο σημείο 0, σχηματίζουμε δηλαδή και τον άξονα των y) και τα σημεία (-1,0),(k,0) (τα σημεία κατασκευάζονται αφού οι συντεταγμένες τους είναι στοιχεία του K). Γράφουμε το ημικύκλιο με διάμετρο ΒΕ, με Β(-1,0) και Ε(k,0), το οποίο τέμνει τον άξονα στο $(0, u)$.



Τα τρίγωνα ΑΒΟ και ΑΟΕ είναι όμοια, άρα $\frac{OE}{AO} = \frac{AO}{BO} \Rightarrow \frac{k}{u} = \frac{u}{1} \Rightarrow u = \sqrt{k}$ και το $\sqrt{k}$ κατασκευάστηκε. Αυτό ολοκληρώνει την απόδειξη.

□

Λήμμα 1.2.5:

Έστω K υπόσωμα του $\mathbb{R}$, που παράγεται από τις συντεταγμένες των σημείων ενός συνόλου P, $P \subseteq \mathbb{R}^2$ και έστω τα $a, b \in L$, όπου L υπόσωμα του $\mathbb{R}$, επέκταση του K τ.ω. να υπάρχει πεπερασμένη ακολουθία σωμάτων $K = K_0 \subseteq K_1 \subseteq ... \subseteq K_r = L$ με $[K_{i+1} : K_i] = 2$ για κάθε $i = 0, ..., r-1$, τότε το (a, b) κατασκευάζεται από το P.

Απόδειξη:

Αν $r = 0$, τότε σύμφωνα με το λήμμα 1.2.3, έχουμε τελειώσει.

Αν $r \neq 0$, τότε το (a, b), σύμφωνα με το λήμμα 1.2.4 κατασκευάζεται από το K_{r-1} και συνεχίζοντας επαγωγικά, από το P.

□

Παρατήρηση:

Ισχύει και το αντίστροφο του λήμματος 1.2.5 λόγω του θεωρήματος 1.2.2.

Πρόταση 1.2.6:

Αν K υπόσωμα του $\mathbb{R}$, παραγόμενο από τις συντεταγμένες των σημείων κάποιου $P \subseteq \mathbb{R}^2$ και αν $a, b \in L$, όπου L υπόσωμα του $\mathbb{R}$, κανονική επέκταση του K, βαθμού $[L : K] = 2^r$, τότε το (a, b) κατασκευάζεται από το P.

Απόδειξη:

Η L/K είναι διαχωρίσιμη, αφού η χαρακτηριστική του σώματος K είναι μηδέν. Επίσης είναι και κανονική, άρα είναι Galois, τότε αν θέσουμε $G = Gal(L/K)$ θα έχουμε $\sharp G = [L : K] = 2^r$.

Από το λήμμα 4.1.5 αφού η G είναι μία 2-ομάδα έχει πεπερασμένη ακολουθία κανονικών υποομάδων:

$$< id >= G_0 \leq G_1 \leq ... \leq G_r = G \quad (1)$$

τ.ω. $|G_i| = 2^i$, για κάθε $i = 0, ..., r$.

Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois θα έχουμε την αντίστοιχη ακολουθία ενδιάμεσων σωμάτων:

$$K = K_0 \subseteq K_1 \subseteq ... \subseteq K_r = L$$

και οι υποομάδες G_i της (1) γράφονται σαν ομάδες Galois των σωμάτων αυτών:

$$< id >= Gal(L/L) \leq Gal(L/K_{r-1}) \leq ... \leq Gal(L/K_1) \leq Gal(L/K) = G$$

όπου $|Gal(L/K_{r-i})| = 2^i$.

Επίσης

$$[K_1 : K] = \frac{|G|}{|Gal(L/K_1)|} = \frac{2^r}{2^{r-1}} = 2$$

$$[K_2 : K] = \frac{|G|}{|Gal(L/K_2)|} = \frac{2^r}{2^{r-2}} = 2^2$$

$$\vdots$$

$$[K_r : K] = \frac{|G|}{|Gal(L/K_r)|} = \frac{2^r}{2^{r-r}} = 2^r$$

Άρα από τον τύπο γινομένου διαστάσεων έχουμε:

$[K_{j+1} : K_j] = 2$, για κάθε $j = 0, ..., r-1$.

Επομένως, σύμφωνα με το λήμμα 1.2.5, το (a, b) κατασκευάζεται από το P.

□

Ορισμός: Ένας $n \in \mathbb{N}$ θα λέμε ότι είναι κατασκευάσιμος αν και μόνο αν το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη.

Λήμμα 1.2.7:

1)Αν n κατασκευάσιμος και $m|n$ τότε ο m είναι κατασκευάσιμος.

2)Αν (m,n)=1 και m,n κατασκευάσιμοι τότε και ο mn είναι κατασκευάσιμος.

Απόδειξη:

1) Αν ο n είναι κατασκευάσιμος, κατασκευάζουμε το κανονικό m-γωνο ενώνοντας κάθε $\frac{n}{m}$-οστή κορυφή του n-γώνου.

2)Αν $(m,n) = 1 \Rightarrow am + bn = 1 \Rightarrow a\frac{1}{n} + b\frac{1}{m} = \frac{1}{mn} \Rightarrow a\frac{2\pi}{n} + b\frac{2\pi}{m} = \frac{2\pi}{mn}$, για κάποια $a, b \in \mathbb{Z}$.

Δηλαδή $K = La + bM$, όπου K, L και M οι χορδές που αντιστοιχούν στις πλευρές του κανονικού mn-γώνου, n-γώνου και m-γώνου αντίστοιχα. Όμως τα μήκη των χορδών L και M είναι γνωστά (m,n κατασκευάσιμοι), άρα υπολογίζουμε την χορδή K.

□

Πόρισμα:

Αν $n = p_1^{a_1}...p_r^{a_r}$, όπου p_i διακεκριμένοι πρώτοι, τότε ο n είναι κατασκευάσιμος αν και μόνο αν ο $p_i^{a_i}$ είναι κατασκευάσιμος για κάθε $i = 1, ..., r$.

Λήμμα 1.2.8:

Το 2^a είναι κατασκευάσιμος για κάθε $a \in \mathbb{N}_{>1}$.

Απόδειξη:

Η απόδειξη είναι άμεση συνέπεια του γεγονότος ότι το τετράγωνο κατασκευάζεται μέσω των κατασκευών (i) και (ii), ενώ για κάθε φυσικό $a > 2$ με διχοτόμηση γωνιών.

□

Λήμμα 1.2.9:

Έστω πρώτος p τ.ω. p^n κατασκευάσιμος και ζ πρωταρχική p^n-ρίζα της μονάδας στο $\mathbb{C}$, τότε $deg(Irr(\zeta, \mathbb{Q})) = 2^m$, για κάποιο $m \in \mathbb{N} \cup \{0\}$.

Απόδειξη:

$\zeta = e^{\frac{2\pi i}{p^n}} = (cos\frac{2\pi}{p^n}, sin\frac{2\pi}{p^n}) := (a, b)$

Τα a, b είναι κατασκευάσιμα αφού ο p^n κατασκευάσιμος. Από το θεώρημα 1.2.2 έχουμε $[\mathbb{Q}(a,b) : \mathbb{Q}] = 2^r$. Άρα $[\mathbb{Q}(a,b,i) : \mathbb{Q}] = 2^{r+1}$, $(a, b \in \mathbb{R}$, άρα $Irr(i, \mathbb{Q}(a,b)) = x^2 + 1)$.

Επίσης $\zeta \in \mathbb{Q}(\zeta)$, άρα $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(a,b,i) \Rightarrow [\mathbb{Q}(\zeta) : \mathbb{Q}] \cdot [\mathbb{Q}(a,b,i) : \mathbb{Q}(\zeta)] = [\mathbb{Q}(a,b,i) : \mathbb{Q}] = 2^{r+1}$, άρα $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^m$, για κάποιο $m \in \mathbb{N} \cup \{0\}$, δηλαδή $deg(Irr(\zeta, \mathbb{Q})) = 2^m$, για κάποιο $m \in \mathbb{N} \cup \{0\}$.

□

Λήμμα 1.2.10:

Έστω p πρώτος και ζ πρωταρχική p ρίζα της μονάδας στο $\mathbb{C}$, τότε $Irr(\zeta, \mathbb{Q}) = 1 + t + ... + t^{p-1}$.

Απόδειξη:

Έχουμε ζ$\neq 1$, αφού ζ πρωταρχική ρίζα, άρα ζ ρίζα του πολυωνύμου $f(t) = 1 + t + ... + t^{p-1}$. Θα αποδείξουμε ότι το πολυώνυμο είναι ανάγωγο με τη βοήθεια της παρατήρησης που λέει ότι:

$f(x)$ ανάγωγο στο $\mathbb{Q} \Leftrightarrow f(x + c)$ ανάγωγο στο $\mathbb{Q}$, για κάποιο $c \in \mathbb{Z}$.

Για να δείξουμε λοιπόν ότι το $f(t)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$, αρκεί να δείξουμε ότι το $f(t+1)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$. Είναι

$f(t+1) = \frac{(t+1)^p - 1}{t+1-1} = \frac{t^p + \binom{p}{p-1}t^{p-1} + ... + \binom{p}{1}t + 1 - 1}{t}$

$f(t+1) = t^{p-1} + \binom{p}{p-1}t^{p-2} + ... + \binom{p}{2}t + \binom{p}{1}$

$f(t+1) = t^{p-1} + \binom{p}{p-1}t^{p-2} + ... + \binom{p}{2}t + p$

Τότε έχουμε ότι $p|\binom{p}{p-1}, ..., \binom{p}{2}, p$, $p \not| 1$ και $p^2 \not| p$, άρα από το κριτήριο Eisenstein το $f(t+1)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$.

□

Λήμμα 1.2.11:

Έστω p πρώτος και ζ πρωταρχική p^2-οστή ρίζα του 1 στο $\mathbb{C}$, τότε $Irr(\zeta, \mathbb{Q}) = 1 + t^p + t^{2p} + ... + t^{(p-1)p}$.

Απόδειξη:

Έστω $g(x) = 1 + t^p + t^{2p} + ... + t^{(p-1)p} = \frac{t^{p^2}-1}{t^p-1}$. Είναι $g(\zeta) = 0$, αφού $\zeta^{p^2} - 1 = 0$ και $\zeta^p \neq 1$. Όπως πριν, για να δείξουμε ότι $g(t)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$, αρκεί να δείξουμε ότι το $g(t+1)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$.

Έχουμε $g(1+t) = 1 + (1+t)^p + ... + (1+t)^{(p-1)p} = \frac{(1+t)^{p^2}-1}{(1+t)^p-1} \equiv \frac{t^{p^2}}{t^p} \equiv t^{p(p-1)} \pmod{p}$. Άρα $g(1+t) = t^{p(p-1)} + pk(t),\ k(t) \in \mathbb{Z}[x]$. Από το κριτήριο του Eisenstein για p το $g(t+1)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$, άρα και το $g(t)$.

□

Λήμμα 1.2.12:

Έστω K σώμα με χαρακτηριστική 0 $(chK = 0)$ και L το σώμα ανάλυσης του $t^p - 1$ στο K, όπου p πρώτος, τότε η ομάδα $Gal(L/K)$ είναι αβελιανή.

Απόδειξη:

Οι ρίζες του t^p-1, δηλαδή οι p-ρίζες του 1, αποτελούν πολλαπλασιαστική ομάδα, τάξης p, άρα κυκλική. Αν ε ένας γεννήτοράς της, τότε $L = K(\varepsilon)$.

Κάθε K-αυτομορφισμός του L καθορίζεται από τη δράση του στο ε και είναι μια μετάθεση των ριζών του $t^p - 1$. Άρα θα είναι της μορφής $\sigma_j(\varepsilon) = \varepsilon^j$. Όμως τότε η ομάδα θα είναι αβελιανή αφού $\sigma_i \circ \sigma_j(\varepsilon) = \varepsilon^{ij} = \sigma_j \circ \sigma_i(\varepsilon)$.

□

Λήμμα 1.2.13:

Το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη αν και μόνο αν $n = 2^r p_1...p_s$, όπου $r, s \in \mathbb{N} \cup \{0\}$ και $p_1, ..., p_s$ είναι περιττοί πρώτοι της μορφής $2^{2^n} + 1$, για θετικούς ακεραίους n (πρώτοι του Fermat).

Απόδειξη:

$(\Rightarrow)$

Έστω n κατασκευάσιμο και $n = 2^r p_1^{a_1}...p_s^{a_s}$ η μονοσήμαντη ανάλυση του n σε πρώτους (p_i διακριτοί περιττοί πρώτοι).

Από το λήμμα 1.2.7 κάθε $p_i^{a_i}$ είναι κατασκευάσιμος. Αν $a_i \geq 2$ τότε το p_i^2 είναι κατασκευάσιμο (πάλι από το λήμμα 1.2.7, αφού $p_i^2 | p_i^{a_i}$). Άρα από το λήμμα 1.2.9 έχουμε ότι ο βαθμός $deg(Irr(\zeta, \mathbb{Q})) =$ είναι δύναμη του 2, όπου ζ πρωταρχική p_i^2-ρίζα της μονάδας στο $\mathbb{C}$. Από το λήμμα 1.2.11, $deg(Irr(\zeta, \mathbb{Q})) = p_i(p_i - 1)$. Τότε όμως θα πρέπει το $p_i(p_i - 1)$ να είναι δύναμη του 2, δηλαδή ο περιττός πρώτος p_i πρέπει να διαιρεί το 2, άτοπο! Άρα $a_i = 1$ για κάθε i.

Μένει να δείξουμε ότι οι πρώτοι p_i, για $i = 1, ..., s$ είναι πρώτοι του Fermat. Από το λήμμα 1.2.10, αν ζ πρωταρχική p_i-ρίζα της μονάδας στο $\mathbb{C}$ τότε $deg(Irr(\zeta, \mathbb{Q})) = p_i - 1$ και από το λήμμα 1.2.9 θα πρέπει να είναι ίσο με 2^{s_i}, για κάποιο $s_i \in \mathbb{N}$.

Έστω ότι ο s_i έχει περιττό διαιρέτη $a > 1$, τότε $s_i = ab \Rightarrow p_i = 2^{ab} + 1 = (2^b)^a + 1 = (2^b + 1)(2^{b(a-1)} - ... + 1)$, με $2^b + 1$ και $2^{b(a-1)} - ... + 1$ ακέραιοι, μεγαλύτεροι του 1, άτοπο!

Άρα το s_i δεν έχει περιττό διαιρέτη, άρα είναι δύναμη του 2, δηλαδή ο n είναι της μορφής $2^{2^n} + 1$, για κάποιο $n \in \mathbb{N}$ και η αναγκαία συνθήκη για να είναι ένα κανονικό n-γωνο κατασκευάσιμο αποδείχθηκε.

$(\Leftarrow)$

Αρκεί να δείξουμε ότι οι 2^r,p_i είναι κατασκευάσιμοι. Το 2^r είναι κατασκευάσιμο από το λήμμα 1.2.8. Θα δείξουμε την κατασκευασιμότητα των p_i. Έστω ζ p_i-οστή πρωταρχική ρίζα της μονάδας στο $\mathbb{C}$. Τότε από το λήμμα 1.2.10 $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p_i - 1 = 2^{2^n} + 1 - 1 = 2^{2^n} := 2^a$.

Το $\mathbb{Q}(\zeta)$ είναι το σώμα ανάλυσης του $f(t) = 1 + t + ... + t^{p_i - 1}$ στο $\mathbb{Q}$, άρα $\mathbb{Q}(\zeta)/\mathbb{Q}$ κανονική και διαχωρίσιμη (χαρακτηριστική 0), άρα Galois. Από το λήμμα 1.2.12 η $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ είναι αβελιανή.

Έστω $K = \mathbb{R} \cap \mathbb{Q}(\zeta), \ \ (\mathbb{Q} \subseteq K = \mathbb{R} \cap \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta))$. Είναι $[Q(\zeta) : K] = 2$ $(Irr(\zeta, K) = (x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + \zeta\zeta^{-1} = x^2 - 2cos(\frac{2\pi}{p_i})x + 1 \in K[x])$.

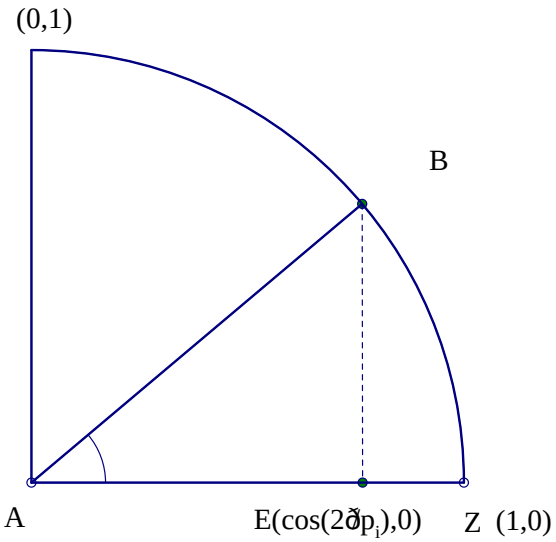
Έχουμε ότι $Gal(\mathbb{Q}(\zeta)/K) \trianglelefteq Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, (αφού κάθε υποομάδα αβελιανής ομάδας είναι κανονική). Άρα από το Θεμελιώδες Θεώρημα της Θεωρίας Galois (δείτε το παράρτημα με τη θεωρία Galois) έχουμε ότι η επέκταση $K/\mathbb{Q}$ είναι Galois, άρα κανονική και επίσης:

$2^a = [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : K] \cdot [K : \mathbb{Q}] = 2[K : \mathbb{Q}] \Rightarrow [K : \mathbb{Q}] = 2^{a-1}$.

Αφού λοιπόν η $K/\mathbb{Q}$ είναι κανονική επέκταση βαθμού δύναμη του 2, από την πρόταση 1.2.6 έχουμε ότι κάθε στοιχείο του K είναι κατασκευάσιμο.

Όμως τα $\zeta = cos\frac{2\pi}{p_i} + isin\frac{2\pi}{p_i}$ και $\zeta^{-1} = cos\frac{2\pi}{p_i} - isin\frac{2\pi}{p_i}$ ανήκουν στο $\mathbb{Q}(\zeta)$, άρα και το $\zeta + \zeta^{-1} = 2cos\frac{2\pi}{p_i}$ ανήκει στο $\mathbb{Q}(\zeta)$, το οποίο όμως είναι πραγματικός αριθμός, άρα ανήκει στο K.

Δηλαδή το $2cos\frac{2\pi}{p_i}$ κατασκευάζεται, άρα κατασκευάζεται το $cos\frac{2\pi}{p_i}$ και συνεπώς μπορούμε να κατασκευάσουμε και το σημείο $(cos\frac{2\pi}{p_i}, 0)$ του $\mathbb{R}^2$. Σχηματίζουμε λοιπόν τον μοναδιαίο κύκλο και το σημείο Γ=$(cos\frac{2\pi}{p_i}, 0)$.



Τότε $cos\theta = \frac{AE}{AB} = \frac{cos(\frac{2\pi}{p_i})}{1} = cos\frac{2\pi}{p_i}$, άρα η ΒΖ είναι η πλευρά του κανονικού p_i-γώνου.

□

1.3 Η κατασκευή του ισοπλεύρου τριγώνου και του κανονικού πενταγώνου κατά τον Ευκλείδη

Είδαμε ότι το πρόβλημα κατασκευής κανονικού n-γώνου με κανόνα και διαβήτη ανάγεται στο πρόβλημα κατασκευής κανονικού p-γώνου, όπου p πρώτος του Fermat. Οι πρώτες κατασκευές τέτοιων p-γώνων έγιναν περίπου 2000 χρόνια πριν από τον Gauss, από τους αρχαίους Έλληνες. Αυτές ήταν οι κατασκευές του ισοπλεύρου τριγώνου και του κανονικού πενταγώνου (Στοιχεία του Ευκλείδη, βιβλίο 4, 300 π.Χ.).

Αρχικά θα αποδείξουμε τέσσερεις προτάσεις που θα μας χρησιμεύσουν στη συνέχεια, μετά θα κατασκευάσουμε το κανονικό πεντάγωνο και τέλος το κανονικό εξάγωνο από το οποίο προκύπτει και το ισόπλευρο τρίγωνο.

Πρόταση 1.3.1:

Να διαιρεθεί δοσμένο ευθύγραμμο τμήμα ώστε το ορθογώνιο που ορίζει το τμήμα και το ένα μέρος του, να είναι ισοδύναμο με το τετράγωνο που έχει πλευρά το άλλο μέρος.

Απόδειξη:

Η απόδειξη που θα δώσουμε είναι σύγχρονη (αλγεβρική), η γεωμετρική απόδειξη του Ευκλείδη βρίσκεται στα στοιχεία, βιβλίο 2, πρόταση 11.

Έστω ΑΒ το δοσμένο τμήμα, το ζητούμενο είναι να βρούμε σημείο Θ τέτοιο ώστε ΑΒ·ΒΘ=ΑΘ^2, δηλαδή $AB \cdot B\Theta$=(ΑΒ-ΒΘ)^2. Έστω x και d (γνωστό) τα μήκη των ΒΘ και ΑΒ αντίστοιχα.

Τότε

$$dx = (d-x)^2$$
$$x^2 - 3dx + d^2 = 0$$
$$x = \frac{3d + d\sqrt{5}}{2} = d \cdot \frac{3+\sqrt{5}}{2},$$

άρα x κατασκευάσιμο. Φέρνουμε κύκλο κέντρου Β και ακτίνας x, το σημείο τομής του κύκλου με το ευθύγραμμο τμήμα ΑΒ είναι το ζητούμενο σημείο Θ.

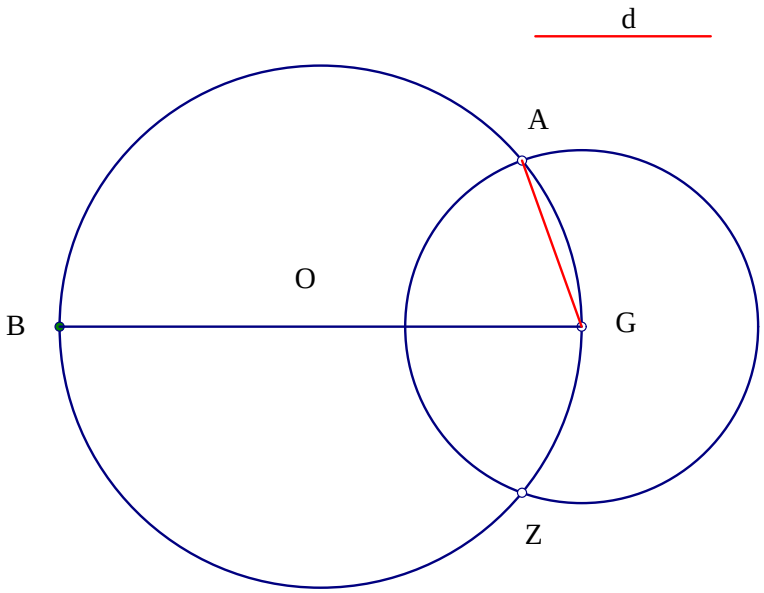
□

Πρόταση 1.3.2 (Στοιχεία, IV.1):

Αν δοθούν κύκλος και ευθύγραμμο τμήμα μικρότερο ή ίσο από τη διάμετρο του κύκλου, να κατασκευαστεί χορδή του κύκλου ίση προς το δοθέν ευθύγραμμο τμήμα.

Απόδειξη:

Έστω κύκλος κέντρου Ο και ακτίνας ρ και ευθύγραμμο τμήμα d μικρότερο ή ίσο με τη διάμετρο του κύκλου.



Φέρνουμε μια διάμετρο του κύκλου, έστω BG. Αν το d είναι ίσο με τη διάμετρο τελειώσαμε. Αν το d είναι μικρότερο από τη διάμετρο, φέρνουμε κύκλο κέντρου G και ακτίνας d, ο οποίος τέμνει τον (O,ρ) στα A και Z. Η $GA = d$ είναι η ζητούμενη χορδή.

□

Η παραπάνω κετασκευή δεν "ταιριάζει" με τις άλλες κατασκευές του τέτερτου βιβλίου των Στοιχείων και μάλλον θα πρέπει να είναι του ίδιου του Ευκλείδη, ο οποίος τη χρησιμοποιεί σαν λήμμα σε μια σειρά προτάσεων (π.χ. Στοιχεία IV.16,XII.16).

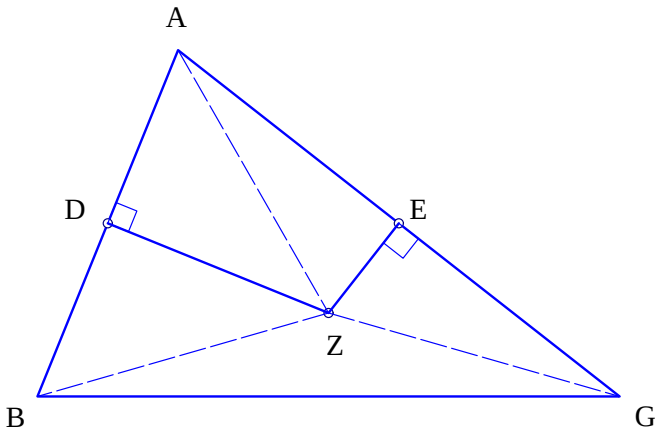
Πρόταση 1.3.3 (Στοιχεία, IV.5):

Περί δοθέν τρίγωνο να περιγραφεί κύκλος.

Απόδειξη:

Δίνεται τρίγωνο ABG και θέλουμε να φέρουμε κύκλο περί αυτού, δηλαδή να κατασκευάσουμε κύκλο που να διέρχεται από τις κορυφές του τριγώνου A, B και G.

Παίρνουμε τα μέσα D και E των πλευρών AB και AG αντίστοιχα και φέρνουμε κάθετες στις AB και AG που να διέρχονται από τα D και E. Οι κάθετες αυτές τέμνονται ή εντος του τριγώνου ή σε σημείο της BG ή εκτός του τριγώνου. Έστω ότι τέμνονται σε σημείο Z εσωτερικό του τριγώνου.



Φέρνουμε τα ευθύγραμμα τμήματα ZA,ZB και ZG. Τα ορθογώνια τρίγωνα DAZ και DBZ έχουν $AD = DB = \frac{AB}{2}$ και DZ κοινή, άρα είναι ίσα, επομένως ZA=ZB. Ομοίως αποδεικνύεται ότι ZG=ZA. Άρα ZA=ZB=ZG=r.

Τότε ο κύκλος (Z,r) διέρχεται από τις κορυφές A, B, G και είναι ο περιγεγραμμένος περί του τριγώνου ABG. Όμοια εργαζόμαστε και στις άλλες περιπτώσεις.

□

Πρόταση 1.3.4 (Στοιχεία, IV.10):

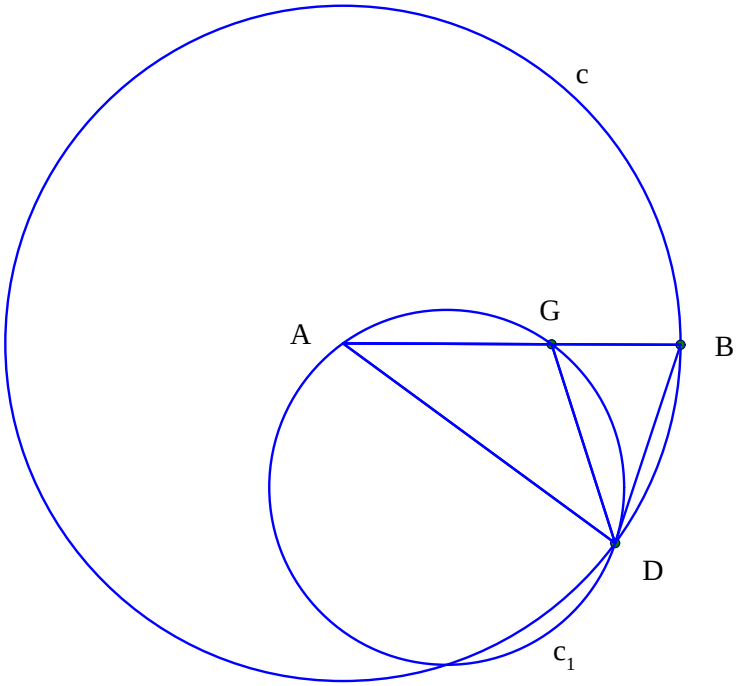
Να κατασκευαστεί ισοσκελές τρίγωνο, του οποίου η γωνία της βάσης να είναι διπλάσια από τη γωνία της κορυφής του.

Απόδειξη:

Παίρνουμε ευθύγραμμο τμήμα ΑΒ και σημείο του G, τέτοιο ώστε $AB \cdot BG = AG^2$ (από πρόταση 1.3.1). Με κέντρο το Α και ακτίνα ΑΒ γράφουμε κύκλο c και κατασκευάζουμε χορδή BD του c ίση με το AG, η οποία δεν είναι μεγαλύτερη από τη διάμετρο του κύκλου (πρόταση 1.3.2). Φέρνουμε τα AD, DG και τον περιγεγραμμένο κύκλο c_1 του τριγώνου AGD (πρόταση 1.3.3).

Έχουμε ότι $AB \cdot BG = AG^2$ και $AG = BD$, άρα $AB \cdot BG = BD^2$.

Από το Β, που βρίσκεται εκτός του κύκλου c_1, διέρχονται δυο ευθείες, εκ των οποίων η μία τέμνει τον c_1 στα σημεία Α και G και η άλλη έχει κοινό σημείο με τον c_1 το D και επειδή $AB \cdot BG = BD^2$, η BD θα εφάπτεται στον c_1 στο σημείο D.



Άρα η γωνία BDG είναι ίση με τη GAD (γωνία χορδής και εφαπτομένης). Επομένως $B\hat{D}G + G\hat{D}A = G\hat{A}D + G\hat{D}A$ ή $B\hat{D}A = G\hat{A}D + G\hat{D}A$. Αλλά $G\hat{A}D + G\hat{D}A = B\hat{G}D$ (η BGD γωνία είναι εξωτερική του τριγώνου AGD). Συνεπώς $B\hat{D}A = B\hat{G}D \quad (1)$.

Ακόμα $B\hat{D}A = D\hat{B}A \quad (2)$, αφού το ABD είναι ισοσκελές, ($AB = AD$=ακτίνα του κύκλου c).

Από τις (1) και (2) προκύπτει ότι $B\hat{G}D = D\hat{B}A$. Άρα $B\hat{D}A = D\hat{B}A = B\hat{G}D$

και επειδή $D\hat{B}G = D\hat{G}B$, στο τρίγωνο DBG θα είναι $DB = DG$. Αλλά $DB = AG$, άρα $AG = GD$, δηλαδή στο τρίγωνο GAD ισχύει $G\hat{A}D = G\hat{D}A$.

Επίσης $G\hat{A}D + G\hat{D}A = B\hat{G}D$. Άρα $B\hat{G}D = 2D\hat{A}G$ και αφού $B\hat{G}D = A\hat{B}D = A\hat{D}B$, θα έχουμε $A\hat{B}D = A\hat{D}B = 2D\hat{A}G$. Άρα το ABD είναι το ζητούμενο τρίγωνο.

□

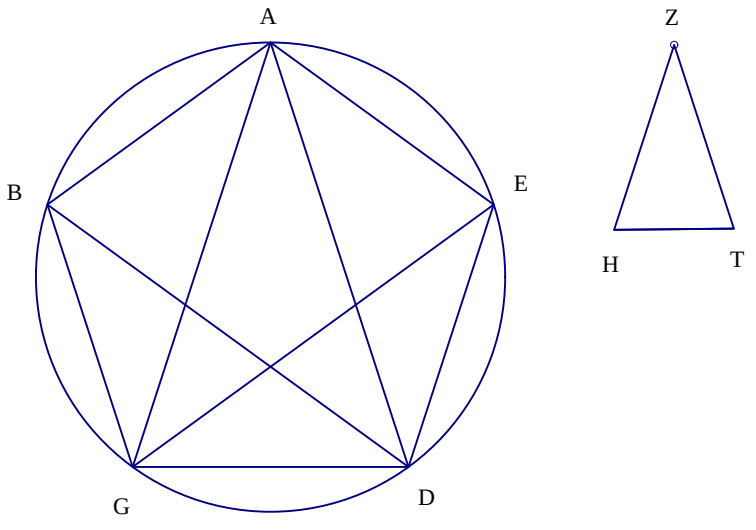
Προφανώς το τρίγωνο έχει γωνίες 36^o,72^o,72^o. Η πρόταση αυτή χρησιμεύει για την κατασκευή του κανονικού πενταγώνου, για το λόγο αυτό πολλοί αποδίδουν την πρόταση στους Πυθαγορείους. Με τη θέση αυτή π.χ. συμφωνεί και ο Πρόκλος, όπως ο ίδιος γράφει σχετικά.

Πρόταση 1.3.5 (Στοιχεία, IV.11):

Σε δοθέντα κύκλο να εγγραφεί πεντάγωνο ισόπλευρο και ισογώνιο.

Απόδειξη:

Έστω ότι δίνεται κύκλος κέντρου Ο και ακτίνας ρ και θέλουμε να εγγράψουμε πεντάγωνο ισόπλευρο και ισογώνιο. Κατασκευάζουμε ισοσκελές τρίγωνο ΖΗΤ με $\hat{H} = \hat{T} = 2\hat{Z}$, πρόταση 1.3.4 και στη συνέχεια εγγράφουμε στον κύκλο (Ο,ρ) τρίγωνο AGD όμοιο με το ΖΗΤ, τέτοιο ώστε $G\hat{A}D = \hat{Z}$ και $A\hat{G}D = \hat{H} = \hat{T} = A\hat{D}G$, όπως στο σχήμα.



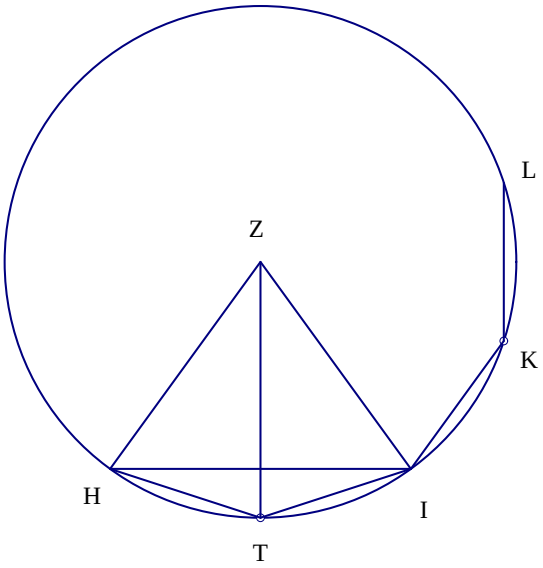
Άρα $A\hat{G}D = G\hat{D}A = 2G\hat{A}D$

Φέρνουμε τις διχοτόμους GE και DB των γωνιών AGD και GDA αντίστοιχα και τα ευθύγραμμα τμήματα AB, BG, GD, DE και EA. Επειδή $A\hat{G}D = G\hat{D}A = 2G\hat{A}D$ και οι GE, DB είναι οι διχοτόμοι των AGD και GDA, θα έχουμε $A\hat{G}E = E\hat{G}D = A\hat{D}B = B\hat{D}G = G\hat{A}D$. Άρα τα αντίστοιχα τόξα θα είναι ίσα, συνεπώς και οι αντίστοιχες πλευρές, δηλαδή $AB = BG = GD = DE = EA$. Επομένως το πεντάγωνο είναι ισόπλευρο. Θα δείξουμε ότι είναι και ισογώνιο.

Όπως είδαμε τα τόξα AB και DE είναι ίσα, άρα και το τόξο $AB + BGD$ είναι ίσο με το $DE + BGD$, δηλαδή τα τόξα $ABGD$ και $EDGB$ είναι ίσα. Φυσικά και οι εγγεγραμμένες γωνίες $A\hat{E}D$ και $B\hat{A}E$ που βαίνουν στα τόξα αυτά είναι ίσες. Όμοια αποδεικνύουμε ότι $B\hat{A}E = A\hat{B}G = B\hat{G}D = G\hat{D}E = A\hat{E}D$. Δηλαδή το πεντάγωνο είναι και ισογώνιο.

□

Παρατηρούμε ότι ο Ευκλείδης για την απόδειξη της πρότασης 1.3.5, χρησιμοποιεί την 1.3.4. Θα μπορούσαμε όμως να κατασκευάσουμε το κανονικό πεντάγωνο κατασκευάζοντας τις επίκεντρες γωνίες 36^o. Από την πρόταση 1.3.4 έχουμε ισοσκελές τρίγωνο ZHT με γωνίες $H = T$=72^o και Z=36^o. Με κέντρο την κορυφή Z και ακτίνα ZH γράφουμε κύκλο (Z,ZH), παίρνουμε τόξα $HT = TI = ...$ και φέρνουμε τις χορδές HI,IL,...



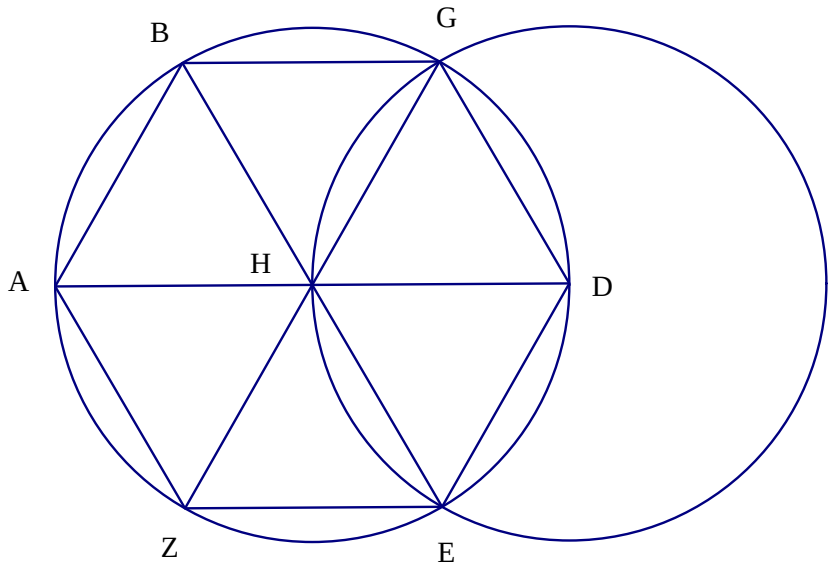
Η ευφυής στραγγική της χρήσης ενός γνωστού σχήματος για την κατασκευή ενός ζητουμένου χρησιμοποιείται συχνά από τον Ευκλείδη (π.χ. Στοιχεία, βιβλίο IV, πρόταση 16).

Πρόταση 1.3.6 (Στοιχεία, IV.11):

Σε δοθέντα κύκλο να εγγραφεί εξάγωνο ισόπλευρο και ισογώνιο.

Απόδειξη:

Έστω δοθέν κύκλος (Η,ρ) και θέλουμε να εγγράψουμε εξάγωνο ισόπλευρο και ισογώνιο. Φέρνουμε τη διάμετρο AD του κύκλου και γράφουμε κύκλο (D, DH) που τέμνει το δοθέντα κύκλο στα σημεία G και E. Φέρνουμε τις EH και GH που τέμνουν τον (Η,ρ) στα B και Z αντίστοιχα.



Γράφουμε τα ευθύγραμμα τμήματα AB, BG, GD, DE, EZ και ZA. Θα δείξουμε ότι το εξάγωνο $ABGDEZ$ είναι ισόπλευρο και ισογώνιο.

Έχουμε ότι $HE = HD$ (ακτίνες του (Η,ρ)) και $DE = DH$ (ακτίνες του (D, DH)), άρα $HE = DE$. Επομένως το τρίγωνο EHD είναι ισόπλευρο.

Άρα $E\hat{H}D = H\hat{D}E = D\hat{E}H$ και αφού το άθροισμα τους είναι ίσο με δυο ορθές, θα είναι $E\hat{H}D = \frac{1}{3} \cdot 2$ ορθές.

Ομοίως αποδεικνύουμε ότι $D\hat{H}G = \frac{1}{3} \cdot 2$ ορθές και επειδή $E\hat{H}G + G\hat{H}B = 2$ ορθές (παραπληρωματικές), θα είναι $G\hat{H}B = \frac{1}{3} \cdot 2$ ορθές.

Επομένως οι γωνίες $E\hat{H}D$, $D\hat{H}G$, $G\hat{H}B$ είναι ίσες, άρα και οι κατακορυφήν τους $B\hat{H}A$, $A\hat{H}Z$, $Z\hat{H}E$ είναι ίσες προς αυτές. Άρα τα αντίστοιχα τόξα είναι ίσα και αφού ίσα τόξα αντιστοιχούν σε ίσες χορδές, θα έχουμε ότι $AB = BG = GD = DE = EZ = ZA$, δηλαδή το εξάγωνο είναι ισόπλευρο. Θα δείξουμε ότι είναι και ισογώνιο.

Είδαμε ότι τα τόξα AZ και DE είναι ίσα, άρα θα είναι ίσο και το τόξο $AZ + ABGD$ με το $DE + ABGD$, επομένως τα τόξα $ZABGD$ και $EDGBA$ είναι ίσα. Άρα $Z\hat{E}D = A\hat{Z}E$ (εγγεγραμμένες που βαίνουν σε ίσα τόξα).

Όμοια αποδυκνείεται ότι $A\hat{Z}E = Z\hat{A}B = A\hat{B}G = B\hat{G}D = G\hat{D}E = D\hat{E}Z$. Άρα το εξάγωνο $ABGDEZ$ είναι και ισογώνιο και έχει εγγραφεί σε δοθέντα κύκλο.

□

Τώρα συνδέοντας π.χ. τις άρτιες κορυφές του κανονικού εξαγώνου κατασκευάζουμε το ισόπλευρο τρίγωνο.

1.4 Η κατασκευή του κανονικού 17-γώνου από το Gauss

Σε αυτό το κεφάλαιο θα δούμε πως ο Gauss μελέτησε την κυκλοτομική επέκταση $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, όπου p είναι περιττός πρώτος. Μελετώντας την επέκταση αυτή 30 χρόνια πριν το Galois, ο Gauss περιέγραψε τα ενδιάμεσα σώματά της και τα χρησιμοποίησε για να δείξει ότι η $x^p - 1 = 0$ είναι επιλύσιμη με ριζικά.

Θα δούμε κάποια αποτελέσματα, τα οποία προκύπτουν εύκολα από τη θεωρία Galois και τα οποία είχε κατανοήσει ο Gauss χρόνια πριν.

Έστω p περιττός πρώτος, τότε $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq \mathbb{Z}_p^*$. Η ισομορφία αυτή προκύπτει εύκολα, αν θεωρήσουμε την απεικόνιση $\Theta : Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{Z}_p^*$, η οποία στέλνει τη $\sigma(\zeta_p) = \zeta_p^t$ στο $t + p\mathbb{Z}$, με $p \not| t$.

Η Θ είναι ομομορφισμός ομάδων. Έστω $\sigma(\zeta_p) = \zeta_p^t$ και $\tau(\zeta_p) = \zeta_p^s$ δυο στοιχεία της ομάδας Galois, τότε $\sigma\tau(\zeta_p) = \sigma(\zeta_p^s) = \zeta_p^{st} = \zeta_p^t\zeta_p^s = \sigma(\zeta_p)\tau(\zeta_p)$, επίσης είναι 1-1, αφού $Ker\theta =< id >$ και επί.

Η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική τάξης $p-1$. Για κάθε θετικό διαιρέτη f του $p-1$ η $\mathbb{Z}_p^*$ έχει μοναδική υποομάδα H_f τάξης f (στο παράρτημα με τις p-ομάδες δείξαμε ότι ισχύει για κάθε αβελιανή), η οποία είναι και κανονική υποομάδα (κάθε υποομάδα αβελιανής ομάδας είναι κανονική).

Ακολουθώντας τον Gauss, ας θέσουμε $e = \frac{p-1}{f}$, δηλαδή $ef = p-1$. Η ομάδα H_f έχει δείκτη e στη $\mathbb{Z}_p^*$.

Λήμμα 1.4.1:

Έστω f και f' θετικοί διαιρέτες του p-1, τότε $H_f \subset H_{f'}$ αν και μόνο αν $f|f'$.

Απόδειξη:

($\Rightarrow$)

Προφανές, αφού από θεώρημα Lagrange ξέρουμε ότι η τάξη της υποομάδας διαιρεί την τάξη της ομάδας.

($\Leftarrow$)

Έχουμε ότι $f|p-1$, άρα υπάρχει μοναδική υποομάδα H_f της G με $|H_f| = f$.

Όμοια έχουμε μοναδική υποομάδα $H_{f'} \subset G$, με $|H_{f'}| = f'$.

Όμως $f|f'$, άρα υπάρχει μοναδική υποομάδα H της $\mathbb{Z}_p^*$ με $|H| = f$, τ.ω. $H \subset H_{f'} \subset G$. Τότε όμως $H \subset G$, με $|H| = f$.

Από μοναδικότητα της H_f έχουμε $H = H_f$.

□

Από την ισομορφία $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq \mathbb{Z}_p^*$ και την αντιστοιχία Galois, τα ενδιάμεσα σώματα της $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ είναι τα σώματα:

$$L_f = \{a \in \mathbb{Q}(\zeta_p) \mid \sigma(a) = a, \text{ για κάθε } \sigma \text{ με } \sigma(\zeta_p) = \zeta_p^i,\ i \in H_f\}$$

όπου το f διατρέχει τους θετικούς διαιρέτες του $p-1$.

Αυτά τα σώματα έχουν τις ακόλουθες ωραίες ιδιότητες.

Πρόταση 1.4.2:

$i)$ Αν L_f ένα ενδιάμεσο σώμα της επέκτασης $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, τότε η $L_f/\mathbb{Q}$ είναι επέκταση Galois, βαθμού e.

$ii)$ Αν f, f' θετικοί διαιρέτες του $p-1$, τότε για τα αντίστοιχα σώματα L_f και $L_{f'}$ ισχύει $L_{f'} \subseteq L_f$ αν και μόνο αν $f|f'$.

Απόδειξη:

$i)$ Από το θεμελιώδες θεώρημα της θεωρίας Galois ξέρουμε ότι αφού $H_f \lhd Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, τότε η $L_f/\mathbb{Q}$ είναι επάκταση Galois βαθμού $[L_f : \mathbb{Q}] = [Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) : H_f] = e$.

$ii)$ $(\Rightarrow)$

Έχουμε $L_{f'} \subseteq L_f$, άρα $H_f \subset H_{f'}$, άρα $f|f'$.

$(\Leftarrow)$

Αφού $f|f'$, από το λήμμα 1.4.1 έχουμε $H_f \subset H_{f'}$, τότε

$x \in L_{f'} \Rightarrow x \in \{a \in \mathbb{Q}(\zeta_p) \mid \sigma(a) = a,\ \forall\sigma : \sigma(\zeta_p) = \zeta_p^i,\ i \in H_{f'}\}$

$\Rightarrow x \in \{a \in \mathbb{Q}(\zeta_p) \mid \sigma(a) = a,\ \forall\sigma : \sigma(\zeta_p) = \zeta_p^i,\ i \in H_f\}$

$\Rightarrow x \in L_f$, άρα $L_{f'} \subseteq L_f$.

□

Ας θεωρήσουμε λοιπόν ότι $p-1 = q_1 \cdot q_2 \cdot \ldots \cdot q_r$ είναι η ανάλυση του $p-1$ σε πρώτους (όχι κατ' ανάγκη διαφορετικούς), τότε θα έχουμε τον πύργο σωμάτων:

$\mathbb{Q} = L_{q_1 \ldots q_r} \subset L_{q_2 \ldots q_r} \subset \ldots \subset L_{q_{r-1} q_r} \subset L_{q_r} \subset L_1 = \mathbb{Q}(\zeta_p)$,

όπου

$$[L_{q_{i+1}\dots q_r} : L_{q_i q_{i+1}\dots q_r}] = \frac{|H_{q_i q_{i+1}\dots q_r}|}{|H_{q_{i+1}\dots q_r}|} = q_i.$$

Περίοδοι

Έστω $ef = p-1$ και $H_f \subset \mathbb{Z}_p^*$ η μοναδική υποομάδα τάξης f. Δοθέντος ενός στοιχείου $a = [i] \in \mathbb{Z}_p^*$, έχουμε $\zeta_p^a = \zeta_p^i$ (αφού $\zeta_p^p = 1$).

Ορισμός:

Έστω $\lambda \in \mathbb{Z}$, με $(\lambda, p) = 1$, τότε $[\lambda] \in \mathbb{Z}_p^*$. Θεωρούμε το σύμπλοκο $[\lambda]H_f$ της H_f στο $\mathbb{Z}_p^*$, τότε ορίζουμε την f-περίοδο του λ να είναι το άθροισμα:

$$(f, \lambda) = \sum_{a \in [\lambda]H_f} \zeta_p^a.$$

Τώρα θα δούμε κάποιες από τις ιδιότητες των f-περιόδων.

Λήμμα 1.4.3:

Έστω $ef = p-1$ και (f, λ) όπως ορίσαμε παραπάνω. Τότε:

$i)$ Δυο f-περίοδοι είτε ταυτίζονται είτε δεν έχουν κανένα κοινό όρο στο άθροισμα.

$ii)$ Υπάρχουν e διακριτές f-περίοδοι.

$iii)$ Οι f-περίοδοι είναι γραμμικά ανεξάρτητες στο $\mathbb{Q}$.

$iv)$ Έστω $\sigma \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ τ.ω. $\sigma(\zeta_p) = \zeta_p^i$, τότε για οποιαδήποτε f-περίοδο (f, λ) θα έχουμε $\sigma((f, \lambda)) = (f, i\lambda)$.

Απόδειξη:

$i)$ Ξέρουμε ότι οι $1, \zeta_p, \dots, \zeta_p^{p-2} \in \mathbb{Q}(\zeta_p)$ είναι γραμμικά ανεξάρτητα στο $\mathbb{Q}$, (αφού $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$). Πολλαπλασιάζοντας με ζ_p, έχουμε ότι και οι $\zeta_p, \dots, \zeta_p^{p-1}$ είναι γραμμικά ανεξάρτητα στο $\mathbb{Q}$. Αυτό σημαίνει ότι δυο f-περίοδοι (ας θυμηθούμε ότι η (f, λ) είναι αθροίσματα όρων $\zeta_p^a,\ a \in [\lambda]H_f$ και αυτοί οι όροι είναι γραμμικά ανεξάρτητοι) ταυτίζονται αν και μόνο αν τα αντίστοιχα σύμπλοκα είναι τα ίδια. Επειδή όμως τα σύμπλοκα είτε είναι ίδια είτε δεν έχουν κοινά στοιχεία, το ίδιο θα ισχύει και για τις f-περιόδους.

$ii)$ Είδαμε λοιπόν ότι κάθε f-περίοδος αντιστοιχεί σε ένα σύμπλοκο, σύμπλοκα όμως έχουμε $\frac{p-1}{f} = e$ (όσος είναι και ο δείκτης της H_f στη $\mathbb{Z}_p^*$).

$iii)$ Από το $i)$ είδαμε ότι οι f-περίοδοι είτε είναι ίδιες είτε δεν έχουν κανένα κοινό όρο στο άθροισμα, άρα αν ήταν γραμμικά εξαρτημένες το ίδιο θα έπρεπε να ισχύει

και για τα $\zeta_p, ..., \zeta_p^{p-1}$, άτοπο.

iv) Θυμόμαστε ότι $\zeta_p^i = \zeta_p^{[i]}$. Τότε

$$\sigma((f,\lambda)) = \sum_{a\in[\lambda]H_f} (\zeta_p^i)^a = \sum_{a\in[\lambda]H_f} \zeta_p^{[i]a},$$

θέτουμε $b = [i]a \in \mathbb{Z}_p^*$ και έχουμε

$$\sigma((f,\lambda)) = \sum_{b\in[i\lambda]H_f} \zeta_p^b = (f, i\lambda).$$

□

Τώρα θα δείξουμε ότι οι f-περίοδοι είναι πρωταρχικά στοιχεία της $L_f/\mathbb{Q}$ και μάλιστα αποτελούν βάση της L_f πάνω από το $\mathbb{Q}$.

Πρόταση 1.4.4:

Έστω L_f το ενδιάμεσο σώμα της επέκτασης $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ που αντιστοιχεί στη H_f, τότε ισχύουν:

i) Αν $(f,\lambda_1), ..., (f,\lambda_e)$ οι διακριτές $f-$περίοδοι, τότε το

$$g(x) = (x-(f,\lambda_1))...(x-(f,\lambda_e))$$

ανήκει στο $\mathbb{Q}[x]$ και είναι το ελάχιστο πολυώνυμο υπέρ του $\mathbb{Q}$ για οποιαδήποτε f-περίοδο.

ii) Κάθε f-περίοδος είναι πρωταρχικό στοιχείο της επέκτασης $L_f/\mathbb{Q}$.

Απόδειξη:

i) Ξέρουμε ότι αν έχουμε μια επέκταση Galois L/K και $G = Gal(L/K)$, τότε για να βρούμε το ανάγωγο πολυώνυμο $p(x)$ πάνω από το K ενός στοιχείου $a \in L$, αρκεί να βρούμε τα συζυγή του ως προς τις μεταθέσεις $\sigma,\ \sigma \in G$, έστω $b_1, ..., b_n$ και τότε

$$p(x) = (x-b_1)...(x-b_n).$$

Έστω λοιπόν μια f-περίοδος $\eta = (f,\lambda)$ που αντιστοιχεί σε ένα σύμπλοκο $[\lambda]H_f$. Αν $[i] \in \mathbb{Z}_p^*$, τότε η f-περίοδος $(f, i\lambda)$ που αντιστοιχεί στο σύμπλοκο $[i\lambda]H_f$ είναι η συζυγής του η πάνω από το $\mathbb{Q}$, όπως είδαμε στο Λήμμα 1.4.3 (iv).

Εφόσον το $[i\lambda]H_f$ μας δίνει όλα τα σύμπλοκα της H_f στη $\mathbb{Z}_p^*$ καθώς μεταβάλλεται το $[i]$, τα συζυγή του η πάνω από το $\mathbb{Q}$ θα είναι οι e διακριτές f-περίοδοι $(f, \lambda_1), ..., (f, \lambda_e)$. Επομένως το ανάγωγο πολυώνυμο στο $\mathbb{Q}$ είναι πράγματι το $g(x)$.

$ii)$ Έχουμε ότι η $\mathbb{Q}(\eta)/\mathbb{Q}$ είναι επέκταση βαθμού e (προκύπτει από το βαθμό του αναγώγου πολυωνύμου), όμως και η $L_f/\mathbb{Q}$ έχει βαθμό e. Αφού η $Gal(\mathbb{Q}(\zeta_p/\mathbb{Q})) \simeq Z_p^*$ έχει μοναδική υποομάδα βαθμού e, την H_e, αυτή ορίζει (αντιστοιχία Galois) ένα ενδιάμεσο σώμα που να έχει βαθμό e, άρα θα πρέπει $\mathbb{Q}(\eta) = L_f$ και προκύπτει το (ii).

□

Σαν συνέπεια έχουμε την παρακάτω ενδιαφέρουσα βάση της $L_f/\mathbb{Q}$

Λήμμα 1.4.5:

Οι f-περίοδοι αποτελούν βάση του L_f πάνω από το $\mathbb{Q}$.

Απόδειξη:

Από την πρόταση 1.4.4 έχουμε ότι οι f-περίοδοι είναι πρωταρχικά στοιχεία του L_f, γραμμικά ανεξάρτητα (από λήμμα 1.4.3) και είναι e το πλήθος, αφού $[L_f : \mathbb{Q}] =$e. Συνεπώς αποτελούν βάση του L_f πάνω από το $\mathbb{Q}$.

□

Θα αποδείξουμε ένα λήμμα από τη θεωρία ομάδων το οποίο θα μας φανεί χρήσιμο στη συνέχεια.

Λήμμα 1.4.6:

Έστω $A \subset B$ υποομάδες μιας ομάδας $(G, \cdot)$ και ο δείκτης $[B : A]$ της A στην B είναι d. Κάθε αριστερό σύμπλοκο της B στη G είναι διακριτή ένωση d αριστερών συμπλόκων της A στη G.

Απόδειξη:

$[B : A] = d$, τότε $B = \cup_{j=1}^{d} b_j A$ (διακριτή ένωση) με $b_j \in B$. Ας θεωρήσουμε στοιχείο $g \in G$ και να πάρουμε το αριστερό σύμπλοκο:

$gB = g \cup_{j=1}^{d} b_j A = \cup_{j=1}^{d} g b_j A \cup_{j=1}^{d} h_j A$, με $h_j = g b_j \in G$.

Για να ολοκληρωθεί η απόδειξη πρέπει να δείξουμε ότι η ένωση είναι διακριτή. Έστω $h_k A = h_l A$, με $k, l \in 1, ..., d$, δηλαδή $h_k \in h_l A$, τότε $g b_k \in g b_l A$ και έχουμε ότι $g b_k = g b_l a$, για κάποιο $a \in A$.

Αφού η $(G,\cdot)$ ομάδα, θα υπάρχει το g^{-1} και πολλαπλασιάζοντας με αυτό από αριστερά την πάνω σχέση έχουμε ότι $b_k = b_l a$, δηλαδή $b_k \in b_l A$ που συνεπάγεται ότι $b_l A = b_k A$ το οποίο είναι άτοπο αφού $B = \cup_{j=1}^{d} b_j A$, με $b_j \in B$ είναι διακριτή ένωση.

□

Στη συνέχεια θα περιγράψουμε την επέκταση $L_f/L_{f'}$ με τη βοήθεια των περιόδων, όπου f, f' θετικοί διαιρέτες του $p-1$, με $f|f'$. Αν θέσουμε $d = \frac{f'}{f}$, όπως έχουμε δει θα έχουμε $[L_f : L_{f'}] = \frac{[L_f:\mathbb{Q}]}{[L_{f'}:\mathbb{Q}]} = \frac{e}{e'} = \frac{\frac{p-1}{f}}{\frac{p-1}{f'}} = \frac{f'}{f} = d$. Κάθε f-περίοδος (f,λ) είναι πρωταρχικό στοιχείο του L_f πάνω από το $L_{f'}$. Θα περιγράψουμε το ελάχιστο πολυώνυμο της (f,λ) πάνω από το $L_{f'}$.

Ας υποθέσουμε λοιπόν ότι η H_f είναι η υποομάδα με δείκτη $d = \frac{f'}{f}$ στην $H_{f'}$. Από το λήμμα 1.4.6 κάθε σύμπλοκο του $H_{f'}$ στο Z_p^* είναι διακριτή ένωση d συμπλόκων του H_f.

Έχουμε ότι το $[\lambda]H_{f'}$ είναι η διακριτή ένωση:

$$[\lambda]H_{f'} = [\lambda_1]H_f \bigcup ... \bigcup [\lambda_d]H_f \qquad (1)$$

μπορούμε να θεωρήσουμε $\lambda = \lambda_1$, αφού $[\lambda]H_f \subset [\lambda]H_{f'}$. Αυτό θα μας βοηθήσει στην ακόλουθη περιγραφή του ελάχιστου πολυωνύμου.

Πρόταση 1.4.7:

Έστω f, f' θετικοί διαιρέτες του $p-1$, με $f|f'$ και $d = \frac{f'}{f}$. Δοσμένης f-περιόδου (f,λ), θεωρούμε $\lambda_1 = \lambda, \lambda_2, ..., \lambda_d$ όπως στην (1). Τότε το $h(x) = (x-(f,\lambda_1))...(x-(f,\lambda_d))$ ανήκει στο $L_{f'}[x]$ και είναι το ελάχιστο πολυώνυμο της (f,λ) πάνω από το $L_{f'}$.

Απόδειξη:

Όπως και στην απόδειξη 1.4.4, θεωρούμε $\eta = (f,\lambda)$ μια f-περίοδο, αρκεί να δείξουμε ότι καθώς η σ διατρέχει τα σχτοιχεία της $Gal(\mathbb{Q}(\zeta_p)/L_{f'})$, τα στοιχεία $\sigma(\eta)$ μας δίνουν τις f-περιόδους $(f,\lambda_1), ..., (f,\lambda_d)$.

Για να το δείξουμε αυτό θεωρούμε $\sigma \in Gal(\mathbb{Q}(\zeta_p)/L_{f'})$ με $\sigma(\zeta_p) = \zeta_p^i$, για $[i] \in H_{f'}$, τότε $\sigma(\eta) = \sigma((f,\lambda)) = (f, i\lambda)$, (λήμμα 1.4.3 (iv)).

Η $(f,i\lambda)$ αντιστοιχεί στο σύμπλοκο $[i\lambda]H_f$. Όμως $[i\lambda]H_f \subset [i\lambda]H_{f'} = [\lambda][i]H_{f'} = [\lambda]H_f$, αφού $[i] \in H_{f'}$.

Από τη σχέση $[i\lambda]H_f \subset [\lambda]H_f$ και από την (1) $[\lambda]H_{f'} = [\lambda_1]H_f \bigcup ... \bigcup [\lambda_d]H_f$ έπεται ότι $[i\lambda]H_f = [\lambda_j]H_f$ για κάποιο $j = 1, .., d$. Επειδή λοιπόν τα σύμπλοκα είναι

ίδια θα είναι ίδιες και οι αντίστοιχες f-περίοδοι. Δηλαδή $(f, i\lambda) = (f, \lambda_j)$, οπότε και $\sigma(\eta) = (f, \lambda_j)$.

Έχουμε δείξει ότι τα $\sigma(\eta)$ παίρνουν τιμές από το σύνολο $\{(f, \lambda_1), ..., (f, \lambda_d)\}$. Για να ολοκληρωθεί η απόδειξη θα πρέπει να δείξουμε ότι για κάθε f-περίοδο (f, λ_j), με $j = 1, ..., d$ υπάρχει $i \in H_{f'}$ τ.ω. $\sigma(\eta) = (f, \lambda_j)$, δηλαδή $(f, i\lambda) = (f, \lambda_j)$. Από την (1) υπάρχει στοιχείο, έστω $i \in H_{f'}$ τ.ω. $\lambda i = \lambda_j a$ για κάποιο $a \in H_f$.

Συνεπώς $[\lambda i]H_f = [\lambda_j a]H_f = [\lambda_j]H_f$ (αφού $a \in H_f$), άρα $(f, i\lambda) = (f, \lambda_j)$.

Αφού λοιπόν δείξαμε ότι τα συζυγή του η είναι (f, λ_j) για κάποια $j = 1, ..., d$ και ότι για κάθε $i = 1, ..., d$ το (f, λ_j) είναι συζυγές του η, έχουμε ότι είναι ακριβώς αυτά και η πρόταση αποδείχθηκε.

□

Για να μπορέσουμε να μελετήσουμε συγκεκριμένα προβλήματα με τη χρήση των περιόδων, θα δώσουμε προτάσεις που θα μας βοηθήσουν να τις χειριστούμε καλύτερα.

Βασιζόμενοι πάντα στη σκέψη του Gauss, θεωρούμε ένα γεννήτορα $[g]$ της κυκλικής ομάδας $\mathbb{Z}_p^*$. Αφού η τάξη της ομάδας είναι $p - 1$, έχουμε ότι:

$$\mathbb{Z}_p^* = \{[1], [g], [g^2], ..., [g^{p-2}]\}$$

Με άλλα λόγια οι $p - 1$ αριθμοί $1, g, g^2, ..., g^{p-2}$ είναι οι μη μηδενικές κλάσεις $(\mathrm{mod}\ p)$. Το g ονομάζεται πρωταρχική ρίζα $(\mathrm{mod}\ p)$.

Δοσμένης μιας πρωταρχικής ρίζας g και $ef = p - 1$, έχουμε ότι ο g^e είναι γεννήτορας της H_f (το g^e παράγει υποομάδα της $\mathbb{Z}_p^*$ τάξης f, από μοναδικότητα όμως της H_f πρέπει να είναι ίδιες), δηλαδή:

$$H_f = \{[1], [g^e], [g^{2e}], ..., [g^{(f-1)e}]\}.$$

Επομένως το σύμπλοκο $[\lambda]H_f$ δίνει την f-περίοδο:

$$(f, \lambda) = \sum_{a \in [\lambda]H_f} \zeta_p^a = \sum_{a \in \{[\lambda], [\lambda g^e], [\lambda g^{2e}], ..., [\lambda g^{(f-1)e}]\}} \zeta_p^a = \zeta_p^{\lambda} + \zeta_p^{\lambda g^e} + ... + \zeta_p^{\lambda g^{(f-1)e}}.$$

Μέχρι τώρα θεωρούσαμε ότι $[\lambda] \in \mathbb{Z}_p^*$, δηλαδή $p \not| \lambda$. Όμως η παραπάνω σχέση έχει νόημα για κάθε ακέραιο λ. Αφού $\zeta_p^p = 1$, εύκολα προκύπτει ότι $(f, \lambda) = f$ όταν $p|\lambda$.

Για τυχαίο $\lambda \in \mathbb{Z}$ η (f, λ) λέγεται γενικευμένη περίοδος. Έτσι μια γενικευμένη περίοδος είναι η συνήθης περίοδος αν $p \not| \lambda$ ή είναι ίση με το f αν $p|\lambda$.

Για να υπολογίσουμε τα ελάχιστα πολυώνυμα με τη βοήθεια των προτάσεων 1.4.4 και 1.4.7 θα χρειαστεί να πολλαπλασιάσουμε f-περιόδους. Ο Gauss εξέφρασε το γινόμενο δυο f-περιόδων με τον ακόλουθο τρόπο.

Πρόταση 1.4.8:

Έστω (f, λ) και (f, μ) δυο f-περίοδοι με $p \not| \lambda$ και $p \not| \mu$, τότε

$$(f, \lambda) \cdot (f, \mu) = \sum_{[\lambda'] \in [\lambda] H_f} (f, \lambda' + \mu) = \sum_{j=0}^{f-1} (f, \lambda g^{je} + \mu).$$

Απόδειξη:

Έστω $h = g^e$ γεννήτορας της H_f, τότε

$$(f, \mu) = \sum_{l=0}^{f-1} \zeta_p^{\mu h^l}.$$

Έχουμε επίσης ότι $[\lambda] H_f = [\lambda h^l] H_f$ για κάθε λ (αφού $f \in H_f$), άρα $(f, \lambda) = (f, \lambda h^l)$. Επομένως

$$(f, \lambda) \cdot (f, \mu) = \sum_{l=0}^{f-1} (f, \lambda) \zeta_p^{\mu h^l} = \sum_{l=0}^{f-1} (f, \lambda h^l) \zeta_p^{\mu h^l} = \sum_{l=0}^{f-1} (\sum_{j=0}^{f-1} \zeta_p^{\lambda h^l h^j}) \zeta_p^{\mu h^l} =$$

$$\sum_{j=0}^{f-1} (\sum_{l=0}^{f-1} \zeta_p^{(\lambda h^j + \mu) h^l}) = \sum_{j=0}^{f-1} (f, \lambda h^j + \mu)$$

Αντικαθιστώντας από τη σχέση $h = g^e$, έχουμε $(f, \lambda) \cdot (f, \mu) = \sum_{j=0}^{f-1} (f, \lambda g^{je} + \mu)$.

□

Τώρα είμαστε έτοιμοι να δούμε πως ο Gauss έδειξε ότι η $x^{17} - 1 = 0$ είναι επιλύσιμη με ριζικά (αυτό όπως είδαμε ισοδυναμεί με την κατασκευασιμότητα του κανονικού 17-γώνου).

Ας θεωρήσουμε λοιπόν την επέκταση $\mathbb{Q}(\zeta_{17})/\mathbb{Q}$, τα ενδιάμεσα σώματα L_f, με f διαιρέτες του 17-1=16 και τις αντίστοιχες υποομάδες H_f της $Gal(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \simeq \mathbb{Z}_{17}^*$.

$$\mathbb{Q} \subseteq L_8 \subseteq L_4 \subseteq L_2 \subseteq \mathbb{Q}(\zeta_{17})$$

$$Gal(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \simeq Z_{17}^* \geq H_8 \geq H_4 \geq H_2 \geq < id >$$

Είναι

$\mathbb{Z}_{17}^* = \{1, 2, 3, ..., 16\} =< 3 >$

$H_8 =< 3^{\frac{p-1}{f}} >=< 3^{\frac{17-1}{8}} >=< 3^2 >=< 9 >= \{9, 13, 15, 16, 8, 4, 2, 1\}$

$H_4 =< 3^{\frac{17-1}{4}} >=< 3^4 >=< 13 >= \{1, 4, 13, 16\}$

$H_2 =< 3^{\frac{17-1}{2}} >=< 3^8 >=< 16 >= \{1, 16\}$

Στη συνέχεια θα υπολογίσουμε τις f-περιόδους και τα ελάχιστα πολυώνυμα τους. Αρχικά θα βρούμε το ελάχιστο πολυώνυμο των 8-περιόδων πάνω από το $\mathbb{Q}$. Οι 8-περίοδοι είναι $e = \frac{p-1}{f} = \frac{17-1}{8} = 2$ το πλήθος. Τα σύμπλοκα της H_8 στην $\mathbb{Z}_{17}^*$ είναι οι

$$H_8 = \{1, 2, 4, 8, 9, 13, 15, 16\}$$

$$3H_8 = \{3, 6, 12, 7, 10, 5, 11, 14\}$$

που αντιστοιχούν στις περιόδους (8,1) και (8,3). Από την πρόταση 1.4.4 το ελάχιστο πολυώνυμο των (8,1) και (8,3) είναι το:

$p_1(x) = (x - (8,1))(x - (8,3)) = x^2 - ((8,1) + (8,3))x + (8,1)(8,3)$.

Οι $\zeta_p, \zeta_p^2, ..., \zeta_p^{p-1}$ είναι ρίζες του $x^{p-1} + x^{p-2} + ... + x + 1$ άρα $\sum_{i=1}^{p-1} \zeta_p^i = -1$ (τύποι $Vieta$), τότε

$$(8,1) + (8,3) = \sum_{a \in H_8} \zeta_{17}^a + \sum_{b \in 3H_8} \zeta_{17}^b = \sum_{a \in \mathbb{Z}_{17}^*} \zeta_{17}^a = \sum_{i=1}^{16} \zeta_{17}^i = -1$$

άρα $p_1(x) = x^2 + x + (8,1)(8,3)$. Αρκεί να υπολογίσουμε το $(8,1)(8,3)$. Από την πρόταση 1.4.8 έχουμε:

$$(8,1)(8,3) = \sum_{j=0}^{f-1}(f, \lambda g^{je}+\mu) = \sum_{j=0}^{7}(8, 3^{2j}+3) = (8,4)+(8,12)+(8,16)+(8,1)+$$
$(8,2) + (8,11) + (8,7) + (8,5) = 4(8,1) + 4(8,3) = 4((8,1) + (8,3)) = 4(-1) = -4.$

Δηλαδή

$$p_1(x) = x^2 + x - 4.$$

Το σώμα ανάλυσης του $p_1(x)$ είναι το $L_8/\mathbb{Q}$ (η επέκταση έχει βάση τις 8-περιόδους, δες λήμμα 1.4.5).

Θα βρούμε τώρα το ελάχιστο πολυώνυμο των 4-περιόδων, (που είναι πρωταρχικά στοιχεία της L_4/L_8) πάνω από το L_8. Έχουμε $H_8 = H_4 \cup 2H_4$, δηλαδή $(8,1) = (4,1) + (4,2)$. Το ελάχιστο πολυώνυμο των $(4,1), (4,2)$ στην L_8, από πρόταση 1.4.7 είναι:

$p_2(x) = (x - (4,1))(x - (4,2)) = x^2 - ((4,1) + (4,2))x + (4,1)(4,2) = x^2 - (8,1)x + (4,1)(4,2)$.

Από την πρόταση 1.4.8 έχουμε:

$$(4,1)(4,2) = \sum_{j=0}^{3}(4, 3^{4j} + 2) = (4,3) + (4,15) + (4,1) + (4,6) =$$

$$= \sum_{a\in 3H_4} \zeta_{17}^a + \sum_{b\in 15H_4} \zeta_{17}^b + \sum_{c\in H_4} \zeta_{17}^c + \sum_{d\in 6H_4} \zeta_{17}^d$$

όμως $\mathbb{Z}_{17}^* = 3H_4 \cup 15H_4 \cup H_4 \cup 6H_4$ και έπεται ότι

$$(4,1)(4,2) = \sum_{a\in\mathbb{Z}_{17}^*} \zeta_{17}^a = -1.$$

Δηλαδή το

$$p_2(x) = x^2 - (8,1)x - 1$$

είναι το ελάχιστο πολυώνυμο των (4,1),(4,2) πάνω από το L_8.

Επίσης $3H_8 = 3H_4 \bigcup 6H_4$, δηλαδή (8,3)=(4,3)+(4,6). Από την πρόταση 1.4.7 το ελάχιστο πολυώνυμο των (4,3) και (4,6) πάνω από το L_8 είναι το

$p_3(x) = (x - (4,3))(x - (4,6)) = x^2 - ((4,3) + (4,6))x + (4,3)(4,6)$.

Από τη πρόταση 1.4.8 έχουμε:

$$(4,3)(4,6) = \sum_{j=0}^{3}(4, 3\cdot 3^{4j}+6) = (4,9)+(4,15)+(4,14)+(4,7) = -1$$

Επομένως

$$p_3(x) = x^2 - (8,3)x - 1.$$

Τώρα θα θεωρήσουμε την επέκταση L_2/L_4 και θα υπολογίσουμε το ελάχιστο πολυώνυμο των 2-περιόδων (2,1) και (2,4) πάνω από το L_4.

Έχουμε ότι $H_4 = H_2 \cup 4H_2$, άρα (4,1)=(2,1)+(2,4).

Το ελάχιστο πολυώνυμο των (2,1) και (2,4) πάνω από το L_4, από πρόταση 1.4.7 είναι το

$p_4(x) = (x-(2,1))(x-(2,4)) = x^2 - ((2,1)+(2,4))x + (2,1)(2,4) = x^2 - (4,1)x + (2,1)(2,4)$

Από πρόταση 1.4.8

$(2,1)(2,4) = \sum_{j=0}^{1}(2, 3^{j8}+4) = (2,5)+(2,3) = (4,3)$, (αφού $5H_2 \cup 3H_2 = 3H_4$).

Δηλαδή

$$p_4(x) = x^2 - (4,1)x + (4,3).$$

Οι 1-περίοδοι για $p = 17$ είναι οι 17-ρίζες της μονάδας,

$(1,\lambda) = \sum_{a\in\lambda H_1}\zeta_{17}^a = \sum_{a\in\{\lambda\}}\zeta_{17}^\lambda$, για λ=1,...,16.

$H_2 = H_1 \cup 16H_1$, δηλαδή (2,1)=(1,1)+(1,16)

Το ελάχιστο πολυώνυμο των (1,1)=ζ_{17} και $(1,16) = \zeta_{17}^{16}$ πάνω από το L_2, σύμφωνα με την πρόταση 1.4.7 θα είναι

$$p_5(x) = (x-(1,1))(x-(1,16)) =$$
$$= x^2 - ((1,1)+(1,16))x + (1,1)(1,16) = x^2 - (2,1)x + (1,1)(1,16),$$

με

$$(1,1)(1,16) = \sum_{j=0}(1, 3^{8j}+16) = (1,17) = \zeta_{17}^{17} = 1$$

δηλαδή το $p_5(x) = x^2 - (2,1)x + 1$ είναι το ελάχιστο πολυώνυμο των ζ_{17} και ζ_{17}^{16} πάνω από το L_2, τότε $\zeta_{17} + \zeta_{17}^{16} = -(-(2,1)) = (2,1)$, όμως $\zeta_{17} + \zeta_{17}^{16} = 2\cos\frac{2\pi}{17}$ (αφού $\zeta_p^k + \zeta_p^{p-k} = 2\cos\frac{2k\pi}{p}$), άρα

$$(2,1) = 2\cos\frac{2\pi}{17}.$$

Για να υπολογίσουμε το (2,1) θα πρέπει να λύσουμε τα δευτεροβάθμια πολυώνυμα $p_i(x)$, για $i = 1, 2, 3, 4$. Το πρόβλημα είναι πως θα αντιστοιχίσουμε τις ρίζες στις περιόδους. Για παράδειγμα οι ρίζες του $p_1(x)$ είναι $\frac{-1+\sqrt{17}}{2}$ και $\frac{-1-\sqrt{17}}{2}$, αλλά πως θα τις αντιστοιχίσουμε στις 8-περιόδους (8,1) και (8,3);

Αυτό που έκανε ο Gauss ήταν να υπολογίσει αριθμητικά τις περιόδους και τις εκφρασμένες με ριζικά λύσεις των δευτεροβάθμιων εξισώσεων και να τις συγκρίνει.

Έχουμε λοιπόν ότι:

$(8,1) = \sum_{a \in H_8} \zeta_{17}^a = \zeta_{17} + \zeta_{17}^2 + \zeta_{17}^4 + \zeta_{17}^8 + \zeta_{17}^9 + \zeta_{17}^{13} + \zeta_{17}^{15} + \zeta_{17}^{16}$

με τη βοήθεια της σχέσης $\zeta_p^k + \zeta_p^{p-k} = 2\cos\frac{2k\pi}{p}$ έπεται ότι

$(8,1) = 2\cos\frac{2\pi}{17} + 2\cos\frac{4\pi}{17} + 2\cos\frac{8\pi}{17} + 2\cos\frac{16\pi}{17} \simeq 1,5615528128$

Ομοίως φτάνουμε στα παρακάτω αποτελέσματα:

$(4,1) = 2\cos\frac{2\pi}{17} + 2\cos\frac{8\pi}{17} \simeq 2,0494811777$

$(4,3) = 2\cos\frac{6\pi}{17} + 2\cos\frac{10\pi}{17} \simeq 0,3441507314$

$(2,1) = 2\cos\frac{2\pi}{17} \simeq 1,8649444588$

Άρα η περίοδος $(8,1) \simeq 1,5615528128$ αντιστοιχεί στη ρίζα $\frac{-1+\sqrt{17}}{2}$ του $p_1(x)$. Δηλαδή $(8,1) = \frac{-1+\sqrt{17}}{2}$ και $(8,3) = \frac{-1-\sqrt{17}}{2}$.

Τότε το $p_2(x) = x^2 - (8,1)x - 1 = x^2 - (\frac{-1+\sqrt{17}}{2})x - 1$ έχει ρίζες τις $\frac{1}{4}(-1+\sqrt{17}+\sqrt{34-3\sqrt{17}})$ και $\frac{1}{4}(-1+\sqrt{17}-\sqrt{34-3\sqrt{17}})$. Σύμφωνα με τους υπολογισμούς έχουμε $(4,1) = \frac{1}{4}(-1+\sqrt{17}+\sqrt{34-3\sqrt{17}})$ και $(4,2) = \frac{1}{4}(-1+\sqrt{17}-\sqrt{34-3\sqrt{17}})$.

Από το $p_3(x) = x^2 - (8,3)x - 1 = x^2 + \frac{-1-\sqrt{17}}{2}x - 1$ η 4-περίοδος (4,3) αντιστοιχεί στη ρίζα $\frac{1}{4}(-1-\sqrt{17}+\sqrt{34+2\sqrt{17}})$.

Είδαμε ότι το $(2,1) = 2\cos\frac{2\pi}{17}$ είναι ρίζα του πολυωνύμου $p_4(x) = x^2 - (4,1)x + (4,3) = x^2 - \frac{1}{4}(-1+\sqrt{17}+\sqrt{34-3\sqrt{17}})x + \frac{1}{4}(-1-\sqrt{17}+\sqrt{34+2\sqrt{17}})$

και $(2,1) \simeq 1,8649444588$, υπολογίζοντας τις ρίζες του $p_4(x)$ έχουμε

$$(2,1) = 2(-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34+2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}})$$

δηλαδή

$$\cos\frac{2\pi}{17} = -\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34+2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

□

1.5 Γεωμετρική κατασκευή του κανονικού 17-γώνου από τον Richmond

Η απόδειξη που θα ακολουθήσει βασίζεται σε αυτή του Gauss, αλλά είναι διατυπωμένη έτσι ώστε να μην εμφανίζονται οι f-περίοδοι και να μπορεί να διδαχθεί σε ένα παιδί της δευτεροβάθμιας εκπαίδευσης. Τα x_i, y_i που θα οριστούν " αυθαίρετα " δεν είναι τίποτα άλλο εκτός από τις f-περίοδους του Gauss. Στη συνέχεια θα δούμε τη γεωμετρική απόδειξη του Richmond (1893).

Σκοπός μας είναι να βρούμε εκφράσεις με ριζικά των ριζών του πολυωνύμου $\frac{t^{16}-1}{t-1} = t^{16} + ... + t + 1$, στο $\mathbb{C}$ (1)

Έστω $\theta = \frac{2\pi}{17}$, και $\varepsilon_k = e^{ik\theta} = \cos k\theta + i \sin k\theta$, με $k = 1, ..., 16$.

Τότε οι ρίζες της παραπάνω εξίσωσης στο $\mathbb{C}$ θα είναι οι $\varepsilon_1, ..., \varepsilon_{16}$.

Ορίζουμε

$$x_1 = \varepsilon_1 + \varepsilon_9 + \varepsilon_{13} + \varepsilon_{15} + \varepsilon_{16} + \varepsilon_8 + \varepsilon_4 + \varepsilon_2$$

$$x_2 = \varepsilon_3 + \varepsilon_{10} + \varepsilon_5 + \varepsilon_{11} + \varepsilon_{14} + \varepsilon_7 + \varepsilon_{12} + \varepsilon_6$$

$$y_1 = \varepsilon_1 + \varepsilon_{13} + \varepsilon_{16} + \varepsilon_4$$

$$y_2 = \varepsilon_9 + \varepsilon_{15} + \varepsilon_8 + \varepsilon_2$$

$$y_3 = \varepsilon_3 + \varepsilon_5 + \varepsilon_{14} + \varepsilon_{12}$$

$$y_4 = \varepsilon_{10} + \varepsilon_{11} + \varepsilon_7 + \varepsilon_6$$

Με τη βοήθεια της σχέσης $\varepsilon_k + \varepsilon_{17-k} = 2\cos k\theta$ για $k = 1, ..., 16$ θα έχουμε:

$$x_1 = 2(\cos\theta + \cos 8\theta + \cos 4\theta + \cos 2\theta) \quad (2)$$

$$x_2 = 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta) \quad (3)$$

$$y_1 = 2(\cos\theta + \cos 4\theta) \quad (4)$$

$$y_2 = 2(\cos 8\theta + \cos 2\theta) \qquad (5)$$

$$y_3 = 2(\cos 3\theta + \cos 5\theta) \qquad (6)$$

$$y_4 = 2(\cos 7\theta + \cos 6\theta) \qquad (7)$$

Το άθροισμα ριζών της $t^{16} + ... + t + 1$ είναι ίσο με -(σταθερός όρος)=-1. Δηλαδή, $x_1 + x_2 = \varepsilon_1 + ... + \varepsilon_{16} = -1$.

Από τις σχέσεις (2),(3) και τη σχέση $2\cos(m\theta)\cos(n\theta) = \cos(m+n)\theta + \cos(m-n)\theta$, έχουμε:

$x_1 \cdot x_2 = 2(\cos 4\theta + \cos 2\theta + \cos 8\theta + \cos 6\theta + \cos 4\theta + \cos 6\theta + \cos 5\theta + \cos 7\theta + \cos 11\theta + \cos 5\theta + \cos 15\theta + \cos\theta + \cos 13\theta + \cos 3\theta + \cos 14\theta + \cos 2\theta + \cos 7\theta + \cos\theta + \cos 3\theta + \cos 11\theta + \cos\theta + \cos 9\theta + \cos 2\theta + \cos 10\theta + \cos 5\theta + \cos\theta + \cos 9\theta + \cos 5\theta + \cos 7\theta + \cos 3\theta + 4\cos\theta + \cos 8\theta) = -1$

(Χρησιμοποιώντας τις σχέσεις $\varepsilon_k + \varepsilon_{17-k} = 2\cos k\theta$ και $x_1 + x_2 = -1$)

Άρα $x_1 + x_2 = -1$ και $x_1 \cdot x_2 = -4$, δηλαδή τα x_1 και x_2 είναι ρίζες της

$$t^2 + t - 4 \qquad (8)$$

και $x_1 > 0$, δηλαδή $x_1 > x_2$.

Επίσης $y_1 + y_2 = x_1$ από (4),(5) και $y_1 \cdot y_2 = -1$ (όπως παραπάνω).

Άρα τα y_1, y_2 είναι ρίζες του

$$t^2 - x_1 t - 1 \qquad (9)$$

με $y_1 > y_2$.

Όμοια τα y_3, y_4 είναι ρίζες του

$$t^2 - x_2 t - 1 \qquad (10)$$

με $y_3 > y_4$.

Τώρα $2\cos\theta + 2\cos 4\theta = y_1$ και $4\cos\theta \cdot \cos 4\theta = 2(\cos 5\theta + \cos 3\theta) = y_3$

άρα τα $z_1 = 2\cos\theta$ και $z_2 = 2\cos 4\theta$ είναι ρίζες του

$$t^2 - y_1 t + y_3 \qquad (11)$$

με $z_1 > z_2$.

Λύνοντας τις εξισώσεις (8) εως (11) και με τη βοήθεια των ανισώσεων καταλήγουμε στην ισότητα

$$\cos\theta = -\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34+2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

Είδαμε λοιπόν μια απλουστευμένη μορφή της αλγεβρικής απόδειξης του Gauss, τώρα θα δώσουμε τη γεωμετρική κατασκευή του Richmond.

Έστω φ η μικρότερη οξεία γωνία τέτοια ώστε $tan4\varphi = 4$, έπεται ότι οι $\varphi, 2\varphi$ και 4φ είναι όλες οξείες. Θεωρούμε τα $x_1, x_2, y_1, y_2, y_3, y_4$ όπως πριν, τότε η εξίσωση $t^2 + t - 4$, που όπως είδαμε έχει ρίζες τα x_1,x_2 γράφεται και σαν $t^2 + 4cot(4\varphi)t - 4$ τις οποίας οι ρίζες είναι $2tan2\varphi, -2cot2\varphi$, άρα θα έχουμε $x_1 = 2tan2\varphi$ και $x_2 = -2cot2\varphi$, έτσι αντικαθιστώντας στις $t^2 - x_1 t - 1$ και $t^2 - x_2 t - 1$ θα βρούμε

$$y_1 = tan(\varphi + \frac{\pi}{4})$$

$$y_2 = tan(\varphi - \frac{\pi}{4})$$

$$y_3 = tan\varphi$$

$$y_4 = -cot\varphi$$

Έχουμε $2(cos3\theta + cos5\theta) = y_3$ (από τη σχέση (6))

και $4cos3\theta cos5\theta = 2(cos8\theta + cos2\theta = y_2)$ (από τη σχέση (5)).

Δηλαδή

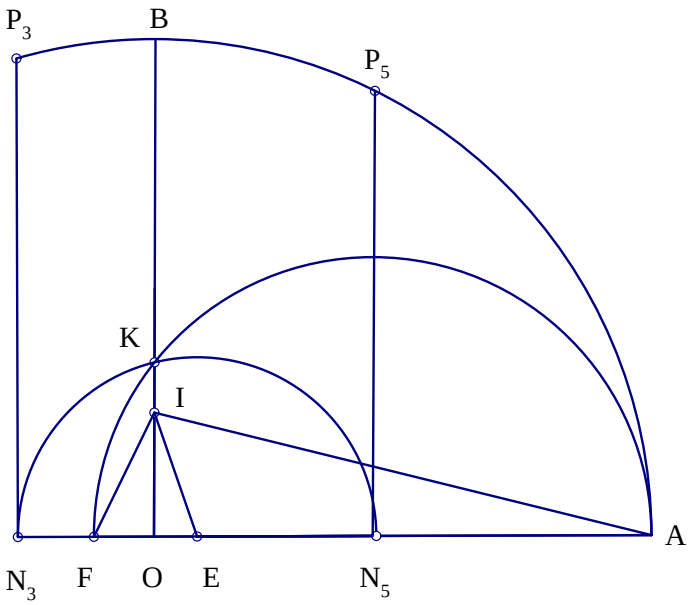
$$2cos3\theta + 2cos5\theta = tan\varphi \;\; και \;\; 4cos3\theta cos5\theta = tan(\varphi - \frac{\pi}{4})$$

Άρα τα $2cos3\theta$ και $2cos5\theta$ είναι ρίζες του $t^2 - tan\varphi \cdot t + tan(\varphi - \frac{\pi}{4})$ $\qquad (*)$.

(Η παραπάνω σχέση είναι πολύ σημαντική για την κατασκευή του κανονικού 17-γώνου.)

Κάνουμε την παρακάτω κατασκευή.

Έστω ΟΑ και ΟΒ δυο κάθετες ακτίνες ενός τυχαίου κύκλου. Παίρνουμε ΟΙ=$\frac{1}{4}$ΟΒ και $O\hat{I}E = \frac{1}{4}O\hat{I}A$. Βρίσκουμε F στην ευθεία ΟΑ τ.ω. $E\hat{I}F = \frac{\pi}{4}$. Φέρνουμε τον κύκλο με διάμετρο AF ο οποίος τέμνει την ΟΒ στο Κ και τον κύκλο κέντρου Ε που διέρχεται από το Κ, ο οποίος κόβει το ΟΑ στα N_3 και N_5. Φέρνουμε N_3P_3 και N_5P_5 κάθετες στην ΟΑ, όπως στο σχήμα.



Είναι $OA = OB = OP_3 = OP_5$ =ακτίνα του κύκλου.

Τότε $O\hat{I}A = 4\varphi$, αφού $tanO\hat{I}A = \frac{OA}{OI} = \frac{OA}{\frac{1}{4}OB} = \frac{OA}{\frac{1}{4}OA} = 4$

και $O\hat{I}E = \frac{1}{4}O\hat{I}A = \frac{1}{4}4\varphi = \varphi$.

Επίσης $2(cosA\hat{O}P_3 + cosA\hat{O}P_5) = 2(cosN_3\hat{O}P_3 - cosN_5\hat{O}P_5) = 2(\frac{ON_3}{OP_3} - \frac{ON_5}{OP_5}) =$

$= 2\frac{ON_3 - ON_5}{OA} = 2\frac{OE + EN_3 - EN_5 + OE}{OA} = 4\frac{OE}{OA} = \frac{4OE}{4OI} = \frac{OE}{OI} = tan\varphi$.

Από τον κύκλο με διάμετρο AF έχουμε $OK^2 = OF \cdot OA \Rightarrow \frac{OK}{OA} = \frac{OF}{OK}$ $\quad (**)$

Από τον κύκλο με διάμετρο N_3N_5 έχουμε $OK^2 = N_5O \cdot N_3O$ $\quad (***)$

Τότε $4cosA\hat{O}P_3 \cdot cosA\hat{O}P_5 = -4\frac{ON_3}{OA}\frac{ON_5}{OA} = -4\frac{OK^2}{OA^2}$ (από τη σχέση $(***)$)
$= -4\frac{OF}{OA}$ (από τη σχέση $(**)$)
$= -4\frac{OF}{4OI} = -\frac{OF}{OI} = tan(\varphi - \frac{\pi}{4})$
Δείξαμε λοιπόν ότι

$$2(cosA\hat{O}P_3 + cosA\hat{O}P_5) = tan\varphi$$

$$4cosA\hat{O}P_3 \cdot cosA\hat{O}P_5 = tan(\varphi - \frac{\pi}{4})$$

Άρα τα $2cosA\hat{O}P_3$ και $2cosA\hat{O}P_5$ είναι ρίζες της εξίσωσης $t^2 - tan\varphi \cdot t + tan(\varphi - \frac{\pi}{4})$ με $cosA\hat{O}P_5 < cosA\hat{O}P_3$.

Όμως από την $(*)$ έχουμε τα $2cos3\theta$ και $2cos5\theta$ σαν ρίζες της εξίσωσης, άρα θα πρέπει

$$2cosA\hat{O}P_3 = 2cos3\theta \quad και \quad 2cosA\hat{O}P_5 = 2cos5\theta$$

Επειδή λόγω κατασκευής των $A\hat{O}P_3$ και $A\hat{O}P_5$ είναι μικρότερες από π όπως και οι 3θ και 5θ, θα έχουμε $A\hat{O}P_3 = 3\theta$ και $A\hat{O}P_5 = 5\theta$

Έπεται λοιπόν ότι τα A, P_3, P_5 είναι η μηδενική, η τρίτη και πέμπτη κορυφή του κανονικού 17-γώνου στον κύκλο με ακτίνα ΟΑ. Τώρα είναι εύκολο να κατασκευάσουμε το κανονικό 17-γωνο που είναι εγγεγραμμένο στον τυχαίο κύκλο ακτίνας ΟΑ. Έστω P_1 το σημείο τομής του τυχαίου κύκλου με τον κύκλο κέντρου P_3 και ακτίνας P_5 που βρίσκεται ανάμεσα στα Α και P_3, τότε το P_1 είναι η πρώτη κορυφή του κανονικού 17-γώνου και η AP_1 η πλευρά του.

1.6 Κύκλοι Carlyle και κατασκευές κανονικών πολυγώνων

Ο Gauss με τη θεωρία των f-περιόδων έδειξε ότι λύνοντας διαδοχικά εξισώσεις δευτέρου βαθμού οδηγούμαστε σε μια έκφραση με ριζικά του $cos\frac{2\pi}{p}$, άρα μπορούμε να το κατασκευάσουμε και στη συνέχεια να κατασκευάσουμε το κανονικό p-γωνο (όπου p πρώτος του Fermat).

Το πρόβλημα είναι κατά πόσο, για παράδειγμα στην περίπτωση του κανονικού 17-γώνου, είναι εύκολο να κατασκευαστεί το μήκος

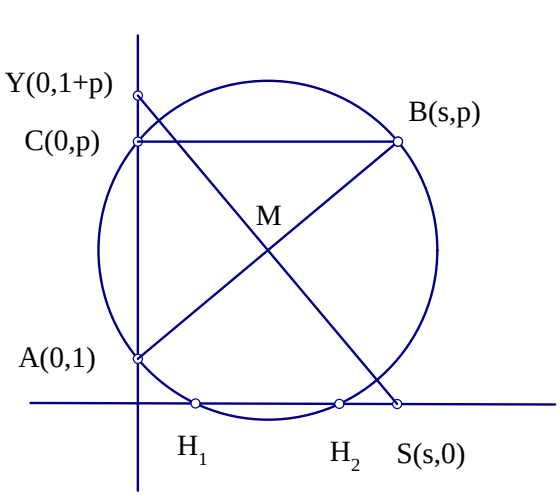
$$-\frac{1}{16}+\frac{1}{16}\sqrt{17}+\frac{1}{16}\sqrt{34-2\sqrt{17}}+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34+2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

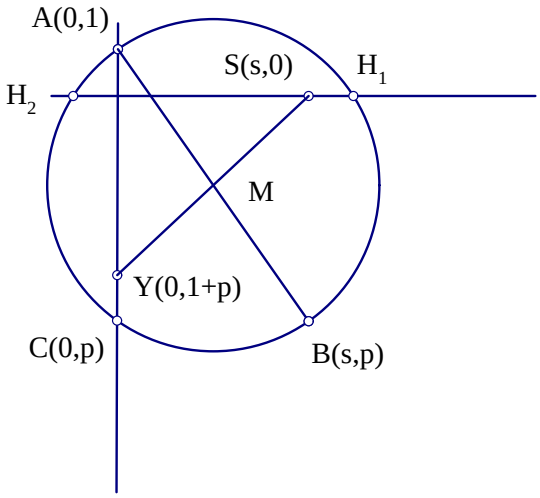
Το πρόβλημα αυτό λύνεται κατασκευάζοντας γεωμετρικά τις ρίζες τριωνύμων με τη βοήθεια των κύκλων Carlyle. Ο Thomas Carlyle (1795-1881) ήταν Σκωτσέζος ιστορικός, ο οποίος πριν ασχοληθεί με τη φιλολογία μελέτησε μαθηματικά, μετέφρασε το Elements de Geometrie του Legendre στα αγγλικά και επινόησε μία όμορφη γεωμετρική κατασκευή των ριζών δευτεροβάθμιων πολυωνύμων.

Υπάρχει ποικιλία μεθόδων κατασκευής των ριζών τριωνύμων, αλλά αυτή του Carlyle είναι ιδιαίτερα ελκυστική. Η μέθοδος αυτή που θα αναπτύξουμε παρακάτω εμφανίστηκε στο Elements of Geometry του Leslie με τη σημείωση " η λύση σε συτό το σημαντικό πρόβλημα που θα εισάγουμε στο κείμενο, προτάθηκε σε εμένα από τον κ. Thomas Carlyle, έναν ευφυή νεαρό μαθηματικό και παλαιότερα μαθητή μου".

Έστω λοιπόν ότι έχουμε ένα ορθοκανονικό σύστημα αξόνων και θέλουμε να κατασκευάσουμε τις ρίζες της δευτεροβάθμιας εξίσωσης $x^2-sx+p=0$, όπου s και p είναι δοσμένα μήκη. Θεωρούμε τώρα τα σημεία $A(0,1)$ και $B(s,p)$. Ο κύκλος με διάμετρο το ευθύγραμμο τμήμα AB λέγεται κύκλος Carlyle $C_{s,p}$ της δοθείσας εξίσωσης. Το κέντρο του $C_{s,p}$ είναι το μέσο του AB, δηλαδή το σημείο $M(\frac{s}{2},\frac{1+p}{2})$. Θα βρούμε χρήσιμη την παρατήρηση ότι το M είναι επίσης το μέσο του ευθυγράμμου τμήματος που ορίζεται από τα σημεία $S(s,0)$ και $Y(0,1+p)$.

Αν υποθέσουμε ότι ο $C_{s,p}$ τέμνει τον χ-άξονα στα σημεία $H_1(x_1,0)$ και $H_2(x_2,0)$ με $x_1\geq x_2$ έχουμε δυο περιπτώσεις, όπως φαίνεται και στο σχήμα.





Σε κάθε περίπτωση έχουμε $OH_1 \cdot OH_2 = OA \cdot OC$, δηλαδή $x_1 \cdot x_2 = 1 \cdot p$, δηλαδή

$$x_1 \cdot x_2 = p.$$

Επίσης η εξίσωση του κύκλου είναι $(x - \frac{s}{2})^2 + (y - \frac{p+1}{2})^2 = r^2$.

Επομένως $(x_1 - \frac{s}{2})^2 + (\frac{p+1}{2})^2 = r^2$ και $(x_2 - \frac{s}{2})^2 + (\frac{p+1}{2})^2 = r^2$,

άρα

$$(x_1 - \frac{s}{2})^2 = (x_2 - \frac{s}{2})^2$$

$$x_1^2 - sx_1 + \frac{s^2}{4} = x_2^2 - sx_2 + \frac{s^2}{4}$$

$$x_1^2 - x_2^2 - sx_1 + sx_2 = 0$$

$$(x_1 - x_2)(x_1 + x_2) + s(-x_1 + x_2) = 0$$

$$(x_1 - x_2)(x_1 + x_2 - s) = 0$$

Άρα $x_1 = x_2$ ή $x_1 + x_2 = s$. Αν $x_1 = x_2 = x$ και θέσουμε $H = H_1 = H_2$ το σημείο $(x, 0)$, βλέπουμε ότι τα H, M έχουν την ίδια τετμημένη, άρα $x = \frac{s}{2}$. Σε κάθε περίπτωση λοιπόν θα έχουμε

$$x_1 + x_2 = s.$$

Είδαμε ότι $x_1 + x_2 = s$ και $x_1 \cdot x_2 = p$, άρα τα x_1, x_2 είναι ρίζες της εξίσωσης $x^2 - sx + p = 0$ και καταλήγουμε στο ακόλουθο θεώρημα:

Θεώρημα 1.6.1:

Αν ο κύκλος Carlyle $C_{s,p}$ τέμνει τον x-άξονα στα x_1 και x_2, τότε τα x_1 και x_2 είναι οι ρίζες του πολυωνύμου $x^2 - sx + p$.

Πρέπει εδώ να σημειώσουμε ότι αν οι ρίζες του πολυωνύμου είναι μιγαδικοί αριθμοί τότε και αυτοί μπορούν να εκφραστούν μέσω των Carlyle κύκλων.

Ας υποθέσουμε ότι η τεταγμένη $\frac{p+1}{2}$ του κέντρου του $C_{s,p}$ είναι μεγαλύτερη από την ακτίνα $r = [(\frac{s}{2})^2 + (\frac{1-p}{2})^2]^{\frac{1}{2}}$, τότε $(\frac{1+p}{2})^2 > (\frac{s}{2})^2 + (\frac{1-p}{2})^2$, δηλαδή $4p > s^2$.

Έπεται ότι η διακρίνουσα Δ=$s^2 - 4p$ του πολυωνύμου είναι αρνητική, η εξίσωση δεν έχει πραγματικές ρίζες και ο κύκλος $C_{s,p}$ δεν τέμνει τον x-άξονα. Οι μιγαδικές ρίζες του πολυωνύμου θα είναι οι

$$z_1 = \frac{s}{2} + \frac{1}{2}i\sqrt{\Delta} \ \ \kappa\alpha\iota \ \ z_2 = \frac{s}{2} - \frac{1}{2}i\sqrt{\Delta}$$

Θα δείξουμε ότι κάθε κύκλος με κέντρο στον x-άξονα που είναι ορθογώνιος στον $C_{s,p}$ τέμνει την κάθετο που διέρχεται από το κέντρο του $C_{s,p}$ στα σημεία

$$(\frac{s}{2}, \frac{1}{2}\sqrt{-\Delta}) \ \ \kappa\alpha\iota \ \ (\frac{s}{2}, -\frac{1}{2}\sqrt{-\Delta})$$

Ας θεωρήσουμε τον κύκλο κέντρου $M'(\xi, 0)$ ο οποίος είναι ορθογώνιος με τον $C_{s,p}$. Η εξίσωση του είναι $(x - \xi)^2 + y^2 = r'^2$.

Για να είναι οι δυο κύκλοι ορθογώνιοι θα πρέπει

$$r'^2 + r^2 = MM'$$

(Η ικανή και αναγκαία συνθήκη για να είναι δύο κύκλοι (Ο,R) και (Ο′,R') ορθογώνιοι είναι $R^2 + R'^2 = OO'^2$.

Ικανή

Έστω Α το σημείο τομής των δύο κύκλων, αφού οι κύκλοι τέμνονται ορθογώνια θα ισχύει $O\hat{A}O' =$ορθή και συνεπώς $R^2 + R'^2 = OO'^2$.

Αναγκαία

Έστω $R^2 + R'^2 = OO'^2$, τότε $(R - R')^2 < OO' < (R + R')^2$ (για $a, b > 0$ ισχύει $(a - b)^2 < a^2 + b^2 < (a + b)^2$) και τότε $|R - R'| < OO' < R + R'$, δηλαδή οι δύο κύκλοι τέμνονται και αν θεωρήσουμε Α το σημείο τομής τους το τρίγωνο ΟΑΟ′, από αντίστροφο του πυθαγορείου θεωρήματος, θα πρέπει να είναι ορθογώνιο, άρα οι δύο κύκλοι τέμνονται ορθογώνια).

Δηλαδή $r'^2 = (\frac{s}{2} - \xi)^2 + (\frac{1+p}{2})^2 - r^2$ και η εξίσωση του κύκλου (M', r') γίνεται

$$(x - \xi)^2 + y^2 = (\frac{s}{2} - \xi)^2 + (\frac{1+p}{2})^2 - r^2,$$

τότε θέτοντας $x = \frac{s}{2}$ βρίσκουμε

$$y^2 = (\frac{1+p}{2})^2 - r^2 = -\frac{1}{4}\Delta$$

Έτσι κάθε τέτοιος, ορθογώνιος με τον $C_{s,p}$ κύκλος μπορεί να χρησιμοποιηθεί για την κατασκευή των z_1, z_2 με τον y-άξονα να αντιπροσωπεύει τον φανταστικό άξονα του μιγαδικού επιπέδου.

Κατασκευή κανονικού πενταγώνου

Αρχικά κατασκευάζουμε τους x,y-άξονες και το μοναδιαίο κύκλο. Ακολουθώντας τον Gauss θα κατασκευάσουμε το κανονικό πεντάγωνο κατασκευάζοντας τις ρίζες της εξίσωσης $z^5 - 1 = 0$. Η ρίζα $z_0 = 1$ αντιπροσωπεύει το σημείο $P_0(1, 0)$ και οι υπόλοιπες ρίζες, οι ρίζες δηλαδή της εξίσωσης $z^4 + z^3 + z^2 + z + 1 = 0$, αντιπροσωπεύονται από τα σημεία P_1, P_2, P_3, P_4.

Έστω $\varepsilon = e^{\frac{2\pi i}{5}}$, πρωταρχική 5-ρίζα της μονάδας, τότε οι ρίζες θα είναι $\varepsilon^1, \varepsilon^2, \varepsilon^3, \varepsilon^4$ οι οποίες έχουν άθροισμα -1 (σαν ρίζες της εξίσωσης $z^4 + z^3 + z^2 + z + 1 = 0$).

Θέτουμε

$$\eta_0 = \varepsilon^1 + \varepsilon^4 = 2cos\frac{2\pi}{5}$$

$$\eta_1 = \varepsilon^2 + \varepsilon^3 = 2cos\frac{4\pi}{5}$$

(από τη σχέση $\varepsilon^k + \varepsilon^{5-k} = 2cos\frac{2k\pi}{5},\ k = 0, 1, 2, 3, 4.$)

Τότε $\eta_0 + \eta_1 = \varepsilon^1 + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1$

και $\eta_0 \cdot \eta_1 = (\varepsilon^1 + \varepsilon^4)(\varepsilon^2 + \varepsilon^3) = \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 = \varepsilon^3 + \varepsilon^4 + \varepsilon^1 + \varepsilon^2 = -1$

με $\eta_0 > 0 > \eta_1$.

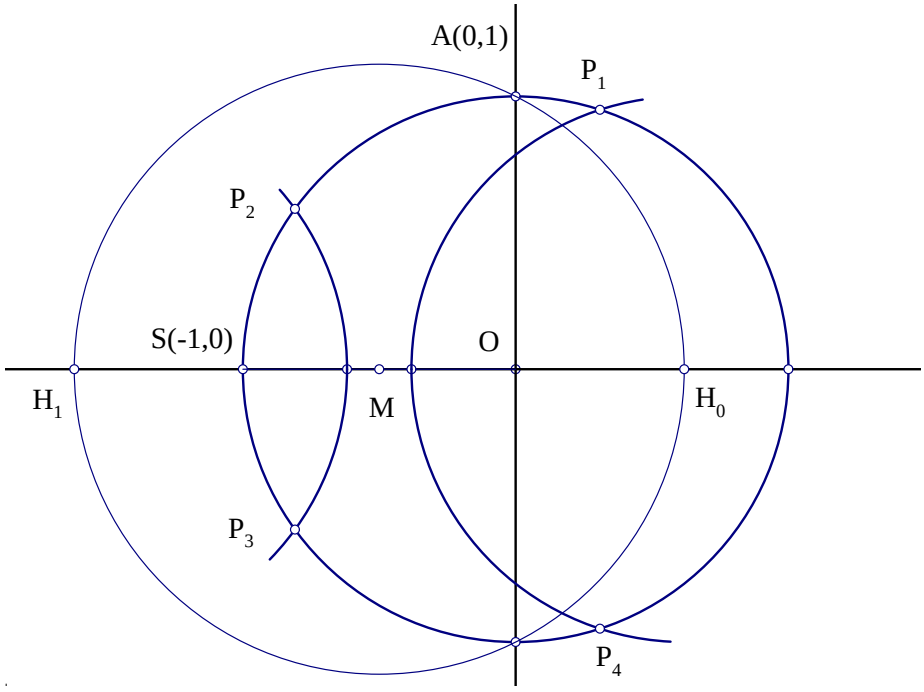
Άρα τα η_0, η_1 είναι ρίζες του πολυωνύμου $x^2 + x - 1$, με $\eta_0 > \eta_1$ και άρα μπορούν να κατασκευαστούν με τη βοήθεια του κύκλου $Carlyle\ C_{-1,-1}$, κέντρου $M(-\frac{1}{2}, 0)$.

Είδαμε ότι το Μ είναι το μέσο των σημείων $S(s,0)$ και $Y(0,p+1)$, δηλαδή των $S(-1,0)$ και Y είναι το κέντρο των αξόνων $O(0,0)$.

Έτσι κατασκευάζουμε το Μ ως μέσο του ευθυγράμμου τμήματος OS και φέρνουμε τον κύκλο κέντρου Μ και ακτίνας MA, με Α(1,0), οπότε τα σημεία τομής του κύκλου με τον x-άξονα θα είναι τα $H_0(\eta_0,0)$ και $H_1(\eta_1,0)$.

Επομένως οι κύκλοι με μοναδιαία ακτίνα και κέντρα τα H_0 και H_1 θα τέμνουν το μοναδιαίο κύκλο στα P_1,P_2,P_3,P_4.

(Το τρίγωνο OP_1H_0 είναι ισοσκελές, $OP_1=P_1H_0=1$, άρα η τετμημένη του P_1 θα είναι $\frac{\eta_0}{2}=cos\frac{2\pi}{5}$ και αφού το P_1 είναι σημείο του μοναδιαίου κύκλου θα έχει τεταγμένη $sin\frac{2\pi}{5}$, άρα το P_1 είναι η ζητούμενη ρίζα. Ομοίως και για τα υπόλοιπα).



Κατασκευή κανονικού δεκαεπταγώνου

Έστω $\varepsilon=e^{\frac{2\pi i}{17}}$, θα κατασκευάσουμε τις ρίζες $\varepsilon^1,\varepsilon^2,...,\varepsilon^{16}$ της εξίσωσης $z^{16}+z^{15}+...+z+1=0$. Η ιδέα του Gauss ήταν να βρει έναν γεννήτορα $g \pmod{17}$ της κυκλικής ομάδας $\mathbb{Z}_{17}^*=\{1,2,...,16\}$, τότε οι ρίζες της εξίσωσης γράφονται:

$$\varepsilon^1,\varepsilon^g,\varepsilon^{g^2},...,\varepsilon^{g^{15}},\varepsilon^{g^{16}}=\varepsilon^1.$$

Το g είναι γεννήτορας της $\mathbb{Z}_{17}^*$, άρα $g^{16} \equiv 1 \pmod{17}$ και $g^r \not\equiv 1 \pmod{17}$, για $1 \leq r \leq 15$, επίσης $\varepsilon^m = \varepsilon^{m \pmod{17}}$.

Το 3 είναι γεννήτορας της $\mathbb{Z}_{17}^*$, επομένως οι ρίζες θα γράφονται:

$$\varepsilon^1, \varepsilon^3, \varepsilon^9, \varepsilon^{10}, \varepsilon^{13}, \varepsilon^5, \varepsilon^{15}, \varepsilon^{11}, \varepsilon^{16}, \varepsilon^{14}, \varepsilon^8, \varepsilon^7, \varepsilon^4, \varepsilon^{12}, \varepsilon^2, \varepsilon^6.$$

Στη συνέχεια όπως είδαμε ο Gauss θεώρησε περιοδικά αθροίσματα των παραπάνω όρων τα οποία ονόμασε περιόδους.

Έτσι κάθε περίοδος αντιπροσωπεύεται από τους αντίστοιχους εκθέτες. Για παράδειγμα η περίοδος

$$\eta_{0,2} = \varepsilon^1 + \varepsilon^9 + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon^8 + \varepsilon^4 + \varepsilon^2$$

θα γράφεται $\eta_{0,2} = (1, 9, 13, 15, 16, 8, 4, 2)$.

Έχουμε τις παρακάτω περιόδους, οι οποίες θα μας χρειαστούν για την κατασκευή:

$$\eta_{0,2} = (1, 9, 13, 15, 16, 8, 4, 2)$$

$$\eta_{1,2} = (3, 10, 5, 11, 14, 7, 12, 6)$$

$$\eta_{0,4} = (1, 13, 16, 4),\ \eta_{2,4} = (9, 15, 8, 2)$$

$$\eta_{1,4} = (3, 5, 14, 12),\ \eta_{3,4} = (10, 11, 7, 6)$$

και $\eta_{0,8} = (1, 16) = \varepsilon^1 + \varepsilon^{16} = 2cos\frac{2\pi}{17},\ \ \eta_{4,8} = (13, 4) = \varepsilon^{13} + \varepsilon^4 = 2cos\frac{8\pi}{17}$ (1)

Εύκολα βρίσκουμε ότι (τα αποτελέσματα αυτά έχουν βρεθεί και στο κεφάλαιο κατασκευής του κανονικού 17-γώνου με τη μέθοδο του Gauss):

$$\eta_{0,8} + \eta_{4,8} = \eta_{0,4},\ \eta_{0,8} \cdot \eta_{4,8} = \eta_{1,4},\ \eta_{0,8} > \eta_{4,8} \qquad (2)$$

$$\eta_{0,4} + \eta_{2,4} = \eta_{0,2},\ \eta_{0,4} \cdot \eta_{2,4} = -1,\ \eta_{0,4} > \eta_{2,4} \qquad (3)$$

$$\eta_{1,4} + \eta_{3,4} = \eta_{1,2},\ \eta_{1,4} \cdot \eta_{3,4} = -1,\ \eta_{1,4} > \eta_{3,4} \qquad (4)$$

$$\eta_{0,2} + \eta_{1,2} = -1,\ \eta_{0,2} \cdot \eta_{1,2} = -4,\ \eta_{0,2} > \eta_{1,2} \qquad (5)$$

(Οι παραπάνω ανισώσεις προκύπτουν με τον αλγεβρικό υπολογισμό των περιόδων).

Τώρα οι εξισώσεις (1)-(5) θα μας οδηγήσουν στην κατασκευή του κανονικού 17-γώνου.

Θεωρούμε τους x,y-άξονες και το μοναδιαίο κύκλο. Από τη σχέση (5) βλέπουμε ότι τα $\eta_{0,2}$ και $\eta_{1,2}$ είναι ρίζες της $x^2 + x - 4 = 0$ με $\eta_{0,2} > \eta_{1,2}$, τις οποίες θα υπολογίσουμε γεωμετρικά με τη βοήθεια του κύκλου Carlyle $C_{-1,-4}$, κέντρου $M_0(-\frac{1}{2}, -\frac{3}{2})$. Έτσι:

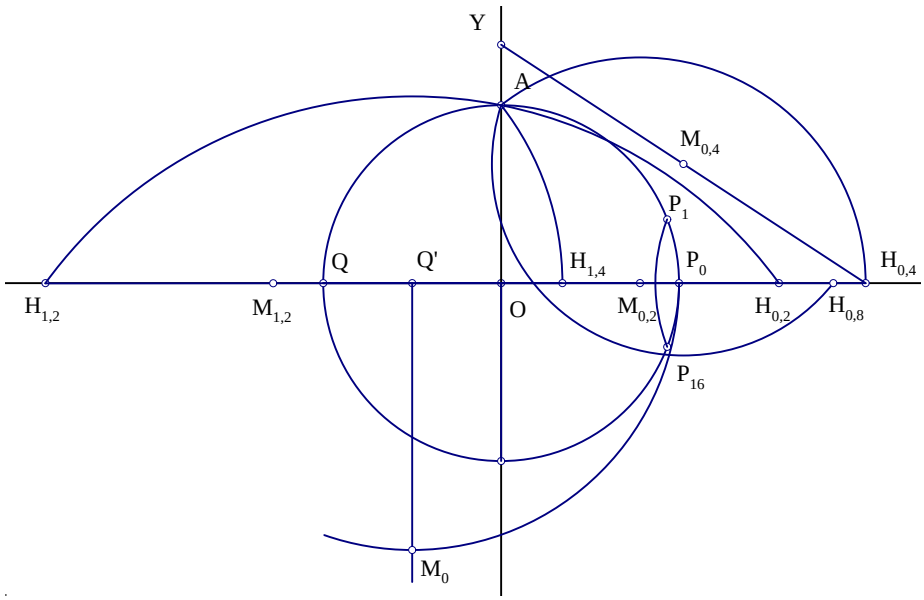
$i)$ Στα δυο πρώτα βήματα θα κατασκευάσουμε το M_0.

Έχουμε $Q = (s, 0) = (-1, 0)$ και $O(0, 0)$. Βρίσκουμε το μέσο του QO, έστω $Q'(-\frac{1}{2}, 0)$ και φέρνουμε τη μεσοκάθετο όπως στο σχήμα. Φέρνουμε

$ii)$ κύκλο κέντρου $Q'(-\frac{1}{2}, 0)$ και ακτίνας $Q'P_0,\ P_0(1, 0)$, το σημείο τομής του κύκλου με τη μεσοκάθετο είναι το $M_0(-\frac{1}{2}, -\frac{3}{2})$.

(Το M_0 βρίσκεται στη μεσοκάθετο άρα έχει τετμημένη $-\frac{1}{2}$ και $|Q'M| = |Q'P_0| = \frac{3}{2}$, άρα έχει τεταγμένη $-\frac{3}{2}$).

$iii)$ τον κύκλο Carlyle κέντρου M_0 και ακτίνας M_0A, όπου $A(0, 1)$, (με $|M_0A| = \sqrt{\frac{26}{4}}$) και βρίσκουμε τα $H_{0,2}(\eta_{0,2}, 0)$ και $H_{1,2}(\eta_{1,2}, 0)$.



Από τις ισότητες (3) και (4) βλέπουμε ότι οι κύκλοι Carlyle με κέντρα τα σημεία $M_{0,2}(\frac{1}{2}\eta_{0,2}, 0)$ και $M_{1,2}(\frac{1}{2}\eta_{1,2}, 0)$ θα μας δώσουν τα $H_{0,4}(\eta_{0,4}, 0)$ και $H_{1,4}(\eta_{1,4}, 0)$.

Φέρνουμε

$iv)$ τις μεσοκαθέτους των $OH_{0,2}$ και $OH_{1,2}$ και βρίσκουμε τα μέσα $M_{0,2}(\frac{\eta_{0,2}}{2}, 0)$ και $M_{1,2}(\frac{\eta_{1,2}}{2}, 0)$.

$v)$ τους κύκλους Carlyle κέντρων $M_{0,2}$ και $M_{1,2}$ και βρίσκουμε τα σημεία $H_{0,4}$ και $H_{1,4}$.

Από την (2) έχουμε ότι το $H_{0,8}(\eta_{0,8}, 0)$ είναι το σημείο τομής του κύκλου Carlyle με κέντρο $M_{0,4}(\frac{\eta_{0,4}}{2}, \frac{\eta_{1,4}+1}{2})$ και του x-άξονα, (αφού οι $\eta_{0,8}$ και $\eta_{4,8}$ είναι ρίζες του $x^2 - \eta_{0,4}x + \eta_{1,4}$).

$vi)$ κύκλο κέντρου Ο και ακτίνας $QH_{1,4} = ||(\eta_{1,4}+1, 0)|| = \eta_{1,4}+1$ και βρίσκουμε το σημείο $Y(0, 1 + \eta_{1,4})$.

$vii)$ Φέρνουμε το ευθύγραμμο τμήμα $YH_{0,4}$.

$viii)$ Βρίσκουμε το μέσο του $YH_{0,4}$, το οποίο είναι το $M_{0,4}$.

$ix)$ Φέρνουμε τον κύκλο Carlyle κέντρου $M_{0,4}$ και βρίσκουμε το σημείο $H_{0,8}$.

Έχουμε δηλαδή το μήκος $\eta_{0,8} = 2cos\frac{2\pi}{17}$.

Τέλος γράφουμε κύκλο κέντρου $H_{0,8}$ και ακτίνας 1, τα σημεία τομής του με τον μοναδιαίο κύκλο θα έχουν τετμημένη $\frac{\eta_{0,8}-0}{2} = cos\frac{2\pi}{17}$ και αφού ανήκουν στο μοναδιαίο είναι οι κορυφές P_1 και P_{16} του κανονικού 17-γώνου. Τότε η P_0P_1 είναι η πλευρά του κανονικού 17-γώνου και η κατασκευή τελείωσε.

Η κατασκευή του κανονικού 257-γώνου από τον Richelot (δείτε [17]) είναι αλγεβρική και στηρίζεται στη μέθοδο που χρησιμοποίησε και ο Gauss για την κατασκευή του κανονικού 17-γώνου. Ο De Temple αναφέρει (δείτε [5]) ότι για τη γεωμετρική κατασκευή του κανονικού 257-γωνου χρειάστηκε 150 κύκλους, από τους οποίους οι 24 ήταν κύκλοι Carlyle, ενώ για την κατασκευή του 65537-γωνου προβλέπει ότι χρειάζονται 1332 ή λιγότεροι κύκλοι Carlyle.

Κεφάλαιο 2

Ο τετραγωνικός νόμος αντιστροφής

2.1 Εισαγωγή

Η εισαγωγή που ακολουθεί αποτελεί μέρος του υπό έκδοση βιβλίου του κ. Γιάννη Α. Αντωνιάδη (δείτε [23]).

Ο πρώτος που ξεκίνησε τη μελέτη των νόμων αντιστροφής ήταν ο Fermat. Σε κάποιο γράμμα του στον Mersenne διατύπωσε την πρόταση:

"*Tout nombre premier, qui surprasse de l'unité un multiple du quaternaire est une seule fois la somme de deux carrés*"

(Κάθε πρώτος ο οποίος είναι κατά ένα μεγαλύτερος πολλαπλάσιου του τέσσερα είναι κατά μοναδικό τρόπο άθροισμα δύο τετραγώνων).

Το πρώτο θεώρημα του Euler που σχετίζεται με τον τετραγωνικό νόμο αντιστροφής ήταν το ομώνυμο κριτήριο. Η απόδειξη που θα δώσουμε στο επόμενο κεφάλαιο οφείλεται στον Dirichlet.

Ο Euler διατύπωσε ένα θεώρημα το οποίο είναι ισοδύναμο με το νόμο τετραγωνικής αντιστροφής, στα 1744. Αυτό βέβαια έγινε γνωστό πολύ αργότερα από το άρθρο του Kronecker "*Bemerkunger zur Geschichte des quadratischen Reciprocitätsgetzes*", Berl. Monatsber (1872) 846-848.

Μια ειδική περίπτωση του νόμου τετραγωνικής αντιστροφής είχε ανακοινωθεί από τον Euler με γράμμα του προς τον Goldbach ήδη στα 1742.

Ο Lagrange κατά τη διετία 1773-75 βρισκόταν στο Βερολίνο. Παρακινούμενος από τον Euler (που είχε επιστρέψει στην Αγία Πετρούπολη), ασχολείται και με την Θεωρία Αριθμών. Την περίοδο αυτή ανακαλύπτει πλήρως τον τετραγωνικό νόμο αντι-

στροφής, δεν καταφέρνει όμως να τον αποδείξει. Η εργασία του αυτή δημοσιεύθηκε, μετά το θάνατο του, στα 1783.

Ο A. M. Legendre ήταν ο πρώτος που δημοσίευσε, στα 1788 (η εργασία παρουσιάστηκε στην Ακαδημία του Παρισιού στα 1785), τον τετραγωνικό νόμο αντιστροφής σε μορφή πολύ κοντινή στη σημερινή του έκφραση.

Στα 1788 ανακοίνωσε τον τετραγωνικό νόμο αντιστροφής στην τελική του μορφή, αφού πρώτα εισήγαγε το ομώνυμο σύμβολο. Για την απόδειξη διέκρινε διάφορες περιπτώσεις, μερικές από τις οποίες κατάφερε να αποδείξει πλήρως. Κάπου όμως παρουσιάστηκαν ανυπέρβλητες δυσκολίες για τον ίδιο και διαπίστωσε ότι χρειάζεται μια βοηθητική πρόταση, για την ορθότητα της οποίας ήταν σίγουρος, αλλά που δεν κατάφερε να αποδείξει. Η εικασία του Legendre δεν ήταν τίποτα άλλο από το θεώρημα του Dirichlet για αριθμητικές προόδους!

Τα αποτελέσματά του περιέχονται στις διάφορες εκδόσεις του βιβλίου του

Essai sur la theorie des nombres

Παρίσι 1798,1808,1830 και 1955.

Τελικά κατάφερε να περιοριστεί σε μία μόνο, αναπόδεικτη τότε υπόθεση (αν p πρώτος, $p \equiv 1 \pmod 4$, τότε υπάρχει ένας τουλάχιστον πρώτος $q \equiv 3 \pmod 4$ τ.ω. $(\frac{p}{q}) = -1$) αλλά παρά τις προσπάθειες του, δεν κατάφερε ποτέ να αποδείξει πλήρως τον τετραγωνικό νόμο αντιστροφής.

Ο πρώτος που απέδειξε πλήρως τον τετραγωνικό νόμο αντιστροφής ήταν ο δεκαοχτάχρονος Gauss. Η απόδειξη περιέχεται στο έργο του Disquisitiones Arithmeticae προτάσεις (Αρθρα) 131-144. Όπως αναφέρει ο ίδιος,

"το θεώρημα αυτό ταλαιπωρούσε για ένα ολόκληρο χρόνο τη σκέψη μου και αντιστεκόταν στις επίμονες προσπάθειες μου, μέχρι που κατάφερα να δώσω την απόδειξη που περιέχεται στο τέταρτο μέρος του έργου μου".

Μάλιστα όπως μας βεβαιώνει ο ίδιος δεν είχε ιδέα από τα επιμέρους αποτελέσματα των Euler και Legendre.

Πως κατάφερε ο Gauss να διατυπώσει και να αποδείξει πλήρως τον τετραγωνικό νόμο αντιστροφής;

Με επιδεξιότητα και αντοχή κατασκεύασε έναν πίνακα στον οποίο υπολόγιζε ποιοί από τους πρώτους, τους μικρότερους του 1000 είναι τετραγωνικά υπόλοιπα και ποιοί όχι, ως προς τους πρώτους από το 3 μέχρι το 503. Έπρεπε να εξετάσει 16000 περιπτώσεις αν είναι τετραγωνικά υπόλοιπα ή όχι.

Στην απόδειξη και ο ίδιος είχε τις δυσκολίες του. Η πρώτη του απόδειξη έμοιαζε με αυτή του Legendre. Χρειάστηκε και ο ίδιος έναν "βοηθητικό πρώτο" και όταν το

βρήκε το ημερολόγιο έγραφε

$$8\ \mathbf{A}\pi\rho\iota\lambda\acute{\iota}ου\ του\ 1796$$

Ο Legendre ονόμασε το θεώρημα "Loi le reciprocite" (Νόμο αντιστροφής). Ο Gauss, "Theorema fundamentale theorie residuorum quadraticorum" (Θεμελιώδες θεώρημα της θεωρίας των τετραγωνικών υπολοίπων) και το κατέταξε στις " ύψιστες αλήθειες της ανώτερης αριθμητικής " ("*Zu den höchsten Wahrheiten der höheren Arithmetik zu rechnen ist*").

Η πρώτη απόδειξη του Gauss δεν θεωρήθηκε ιδιαίτερα κομψή, ο Άγγλος αριθμοθεωρητικός Henry John Stephen Smith αναφέρει ότι "παρουσιάστηκε από τον Gauss σε απρόσιτη μορφή για τον οποιοδήποτε, εκτός από τους πιο επίμονους μαθητές του". Χρησιμοποίησε διπλή επαγωγή. Εκτός από το Disquisitiones Arithmeticae η απόδειξη σε μοντέρνα μορφή περιέχεται και στο βιβλίο Θεωρίας Αριθμών του B. A. Venkov (δείτε [21])

Πάρα πολύ σύντομα, στις 27 Ιουνίου του 1796, ακολούθησε η δεύτερη απόδειξη του Gauss. Σε αυτήν χρησιμοποιεί τη θεωρία των τετραγωνικών μορφών. Ακολούθησαν από τον ίδιο άλλες έξι, συνολικά οκτώ αποδείξεις.

Η πρώτη απόδειξη που θα ακολουθήσει στηρίζεται στο κριτήριο του Euler και το λήμμα του Gauss, το οποίο αποδείχθηκε στα 1807 και αποτελούσε μέρος της τρίτης απόδειξης του τετραγωνικού νόμου αντιστροφής που έδωσε ο ίδιος. Τέλος το τελικό βήμα της απόδειξης είναι του Eisenstein (1844), μαθητή του Gauss.

Εδώ για πρώτη φορά χρησιμοποιούνται γεωμετρικές μέθοδοι, μετρούμε δηλαδή τα ακέραια σημεία ενός ορθογωνίου παραλληλογράμου κατά δύο διαφορετικούς τρόπους. Η κατεύθυνση αυτή αναπτύχθηκε από τον Minkowski και ονομάστηκε Γεωμετρία των Αριθμών. Πρόδρομός της λοιπόν μπορεί να θεωρηθεί ο Eisenstein.

Συνολικά έχουν δοθεί μέχρι σήμερα περισσότερες από 200 αποδείξεις. Βέβαια αρκετές από αυτές παρουσιάζουν αρκετές ομοιότητες μεταξύ τους.

Στα 1963, ο M. Gesterhaber δημοσίευσε την 152η απόδειξη του τετραγωνικού νόμου αντιστροφής (American Mathematical Monthly 70(1963),397-398).

Είχε μετρήσει όλες τις προηγούμενες;

Η απάνηση που έδωσε ήταν πως όχι! Ακολούθησε την πρόταση του A. Weil σε ένα σεμινάριο του Institute for Advanced Studies του Princeton, ο οποίος του είπε ότι γνωρίζει 50 αποδείξεις και για κάθε μία υπάρχουν άλλες δύο που δεν τις γνωρίζει, έτσι συμπέρανε ότι ήταν 150. Στη συνέχεια επέστησε την προσοχή του στην εργασία του Kubota η οποία θα έπρεπε να ήταν η 151η απόδειξη. Επομένως η δική του θα

πρέπει να ήταν η 152α! Σύμφωνα με τον κατάλογο του Lemmermeyer (δείτε [14]) είναι η 149η, δεν έπεσε καθόλου έξω ο A. Weil!

Το μεγάλο πλήθος των αποδείξεων του τετραγωνικού νόμου αντιστροφής (πάνω από 200), καθώς και η δυσκολία για την απόδειξη του, δείχνουν τη σημαντικότητα του. Το σημαντικό είναι ότι ο τετραγωνικός νόμος αντιστροφής απετέλεσε το κίνητρο για την εξέλιξη της θεωρίας αριθμών. Υπάρχουν μάλιστα πολλοί μαθηματικοί που υποστηρίζουν οτι η ιστορία των νόμων αντιστροφής έπαιξε πιο σημαντικό ρόλο και από την εικασία του Fermat.

Μετά από την απόδειξη του τετραγωνικού νόμου αντιστροφής ο Gauss μελέτησε και κυβικές $x^3 \equiv a \pmod{p}$ και διτετραγωνικές $x^4 \equiv a \pmod{p}$ ισοτιμίες καθώς και τον κυβικό και το διτετραγωνικό νόμο αντιστροφής, τους οποίους δεν κατάφερε να αποδείξει πλήρως, κάτι που πέτυχε αργότερα ο μαθητής του Eisenstein.

Πείστηκε οτι δεν μπορεί κανείς να ελπίζει σε εύκολα αποτελέσματα αν παραμείνει στους ακέραιους αριθμούς. Για το σκοπό του μελέτησε μιγαδικούς αριθμούς της μορφής $a + bi$ με $a, b \epsilon \mathbb{Z}$, οι οποίοι αργότερα ονομάστηκαν ακέραιοι του Gauss.

2.2 Εισαγωγικά της θεωρίας αριθμών

Θα ξεκινήσουμε το κεφάλαιο αποδεικνύοντας κάποια βασικά θεωρήματα που θα μας χρησιμεύσουν στη συνέχεια.

Θεώρημα 2.2.1:

Αν $ac \equiv bc \pmod{m}$, τότε $a \equiv b \pmod{\frac{m}{d}}$ όπου $d = (c, m)$.

Απόδειξη:

Από την υπόθεση έχουμε $ac \equiv bc \pmod{m}$ άρα $ml = ac - bc = (a-b)c$. Διαιρούμε με d και βρίσκουμε $\frac{ml}{d} = \frac{(a-b)c}{d} \Rightarrow Ml = (a-b)C$, όπου $c = Cd, m = Md$ και $(C, M) = 1$. Τώρα $M \mid C(a-b)$ και $(C, M) = 1$, άρα $M \mid a - b \Rightarrow a \equiv b \pmod{M}$, δηλαδή $a \equiv b \pmod{\frac{m}{d}}$.

□

Πόρισμα 2.2.2:

Αν $ac \equiv bc \pmod{m}$ και $(c, m) = 1$, τότε $a \equiv b \pmod{m}$.

Θεώρημα 2.2.3:

Αν $\{a_1, a_2, ..., a_{\varphi(m)}\}$ είναι ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων $\pmod{m}$, τότε το ίδιο θα είναι και το $ba_1, ba_2, ..., ba_{\varphi(m)}$, όπου $(b, m) = 1$.

Σημείωση:

Η $\varphi(n)$ είναι ο αριθμός των θετικών ακεραίων $\leq n$ που είναι πρώτοι προς το n και λέγεται συνάρτηση του $Euler$. Μία κλάση αντιπροσώπων θα λέγεται πρώτη κλάση υπολοίπων $\pmod{m}$ αν και μόνο αν ένας αντιπρόσωπος της είναι πρώτος προς το m. Προφανώς υπάρχουν $\varphi(m)$ πρώτες κλάσεις υπολοίπων $\pmod{m}$.

Απόδειξη:

Το πλήθος τους είναι $\varphi(m)$. Αρκεί λοιπόν να αποδείξουμε ότι ανήκουν σε διαφορετικές κλάσεις.

Αν $ba_i \equiv ba_j \pmod{m} \Rightarrow m \mid b(a_i - a_j)$. Όμως $(b, m) = 1 \Rightarrow m \mid a_i - a_j \Rightarrow a_i \equiv a_j \pmod{m}$ και αφού a_i, a_j από το πλήρες σύστημα $\{a_1, a_2, ..., a_{\varphi(m)}\} \Rightarrow a_i = a_j$ και συνεπώς $i = j$.

□

Το παρακάτω θεώρημα λέγεται το μικρό θεώρημα του Fermat.

Θεώρημα 2.2.4:

Αν $(a, m) = 1$ τότε $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Απόδειξη:

Έστω $a_1, a_2, ..., a_{\varphi(m)}$ ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων $\pmod{m}$. Αφού $(a, m) = 1$ σύμφωνα με το θεώρημα 2.2.3 οι αριθμοί $aa_1, aa_2, ..., aa_{\varphi(m)}$ αποτελούν ένα πλήρες σύστημα αντιπροσώπων των πρώτων κλάσεων υπολοίπων $\pmod{m}$. Δηλαδή για κάθε i, με $1 \leq i \leq \varphi(m)$, υπάρχει j με $1 \leq j \leq \varphi(m)$, τέτοιο ώστε $aa_i \equiv a_j \pmod{m}$. Παίρνοντας το γινόμενο όλων των παραπάνω ισοδυναμιών βρίσκουμε

$$aa_1aa_2...aa_{\varphi(m)} \equiv a_1a_2...a_{\varphi(m)} \pmod{m}$$

$$\Rightarrow a^{\varphi(m)}a_1a_2...a_{\varphi(m)} \equiv a_1a_2...a_{\varphi(m)} \pmod{m}$$

Αφού $(a_i, m) = 1$ για κάθε $i, 1 \leq i \leq \varphi(m)$ θα έχουμε $(a_1a_2...a_{\varphi(m)}, m) = 1$ και λόγω της τελευταίας το Πόρισμα 2.2.2 δίνει $a^{\varphi(m)} \equiv 1 \pmod{m}$.

□

Θεώρημα 2.2.5:

Η ισοδυναμία $ax \equiv b \pmod{m}$ έχει λύση ακριβώς τότε όταν $d = (a, m) \mid b$. Αν έχει λύση τότε το πλήθος των λύσεων είναι ακριβώς d.

Απόδειξη:

$(\Leftarrow)$

Έστω $d \mid b$ τότε $b = kd$, για κάποιο $k \epsilon \mathbb{Z}$. Όμως $d = (a, m) \Rightarrow d = ar + ms$, $r, s \epsilon \mathbb{Z} \Rightarrow b = kd = akr + mks \Rightarrow akr \equiv b \pmod{m}$, δηλαδή ο $x_0 = kr$ είναι λύση της ισοδυναμίας.

$(\Rightarrow)$

Έστω x_0 λύση της ισοδυναμίας $\Rightarrow ax_0 \equiv b \pmod{m} \Rightarrow ax_0 - b = ml, l \epsilon \mathbb{Z}$. Αφού $d \mid a$ και $d \mid m \Rightarrow d \mid b = ax_0 - ml$.

Θα δείξουμε τώρα οτι αν η ισοδυναμία έχει λύση τότε το πλήθος των λύσεων είναι ακριβώς d. Έστω x_0 μια λύση της ισοδυναμίας, για κάθε $k \epsilon \mathbb{Z}$ έχουμε $a(x_0 + \frac{km}{d}) =$

$ax_0 + km\frac{a}{d} \equiv ax_0 \equiv b \pmod{m}$, διότι $d \mid a$. Δηλαδή για κάθε $k\epsilon\mathbb{Z}$, το $x_0 + \frac{km}{d}$ είναι επίσης λύση της ισοδυναμίας. Αν πάλι x_0 και x_1 είναι λύσεις της ισοδυναμίας, τότε

$$ax_0 \equiv b \equiv ax_1 \pmod{m}$$

Από το θεώρημα 2.2.1 έχουμε $x_1 \equiv x_0 \pmod{\frac{m}{d}} \Rightarrow x_1 = x_0 + \frac{mk}{d}, d\epsilon\mathbb{Z}$. Δηλαδή αποδείξαμε οτι αν το x_0 είναι λύση της ισοδυναμίας τότε για κάθε ακέραιο κ και το $x_0 + \frac{km}{d}$ είναι λύση και οτι όλες οι λύσεις είναι της παραπάνω μορφής. Το ερώτημα που απομένει είναι πόσες από αυτές είναι διαφορετικές $\pmod{m}$.

Προφανώς οι λύσεις

$$x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, ..., x_0 + \frac{(d-1)m}{d}$$

είναι διαφορετικές, διότι αν $x_0 + \frac{km}{d} \equiv x_0 + \frac{lm}{d} \pmod{m} \Leftrightarrow \frac{(k-l}{m})d \equiv 0 \pmod{m} \Leftrightarrow m \mid \frac{(k-l}{m})d \Leftrightarrow dm \mid m(k-l) \Leftrightarrow d \mid k-l \Leftrightarrow k-l = 0$, (διότι $0 \leq |k-l| < d$) $\Leftrightarrow k = l$.

Τέλος κάθε λύση είναι ισοδύναμη με μία από τις παραπάνω. Πράγματι έστω $x_0 + \frac{km}{d}$ μια λύση, γράφουμε το $k = qd + r, 0 \leq r < d \Rightarrow x_0 + \frac{km}{d} \equiv x_0 + \frac{(qd+r)m}{d} = x_0 + qm + \frac{rm}{d} \equiv x_0 + \frac{rm}{d}$.

□

Θεώρημα 2.2.6 (Lagrange):

Αν p πρώτος και $f(x) = \sum_{i=0}^{n} a_i x^i$ πολυώνυμο βαθμού $n \geq 1$ με ακέραιους συντελεστές και $a_n \not\equiv 0 \pmod{p}$, τότε η ισοδυναμία $f(x) \equiv 0 \pmod{p}$ έχει το πολύ n λύσεις $\bmod p$.

Απόδειξη:

Για $n = 1$ έχουμε $f(x) \equiv a_1 x + a_0$, με $a_1 \not\equiv 0 \pmod{p}$ και η ισοτιμία $f(x) \equiv 0 \pmod{p}$ έχει το πολύ μία λύση, από το θεώρημα 2.2.5.

Υποθέτουμε ότι το θεώρημα είναι αληθές για όλα τα πολυώνυμα, του περιγραφόμενου τύπου, βαθμού $k \geq 1$.

Έστω τώρα ότι ένα πολυώνυμο $f(x)$ βαθμού $k+1$ έχει περισσότερες από $k+2$ λύσεις $\pmod{p}$. Έστω s μία λύση, τότε $f(x) = (x-s)q(x) + r$, όπου r ακέραιος και $q(x)$ πολυώνυμο βαθμού k με ακέραιους συντελεστές. Το $q(x)$ έχει συντελεστή της μεγαλύτερης δύναμης του x τον a_{k+1} και $a_{k+1} \not\equiv 0 \pmod{p}$.Σύμφωνα με την

υπόθεση της μαθηματικής επαγωγής το $q(x)$ έχει το πολύ k λύσεις $(\mathrm{mod}\ p)$. Ακόμη $(s-s)q(s)+r \equiv f(s) \equiv 0\ (\mathrm{mod}\ p)$.

Δηλαδή $r \equiv 0\ (\mathrm{mod}\ p)$. Άρα για κάθε x έχουμε από την παραπάνω σχέση ότι $(x-s)q(x) \equiv f(x)\ (\mathrm{mod}\ p)$. Επομένως αν t είναι κάποια άλλη λύση διαφορετική από $s\ (\mathrm{mod}\ p)$ θα ισχύει

$$(t-s)q(t) \equiv f(t) \equiv 0 \pmod{p}.$$

Αφού $t \not\equiv s\ (\mathrm{mod}\ p)$ συνεπάγεται ότι $q(t) \equiv 0\ (\mathrm{mod}\ p)$, δηλαδή το t είναι λύση και της ισοδυναμίας $q(x) \equiv 0\ (\mathrm{mod}\ p)$.

Αλλά το t διατρέχει όλες τις λύσεις της $f(x) \equiv 0\ (\mathrm{mod}\ p)$ διαφορετικές του s. Σύμφωνα με την υπόθεση υπάρχουν το λιγότερο $k+1$ τέτοιες λύσεις, το οποίο αντιφάσκει με το ότι η $q(x) \equiv 0\ (\mathrm{mod}\ p)$ έχει το πολύ k λύσεις (οι t λύσεις της $f(x)$ είναι και λύσεις της $q(x)$, όπως αποδείχθηκε παραπάνω). Άρα είναι άτοπο το ότι η $f(x)$ έχει το λιγότερο $k+2$ λύσεις.

□

Σαν πόρισμα προκύπτει το ακόλουθο.

Θεώρημα 2.2.7 (Wilson):

Αν p πρώτος τότε $(p-1)! \equiv -1\ (\mathrm{mod}\ p)$

Απόδειξη:

Έστω $f(x) = \prod_{i=1}^{p-1}(x-i) - (x^{p-1}-1) = c_{p-2}x^{p-2} + ... + c_1x + c_0$. Σύμφωνα με το θεώρημα του Fermat η ισοδυναμία $f(x) \equiv 0\ (\mathrm{mod}\ p)$ έχει $p-1$ λύσεις τις $1, 2, ..., p-1$. Είναι όμως πολυώνυμο βαθμού $p-2$, άρα σύμφωνα με το θεώρημα του Lagrange πρέπει

$$c_{p-2} \equiv c_{p-1} \equiv ... \equiv c_1 \equiv c_0 \equiv 0 \pmod{p}$$

Δηλαδή για κάθε ακέραιο x ισχύει $\prod_{i=1}^{p-1}(x-i) - (x^{p-1}-1) \equiv 0\ (\mathrm{mod}\ p) \Rightarrow$ $\prod_{i=1}^{p-1}(x-i) \equiv x^{p-1}-1\ (\mathrm{mod}\ p), \forall x \epsilon \mathbb{Z}$. Για $x = p$ προκύπτει $(p-1)! \equiv -1\ (\mathrm{mod}\ p)$.

□

2.3 Τετραγωνικά υπόλοιπα

Υποθέτουμε ότι θέλουμε να λύσουμε την (τετραγωνική) ισοδυναμία $ax^2 + bx + c \equiv o \pmod{m}$, a, b, $c \epsilon \mathbb{Z}$, $m \epsilon \mathbb{N}$, $m > 1$. Όπως και στη γενική περίπτωση ενός πολυωνύμου n βαθμού, η λύση εξαρτάται από τη λύση ισοδυναμιών της μορφής $ax^2 + bx + c \equiv o \pmod{p}$, όπου p πρώτος. Για μικρές τιμές του p ισοδυναμίες της παραπάνω μορφής μπορούν να λυθούν με τη μέθοδο της δοκιμής και της επιτυχίας. Για μεγάλο p χρειαζόμαστε οπωσδήποτε άλλη μέθοδο.

Υποθέτουμε ότι p είναι περιττός και $(a, p) = 1$. Αφού $(4, p) = 1 \Rightarrow (4a, p) = 1$. Συνεπώς οι λύσεις της $ax^2 + bx + c \equiv o \pmod{p}$ είναι ισοδύναμες προς τις λύσεις της ισοδυναμίας $4a^2x^2 + 4abx + 4ac \equiv o \pmod{p}$, δηλαδή της $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$

Η τελευταία ισοδυναμία μπορεί να λυθεί τότε και μόνο τότε όταν μπορούμε να βρούμε κάποιον ακέραιο x_0 ο οποίος να είναι λύση της ισοδυναμίας $2ax + b \equiv y_0 \pmod{p}$ και y_0 μία λύση της $y^2 \equiv b^2 - 4ac \pmod{p}$. Αφού $(2a, p) = 1$ η πρώτη από τις δύο παραπάνω ισοδυναμίες έχει πάντοτε λύση.

Βλέπουμε δηλαδή ότι το αρχικό μας πρόβλημα ανάγεται στη λύση ισοδυναμιών της μορφής $y^2 \equiv a \pmod{p}$. Αν $a \equiv 0 \pmod{p}$ τότε προφανώς η ισοδυναμία αυτή έχει λύση, $y \equiv 0 \pmod{p}$. Έστω λοιπόν ότι $a \not\equiv 0 \pmod{p}$.

Ορισμός 2.3.1:

Έστω p περιττός πρώτος και a ακέραιος τέτοιος ώστε $(a, p) = 1$. Αν η ισοδυναμία $x^2 \equiv a \pmod{p}$ έχει λύση, τότε ο a θα λέγεται τετραγωνικό υπόλοιπο $\pmod{p}$, αλλιώς θα λέγεται μη τετραγωνικό υπόλοιπο $\pmod{p}$.

Παραδείγματα:

Οι 1 και 4 είναι τετραγωνικά υπόλοιπα $\pmod{5}$.

Οι 1, 2 και 4 είναι τετραγωνικά υπόλοιπα $\pmod{7}$, το a^2 είναι τετραγωνικό υπόλοιπο $\pmod{p}$ για κάθε $p \not| a$.

Ο παρακάτω ορισμός, οφειλόμενος στον Legendre είναι πολύ χρήσιμος για τη μελέτη των τετραγωνικών υπολοίπων.

Ορισμός 2.3.2:

Έστω p περιττός πρώτος και a ακέραιος, $(a, p) = 1$. Το σύμβολο του Legendre $(\frac{a}{p})$ ορίζεται ως εξής

$$(\frac{a}{p}) = \begin{cases} 1, \text{ όταν ο } a \text{ είναι τετραγωνικό υπόλοιπο} \pmod p \\ -1, \text{ όταν ο } a \text{ δεν είναι τετραγωνικό υπόλοιπο} \pmod p \end{cases}$$

Έτσι σύμφωνα με το παραπάνω παράδειγμα ισχύει $(\frac{1}{5}) = (\frac{4}{5}) = 1$, ενώ $(\frac{2}{5}) = (\frac{3}{5}) = -1$. Ακόμη ισχύει $(\frac{a^2}{p}) = 1$ για κάθε ακέραιο a πρώτο προς τον p.

Θεώρημα 2.3.3:

Έστω p περιττός πρώτος και $(a,p) = (b,p) = 1$. Αν $a \equiv b \pmod p$, τότε $(\frac{a}{p}) = (\frac{b}{p})$.

Απόδειξη :

$(\frac{a}{p}) = 1 \Leftrightarrow$ (η $x^2 \equiv a \pmod p$ έχει λύση) $\Leftrightarrow$ (η $x^2 \equiv b \pmod p$ έχει λύση)

$\Leftrightarrow (\frac{b}{p}) = 1.$

□

Δηλαδή, το πρόβλημα για το πότε ο ακέραιος a είναι τετραγωνικό υπόλοιπο $\pmod p$, θα έχει πλήρως λυθεί αν ξέρω ποιοί από τους $1, 2, ..., p-1$ είναι τετραγωνικά υπόλοιπα $\pmod p$, ποιοί όχι και σε ποιά κλάση ισοδυναμίας του p ανήκει ο αριθμός a.

Θεώρημα 2.3.4:

Υπάρχουν ακριβώς $\frac{p-1}{2}$ μη-ισοδύναμα τετραγωνικά υπόλοιπα $\pmod p$, για κάθε περιττό πρώτο p.

Απόδειξη :

Θα πρέπει να πάρουμε όλους τους ακέραιους a τους πρώτους προς τον p για τους οποίους η ισοδυναμία $x^2 \equiv a \pmod p$ έχει λύση. Αν $x^2 \equiv a \pmod p$ και $(a,p) = 1$ τότε $(x,p) = 1$. Επομένως, αφού για $x \equiv y \pmod p$ έπεται ότι $x^2 \equiv y^2 \pmod p$, είναι αρκετό να θεωρήσουμε μόνο τους $1, 2, ..., p-1$.

Αφού είναι $(p-x)^2 \equiv x^2 \pmod p$, αυτό σημαίνει ότι αν πάρουμε το σύνολο $\{1, 2, ..., \frac{p-1}{2}\}$ και το σύνολο $\{\frac{p-1}{2}, ..., p-1\}$, τότε το τετράγωνο καθενός από το πρώτο σύνολο είναι ισοδύναμο με το τετράγωνο κάποιου από το δεύτερο, αρκεί δηλαδή να περιοριστούμε στο πρώτο σύνολο.

Τα τετράγωνα όμως $\{1^2, 2^2, ..., \frac{(p-1)^2}{4}\}$ είναι όλα μεταξύ τους όχι ισοδύναμα, διότι αν ήταν τότε μια ισοδυναμία της μορφής $x^2 \equiv a \pmod p$ θα είχε το λιγότερο 4 μη ισοδύναμες μεταξύ τους λύσεις, άτοπο λόγω του θεωρήματος Lagrange.

Δηλαδή υπάρχουν ακριβώς $\frac{p-1}{2}$ μη-ισοδύναμα τετραγωνικά υπόλοιπα $(\mathrm{mod}\ p)$ και αυτά είναι $\{1^2, 2^2, ..., \frac{(p-1)^2}{4}\}$.

□

2.4 Ο τετραγωνικός νόμος αντιστροφής

Καταρχήν θα αποδείξουμε το παρακάτω θεώρημα, γνωστό στη βιβλιογραφία σαν κριτήριο του Euler. Το κριτήριο δημοσιεύθηκε από τον Euler γύρω στο 1760. Ο ίδιος το είχε ανακοινώσει περισσότερα από δέκα χρόνια πριν. Η απόδειξη που θα ακολουθήσει είναι του Dirichlet.

Θεώρημα 2.4.1:

Αν p περιττός πρώτος και $(a,p)=1$ τότε $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Απόδειξη:

Λόγω του θεωρήματος 2.2.5 για κάθε r, με $1 \leq r \leq p-1$ η ισοδυναμία $rx \equiv a \pmod{p}$ έχει λύση. Έστω s αυτή η λύση, όπου s ο αντιπρόσωπος της κλάσης $\pmod{p}$, ο οποίος πληρεί τη συνθήκη $1 \leq s \leq p-1$.

Αν ο a δεν είναι τετραγωνικό υπόλοιπο $\pmod{p}$ τότε $r \neq s$ και οι αριθμοί $1,2,..,p-1$ μπορούν να συγκεντρωθούν σε δύο ομάδες από $\frac{p-1}{2}$ αριθμούς, τους r_i και s_i τέτοιους ώστε $r_i s_i \equiv a \pmod{p}$ για $i=1,2,...,\frac{p-1}{2}$. Παίρνουμε το γινόμενο αυτών των ισοδυναμιών και έχουμε, με χρήση του θεωρήματος Wilson,

$$-1 \equiv (p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Αλλά, αφού ο a δεν είναι τετραγωνικό υπόλοιπο $\pmod{p}$ ισχύει $(\frac{a}{p}) = -1$, δηλαδή $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Αν τώρα ο a είναι τετραγωνικό υπόλοιπο $\pmod{p}$, τότε για κάποιο ζευγάρι r_0, s_0 έχουμε $r_0 = s_0$ και $r_0^2 \equiv a \pmod{p}$. Στο θεώρημα 2.3.4 έχουμε ήδη δείξει ότι η ισοδυναμία $x^2 \equiv a \pmod{p}$ έχει ακόμη τη λύση $p-r_0$, δηλαδή

$$(p-r_0)^2 \equiv r_0^2 \equiv a \pmod{p}.$$

Σύμφωνα με το θεώρημα του Lagrange δεν υπάρχουν άλλες λύσεις. Αν βγάλουμε λοιπόν τα r_0 και $p-r_0$, μας μένουν οι υπόλοιποι $p-3$ αριθμοί από το σύνολο $1,2,..,p-1$, οι οποίοι ξανά μπορούν να διαιρεθούν σε δύο ομάδες από $\frac{p-3}{2}$ στοιχεία, στους r_i και s_i έτσι ώστε $r_i s_i \equiv a \pmod{p}$ με $r_i \neq s_i$ για $i=1,2,...,\frac{p-3}{2}$.

Πολλαπλασιάζοντας τις ισοδυναμίες κατά μέλη και την ισοδυναμία που θα βρούμε με $r_0(p-r_0)$, κάνοντας δε χρήση του θεωρήματος του Wilson, παίρνουμε:

$$-1 \equiv (p-1)! \equiv r_0(p-r_0)a^{\frac{p-3}{2}} \equiv -r_0^2 a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}} \pmod{p}.$$

Επομένως $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ και συνεπώς $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

□

Στο ερώτημα πόσο χρήσιμο είναι το κριτήριο του Euler έδωσε απάντηση ο ίδιος ο Gauss:

"In praxi nullum fere usum babeat".

Στην πράξη έχει μηδενική αξία (Disquisitiones Arithmeticae (1801), Πρόταση (Άρθρο) 106).

Πόρισμα 2.4.2:

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

2)Αν $a = \prod_{i=1}^{s} m_i$ και $(m_i, p) = 1$ για κάθε i, τότε $(\frac{a}{p}) = \prod_{i=1}^{s} (\frac{m_i}{p})$.

3)Έστω $(a, p) = (b, p) = 1$, τότε

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

Απόδειξη:

1) Από το θεώρημα 2.4.1 έχουμε $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ και επειδή ο p είναι περιττός πρώτος είναι αδύνατο να ισχύει $-1 \equiv 1 \pmod{p}$, άρα $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

2)Λόγω της υπόθεσης, έχουμε $(a, p) = 1$, δηλαδή ορίζεται το σύμβολο του Legendre και συνεπώς σύμφωνα με το 2.4.1 θα έχουμε

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} = \prod_{i=1}^{s} m_i^{\frac{p-1}{2}} \equiv \prod_{i=1}^{s} (\frac{m_i}{p}) \pmod{p}$$

$$\Rightarrow (\frac{a}{p}) - \prod_{i=1}^{s} (\frac{m_i}{p}) = kp, k \epsilon \mathbb{Z}.$$

Από τον ορισμό του συμβόλου Legendre οι δυνατές τιμές του αριστερού μέλους είναι $2, -2, 0$. Αφού όμως p είναι περιττός πρώτος πρέπει $k = 0$, δηλαδή το ζητούμενο.

3)Είναι $(\frac{a}{p})(\frac{b}{p}) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv (\frac{ab}{p}) \pmod{p}$ και $1 \not\equiv -1 \pmod{p}$, άρα $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$.

□

Παρατήρηση:

Αν $a = \prod_{i=1}^{r} p_i^{a_i}$, $a_i \geq 1$ για κάθε i η κανονική παράσταση του ακεραίου αριθμού a και $(a,p) = 1$ για κάποιο περιττό πρώτο p, τότε $(\frac{a}{p}) = \prod_{i=1}^{r} (\frac{p_i}{p})^{a_i}$. Πρόβλημα μας λοιπόν είναι ο υπολογισμός του συμβόλου Legendre της μορφής $(\frac{q}{p})$ όπου $q = 2$ ή περιττός πρώτος. Αυτό θα είναι και ο σκοπός του επόμενου θεωρήματος.

Θεώρημα 2.4.3 (Λήμμα του Gauss):

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

Απόδειξη:

Έστω s το πλήθος των στοιχείων του S που είναι μικρότερα του $\frac{p}{2}$ και r το πλήθος των στοιχείων του S που είναι μεγαλύτερα του $\frac{p}{2}$, τότε $r + s = \frac{p-1}{2}$. Συμβολίζω τα στοιχεία του S με $a_1, a_2, ..., a_s, b_1, b_2, ..., b_r$, όπου $a_i < \frac{p}{2}$ για κάθε i και $b_j > \frac{p}{2}$ για κάθε j. Από τον ορισμό του S προκύπτει ότι

$$\prod_{i=1}^{s} a_i \prod_{j=1}^{r} b_j \equiv (\frac{p-1}{2})! a^{\frac{p-1}{2}} \quad (*)$$

Αφού $\frac{p}{2} < b_j < p$ έπεται ότι $0 < p - b_j < \frac{p}{2}$ για κάθε j .

Επιπλέον ισχύει $a_i \neq p - b_j$ για κάθε i και j , διότι αν ήταν $a_i = p - b_j$ τότε $(h+k)a = ha + ka \equiv a_i + b_j \equiv p \equiv 0 \ (\mathrm{mod}\ p)$ για κάποιους ακεραίους h, k με $h \neq k$, $1 \leq h \leq \frac{p-1}{2}$, $1 \leq k \leq \frac{p-1}{2}$, άρα $p \mid (h+k)a$ και αφού $(p,a) = 1$ συνεπάγεται ότι $p \mid (h+k)$. Αυτό όμως είναι άτοπο διότι $0 < h + k < p$.

Επομένως οι αριθμοί $a_1, ..., a_s, p - b_1, ..., p - b_r$ είναι όλοι διαφορετικοί και πληρούν την ανισότητα $1 \leq x \leq \frac{p-1}{2}$. Το πλήθος τους είναι $\frac{p-1}{2}$. Άρα οι παραπάνω αριθμοί εξαντλούν πλήρως το σύνολο των ακεραίων $1, 2, ..., \frac{p-1}{2}$ οπότε και με τη βοήθεια της (*) θα έχουμε

$$(\tfrac{p-1}{2})! \equiv \prod_{i=1}^{s} a_i \prod_{j=1}^{r} (p - b_j) \equiv (-1)^r \prod_{i=1}^{s} a_i \prod_{j=1}^{r} b_j \equiv^{(*)} (-1)^r (\frac{p-1}{2})! a^{\frac{p-1}{2}} \ (\mathrm{mod}\ p).$$

Αφού $((\frac{p-1}{2})!, p) = 1$ η παραπάνω σχέση δίνει $1 \equiv (-1)^r a^{\frac{p-1}{2}} \ (\mathrm{mod}\ p)$.

Πολλαπλασιάζοντας την τελευταία ισοδυναμία με $(-1)^r$ και κάνοντας χρήση του κριτηρίου του Euler, βρίσκουμε

$$(-1)^r \equiv a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod{p} \Rightarrow (\frac{a}{p}) = (-1)^r$$

(Η τελευταία συνεπαγωγή προκύπτει ακριβώς όπως και στο προηγούμενο θεώρημα)

□

Παράδειγμα:

Αν $\alpha = 2$, θα εξετάσουμε ως προς ποιούς πρώτους p είναι τετραγωνικό υπόλοιπο. Σύμφωνα με το λήμμα του Gauss θα πρέπει να υπολογίσουμε τους άρτιους ανάμεσα στο $\frac{p}{2}$ και στο p. Αρκεί να υπολογίσουμε το πλήθος των ακεραίων στο διάστημα $(\frac{p}{4}, \frac{p}{2})$.

Γράφουμε το p στη μορφή $8k + l$, με $l = 1, 3, 5$ ή 7. Επομένως θα πρέπει να ελέγξουμε αν το πλήθος των ακεραίων στο διάστημα $(2k + \frac{l}{4}, 4k + \frac{l}{2})$ είναι άρτιος ή περιττός.

Στο υποδιάστημα $(2k + \frac{l}{4}, 4k + \frac{l}{4})$ υπάρχει άρτιο πλήθος ακεραίων, ίσο με $2k$, επομένως αρκεί να υπολογίσουμε το πλήθος των ακεραίων, έστω r, στο διάστημα $(4k + \frac{l}{4}, 4k + \frac{l}{2})$ ή στο διάστημα $(\frac{l}{4}, \frac{l}{2})$.

Αν $l = 1$ τότε $r = 0$, αν $l = 3$ τότε $r = 1$, αν $l = 5$ τότε $r = 1$ και αν $l = 7$ τότε $r = 2$.

Επομένως,

Πόρισμα 2.4.4:

$(\frac{2}{p}) = +1$, όταν $p \equiv +1, -1 \pmod{8}$

$(\frac{2}{p}) = -1$, όταν $p \equiv +3, -3 \pmod{8}$

□

Το πόρισμα αυτό μπορεί να διατυπωθεί και ως εξής:

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

Πράγματι: ο εκθέτης $\frac{p^2-1}{8}$ γράφεται $\frac{1}{2}\frac{p-1}{2}\frac{p+1}{2}$.

Οι $p-1$ και $p+1$ είναι διαδοχικοί άρτιοι, άρα μόνο ο ένας διαιρείται από 4. Επομένως ο εκθέτης είναι άρτιος όταν ο παράγοντας αυτός διαιρείται με 8, δηλαδή όταν $p \equiv +1, -1 \pmod 8$ και περιττός όταν δεν διαιρείται με 8, δηλαδή όταν $p \equiv +3, -3 \pmod 8$.

Θεώρημα 2.4.5 (Τετραγωνικός νόμος αντιστροφής):

Αν p και q είναι περιττοί πρώτοι, με $p \neq q$, τότε

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

Απόδειξη:

Η απόδειξη εξαρτάται από το λήμμα του Gauss.

Θεωρούμε τους αριθμούς $q, 2q, ..., \frac{1}{2}(p-1)q$. Για $1 \leq k \leq \frac{p-1}{2}$ από την Ευκλείδεια διαίρεση του kq με το p έχουμε $kq = pq_k + t_k$, όπου q_k και t_k είναι ακέραιοι με $1 \leq t_k \leq p-1$. Επομένως ο t_k είναι ο ελάχιστος αντιπρόσωπος του $kq \pmod p$, δηλαδή $q_k = [\frac{kq}{p}]$ (αφού $\frac{kq}{p} = q_k + \frac{t_k}{p}$, με $\frac{t_k}{p} < 1$). Όπου η συνάρτηση $[\ ]$ δηλώνει το ακέραιο μέρος του $\frac{kq}{p}$ (ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του $\frac{kq}{p}$).

Έστω $a_1, ..., a_s$ είναι οι τιμές των t_k οι οποίες είναι μικρότερες του $\frac{p}{2}$ και $b_1, ..., b_r$ οι τιμές του t_k οι οποίες είναι μεγαλύτερες του $\frac{p}{2}$. Σύμφωνα με το λήμμα του Gauss ισχύει $(\frac{q}{p}) = (-1)^r$.

Θέτουμε $a = \sum_{i=1}^{s} a_i$ και $b = \sum_{j=1}^{r} b_j$, προφανώς ισχύει

$$(A)\ \ a + b = \sum_{i=1}^{s} a_i + \sum_{j=1}^{r} b_j = \sum_{k=1}^{\frac{p-1}{2}} t_k.$$

Όπως και στην απόδειξη του λήμματος του Gauss οι αριθμοί $a_1, ..., a_s, p-b_1, ..., p-b_r$ αποτελούν μια μετάθεση των αριθμών $1, 2, ..., \frac{p-1}{2}$. Συνεπώς

$$(B)\ \ a + rp - b = \sum_{i=1}^{s} a_i + \sum_{j=1}^{r}(p - b_j) = \sum_{k=1}^{\frac{p-1}{2}} k = \frac{p^2-1}{8}.$$

Από την άλλη μεριά, θεωρούμε ξανά τη σχέση $kq = pq_k + t_k$ και κάνοντας χρήση της σχέσης (A) παίρνουμε

$$(C)\ \ p\sum_{k=1}^{\frac{p-1}{2}} q_k + a + b = \sum_{k=1}^{\frac{p-1}{2}} (pq_k + t_k) = \sum_{k=1}^{\frac{p-1}{2}} kq = \frac{p^2-1}{8} q.$$

Αφαιρούμε την (Β) από την (C) και βρίσκουμε

$$(D)\ \ p\sum_{k=1}^{\frac{p-1}{2}} q_k + 2b - rp = \frac{p^2-1}{8}(q-1).$$

Αφού τώρα ο $\frac{p^2-1}{8}$ είναι ακέραιος ($p = 2w+1$ με $w \in \mathbb{Z}$, άρα $\frac{p^2-1}{8} = \frac{4w^2+4w}{8} = \frac{w(w+1)}{2}$ ο οποίος είναι ακέραιος, αφού οι w και $w+1$ είναι διαδοχικοί ακέραιοι και άρα ο ένας διαιρείται από δύο) και $p \equiv q \equiv 1 \pmod 2$ η σχέση (D) δίνει

$$(E)\ \ \sum_{k=1}^{\frac{p-1}{2}} q_k \equiv r \pmod 2.$$

Για λόγους ευκολίας γράφουμε $u = \sum_{k=1}^{\frac{p-1}{2}} q_k = \sum_{k=1}^{\frac{p-1}{2}} [\frac{kq}{p}]$.

Η τελευταία σχέση (E) και το λήμμα του Gauss δίνουν

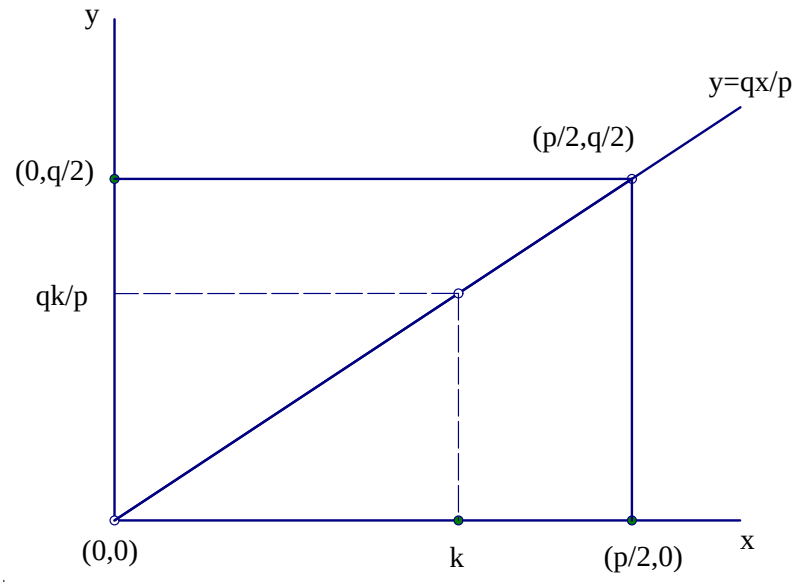
$$(Z)\ \ (\frac{q}{p}) = (-1)^r = (-1)^u.$$

Αν τώρα αλλάξουμε τους ρόλους των p και q και ξανακάνουμε την παραπάνω διαδικασία, θα βρούμε ότι $(\frac{p}{q}) = (-1)^v$, όπου $v = \sum_{j=1}^{\frac{q-1}{2}} [\frac{jp}{q}]$.

Επομένως $(\frac{p}{q})(\frac{q}{p}) = (-1)^{u+v}$. Η απόδειξη του θεωρήματος θα έχει τελειώσει αν αποδειχθεί ακόμη ότι $u + v = \frac{p-1}{2}\frac{q-1}{2}$. Τη γεωμετρική απόδειξη που ακολουθεί έδωσε για πρώτη φορά ο $Eisenstein$ (1844).

Πάνω σε ένα σύστημα καρτεσιανών συντεταγμένων θεωρούμε το ορθογώνιο παραλληλόγραμμο με κορυφές $(0,0), (\frac{p}{2}, 0), (\frac{p}{2}, \frac{q}{2}), (0, \frac{q}{2})$.

Γράφουμε την ευθεία $y = \frac{qx}{p}$, προφανώς αυτή περνάει από τα σημεία $(0,0)$ και $(\frac{p}{2}, \frac{q}{2})$ και χωρίζει το ορθογώνιο σε δύο ίσα μέρη. Ζωγραφίζουμε στο σχήμα μας όλα τα σημεία που έχουν σαν συντεταγμένες ακεραίους αριθμούς.



Πάνω στη διαγώνιο δεν έχουμε τέτοια σημεία διότι το $y = \frac{qx}{p}$ δεν είναι ακέραιος για κάθε τιμή του $x = 1, 2, ..., \frac{p-1}{2}$.

Αν $x = k\epsilon\mathbb{Z}$ και φέρω την κάθετη προς τον άξονα των x, αυτή θα κόψει την $y = \frac{qx}{p}$ στο σημείο $\frac{qk}{p}$. Το πλήθος των σημείων πάνω στην κάθετο με συντεταγμένες ακεραίους αριθμούς είναι $[\frac{qk}{p}]$. Συνολικά λοιπόν στο κάτω τρίγωνο υπάρχουν $\sum_{k=1}^{\frac{p-1}{2}}[\frac{qk}{p}]$ σημεία. Όμοια βρίσκουμε ότι στο πάνω τρίγωνο υπάρχουν ακριβώς $\sum_{l=1}^{\frac{q-1}{2}}[\frac{pl}{q}]$ σημεία. Το πλήθος όμως των σημείων μέσα στο τετράγωνο είναι $\frac{p-1}{2} \times \frac{q-1}{2}$. Δηλαδή

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{qk}{p}] + \sum_{l=1}^{\frac{q-1}{2}}[\frac{pl}{q}] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

□

Παρατήρηση:

Αυτό που λέει ο τετραγωνικός νόμος αντιστροφής, είναι ότι $(\frac{p}{q}) = (\frac{q}{p})$, αν q ή $p \equiv 1 \pmod 4$, ενώ $(\frac{p}{q}) = -(\frac{q}{p})$, αν $q \equiv p \equiv 3 \pmod 4$

Με βάση τον τετραγωνικό νόμο αντιστροφής μπορούμε να ελέγξουμε αν η τετραγωνική ισοτιμία $x^2 \equiv a \pmod{p}$, με p πρώτο και $p \neq 2$, έχει λύση ή οχι. Αρκεί να ακολουθήσουμε τον επόμενο αλγόριθμο.

1. Αναλύουμε τον a σε γινόμενο παραγόντων. Το $(\frac{a}{p})$ γράφεται σαν γινόμενο συμβόλων του Legendre της μορφής $(\frac{q}{p})$, όπου q περιττός πρώτος, $(\frac{-1}{p})$ και $(\frac{2}{p})$.

2. Υπολογίζουμε τα $(\frac{-1}{p})$ και $(\frac{2}{p})$ μέσω των πορισμάτων 2.4.2 και 2.4.4 και εφαρμόζουμε το νόμο τετραγωνικής αντιστροφής για τα $(\frac{q}{p})$ αντικαθιστώντας το με το $(\frac{p}{q})$ ή $-(\frac{p}{q})$.

3. Ανάγουμε το $p \pmod{q}$ και επαναλαμβάνουμε τη διαδικασία.

2.5 Δεύτερη απόδειξη του τετραγωνικού νόμου αντιστροφής

Η δεύτερη απόδειξη που θα δώσουμε έχει αρκετά κοινά σημεία με την πρώτη, αφού στηρίζεται και αυτή στο λήμμα του Gauss και χρησιμοποιεί τη λεγόμενη γεωμετρική μέθοδο, για να μετρήσει τα ακέραια σημεία ενός ορθογωνίου. Αρχικά θα χρειαστεί να δούμε το λήμμα του Gauss σε μια ισοδύναμη μορφή.

Αν δούμε το σύνολο $\{\pm 1, \pm 2, ..., \pm\frac{p-1}{2}\}$ σαν τις μη μηδενικές κλάσεις $(\mathrm{mod}\ p)$, τότε μπορούμε να τις χωρίσουμε φυσιολογικά σε δύο σύνολα, $P = \{1, 2, ..., \frac{p-1}{2}\}$ και $N = \{-1, -2, ..., -\frac{p-1}{2}\} = (-1)P$, που περιέχουν τους θετικούς και τους αρνητικούς ακεραίους αντίστοιχα.

Τότε το λήμμα του Gauss λέει ότι, αν p περιττός πρώτος και a ακέραιος, με $(a, p) = 1$, τότε $(\frac{a}{p}) = (-1)^m$, όπου $m = \mid aP \cap N \mid$.

Η ισοδυναμία με την προηγούμενη μορφή του λήμματος είναι προφανής, αφού το σύνολο aP αντιστοιχεί στο σύνολο S (που είδαμε στο θεώρημα $2.4.3$) και αφού το N αποτελείται από τους αντιπροσώπους που είναι μεγαλύτεροι του $\frac{p}{2}$, ο παραπάνω πληθάριθμος του $aP \cap N$ δίνει ακριβώς το πλήθος των στοιχείων του S που είναι μεγαλύτερα του $\frac{p}{2}$.

Δεύτερη απόδειξη του τετραγωνικού νόμου αντιστροφής:

Έστω τα σύνολα $P = \{1, 2, ..., \frac{p-1}{2}\} \subset \mathbb{Z}_p^*$ και $N = (-1)P$, όπως πριν και όμοια $Q = \{1, 2, ..., \frac{q-1}{2}\} \subset \mathbb{Z}_q^*$. Από το λήμμα του Gauss για $a = q$ έχουμε ότι $(\frac{q}{p}) = (-1)^m$, όπου $m = \mid qP \cap N \mid$ είναι το πλήθος των στοιχείων $x \in P$ τ.ω. να ισχύει η ισοτιμία $qx \equiv n \ (\mathrm{mod}\ p)$ για κάποιο $n \in N$, αυτό σημαίνει ότι υπάρχει ακέραιος y τ.ω. $qx - py \in N \subset \mathbb{Z}$, δηλαδή

$$-\frac{p}{2} < qx - py < 0$$

για κάποιο ακέραιο y.

Τώρα θα δούμε για ποιές τιμές του y ικανοποιείται η παραπάνω συνθήκη.

Για δοσμένο $x \in P$ οι τιμές των $qx - py$ διαφέρουν κατά ακέραια πολλαπλάσια του p (αφού $qx - py_1 - qx + py_2 = p(-y_1 + y_2)$), άρα $-\frac{p}{2} < qx - py < 0$ για τουλάχιστον έναν ακέραιο y.

Για κάθε ακέραιο y που ικανοποιείται η συνθήκη, θα ισχύει

$$0 < \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

Όμως $x \leq \frac{p-1}{2}$, άρα

$$y < \frac{qx}{p} + \frac{1}{2} \leq \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q+1}{2}.$$

Δηλαδή ο y είναι ένας ακέραιος μεταξύ 0 και $\frac{q-1}{2}$, άρα $y \in \{1, 2, ..., \frac{q-1}{2}\} = Q$.

Άρα δείξαμε ότι ο m είναι ο αριθμός των ζευγών $(x, y) \in P \times Q$ τ.ω. $-\frac{p}{2} < qx - py < 0$.

Εναλλάσοντας τα p και q, έχουμε επίσης ότι $(\frac{p}{q}) = (-1)^k$, όπου k είναι το πλήθος των ζευγών $(y, x) \in Q \times P$ τ.ω. να ισχύει ότι

$$0 < qx - py < \frac{q}{2}.$$

Έπεται ότι

$$(\frac{q}{p})(\frac{p}{q}) = (-1)^{m+k},$$

όπου $m + k$ το πλήθος των σημείων $(x, y) \in P \times Q$ τ.ω. $-\frac{p}{2} < qx - py < 0$ ή $0 < qx - py < \frac{q}{2}$.

Δεν υπάρχουν σημεία $(x, y) \in P \times Q$ ώστε $qx - py = 0$, (αφού τα p και q είναι πρώτοι μεταξύ τους και $0 < y \leq \frac{q-1}{2}$ έπεται ότι $(y, q) = 1$, άρα $(py, q) = 1$).

Επομένως μπορούμε να δούμε τις παραπάνω ανισότητες σε μία,

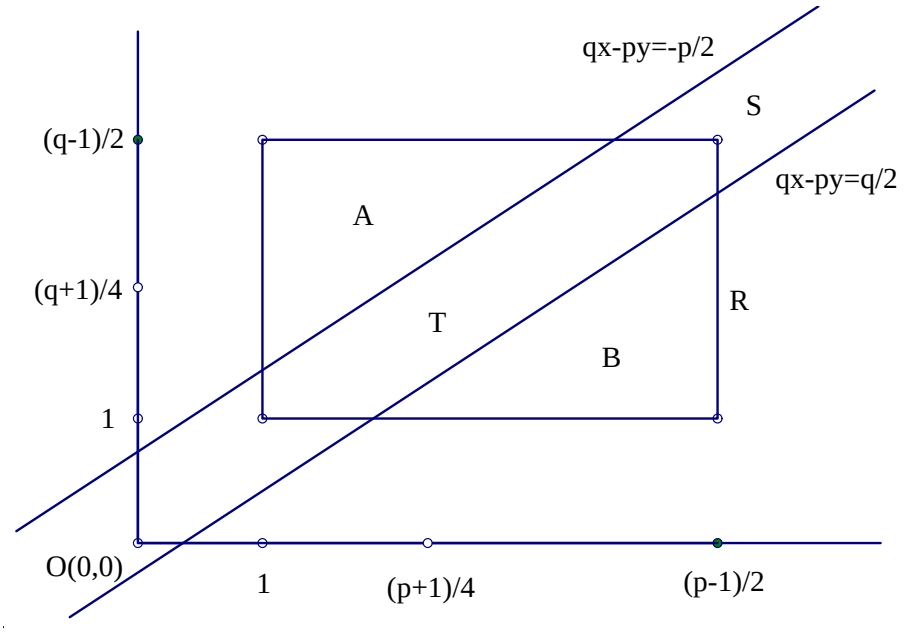
$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

Το σχήμα παριστά το σύνολο $P \times Q$ σαν τα ακέραια σημεία (x, y) στο ορθογώνιο R με $1 \leq x \leq \frac{p-1}{2}$, $1 \leq y \leq \frac{q-1}{2}$

Οι ανισότητες $-\frac{p}{2} < qx - py < \frac{q}{2}$ ορίζουν τη λωρίδα S μεταξύ των δύο παράλληλων ευθειών $qx - py = -\frac{p}{2}$ και $qx - py = \frac{q}{2}$, άρα το $m + k$ είναι το πλήθος των ακέραιων σημείων της περιοχής $T = R \cap S$.

Ο αριθμός των ακέραιων σημείων $(x, y) \in R$ είναι $\mid P \times Q \mid = \mid P \mid \cdot \mid Q \mid = \frac{(p-1)(q-1)}{4}$, άρα

$$m + k = \frac{(p-1)(q-1)}{4} - (a + b),$$



όπου a και b είναι το πλήθος των ακέραιων σημείων στις περιοχές του R, Α και Β, που βρίσκονται πάνω και κάτω από το S. Αν μπορέσουμε να δείξουμε ότι $a = b$, τότε $m + k \equiv \frac{(p-1)(q-1)}{4} \pmod 2$, και έπεται ότι

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Θα δείξουμε λοιπόν ότι $a = b$ χρησιμοποιώντας μία στροφή του ορθογωνίου κατά 180 μοίρες με κέντρο το σημείο $(\frac{p+1}{4}, \frac{q+1}{4})$, (δηλαδή ως προς το κέντρο του ορθογωνίου). Αυτή η μισή στροφή δίνετε από τον τύπο

$$r(x, y) = (x', y') = (\frac{p+1}{2} - x, \frac{q+1}{2} - y).$$

Είναι φανερό ότι η στροφή αυτή στέλνει ακέραια σημεία σε ακέραια σημεία. Επίσης εύκολα βλέπουμε ότι $qx - py < -\frac{p}{2}$ αν και μόνο αν $qx' - py' > \frac{q}{2}$, τότε $r(A)$=Β και $r(B)$=Α, άρα $a = b$ και η απόδειξη ολοκληρώθηκε.

□

2.6 Το σύμβολο του Jacobi και η γενίκευση του τετραγωνικού νόμου αντιστροφής

Θα φανεί χρήσιμο για τη συνέχεια να εισάγουμε μια γενίκευση του συμβόλου Legendre. Ας ορίσουμε το σύμβολο του Jacobi $(\frac{a}{b})$ για ακεραίους a και b, με $(a,b)=1$ και b περιττό με βάση τις ισότητες

$(\frac{a}{b})=(\frac{a}{-b})$, $(\frac{a}{1})=1$ και $(\frac{a}{b})=\prod_{i=1}^{n}(\frac{a}{p_i})$

όπου $b=p_1...p_n$ η ανάλυση του b σε πρώτους και $(\frac{a}{p_i})$ το σύμβολο του Legendre.

Λήμμα 2.6.1:

Έστω ακέραιοι a,b,c και d, με b,c περιττούς και $(a,b)=(a,c)=(d,b)=1$, τότε:

α) $(\frac{a}{b})(\frac{a}{c})=(\frac{a}{bc})$ και $(\frac{a}{b})(\frac{d}{b})=(\frac{ad}{b})$.

β) Αν η ισοτιμία $x^2\equiv a \pmod b$ έχει λύση, τότε $(\frac{a}{b})=1$.

Απόδειξη:

α) Έπεται από τον ορισμό του συμβόλου Jacobi και το πόρισμα 2.4.2.

β) Αν η $x^2\equiv a \pmod b$ έχει λύση, το ίδιο θα ισχύει και για την $x^2\equiv a \pmod{p_i}$ για κάθε i, όπου $b=p_1...p_n$ η ανάλυση σε πρώτους παράγοντες, τότε από τον ορισμό έχουμε

$$(\frac{a}{b})=\prod_{i=1}^{n}(\frac{a}{p_i})=\prod_{i=1}^{n}1=1$$

□

Αρχικά θα αποδείξουμε ένα λήμμα, που θα μας φανεί χρήσιμο στη συνέχεια για τη διατύπωση της γενίκευσης του τετραγωνικού νόμου αντιστροφής.

Λήμμα 2.6.2:

Έστω R περιττός ακέραιος και $R=r_1r_2...$, όπου r_i ακέραιοι διαιρέτες του R, τότε

$$\frac{R-1}{2}\equiv\sum_{i=1,2,...}\frac{r_i-1}{2} \pmod 2.$$

Απόδειξη:

R περιττός ακέραιος με $R = r_1 r_2 ...$, τότε οι $r_1 - 1$,$r_2 - 1$,... είναι όλοι άρτιοι και άρα κάθε γινόμενό τους, που αποτελείται από δύο ή περισσότερους παράγοντες θα είναι $\equiv 0 \pmod 4$.

Αν λοιπόν γράψουμε το R στη μορφή $R = (1 + (r_1 - 1))(1 + (r_2 - 1))...$ και κάνουμε τους πολλαπλασιασμούς, θα καταλήξουμε στη σχέση:

$$R \equiv 1 + (r_1 - 1) + (r_2 - 1) + ... \pmod 4.$$

Δηλαδή

$$\frac{R-1}{2} \equiv \sum_{i=1,2,...} \frac{r_i - 1}{2} \pmod 2.$$

□

Γενίκευση του τετραγωνικού νόμου αντιστροφής:

Έστω δυο θετικοί περιττοί ακέραιοι P, Q με $(P, Q) = 1$, τότε:

$$(\frac{P}{Q})(\frac{Q}{P}) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Θεωρούμε τη μονοσήμαντη ανάλυση του P και Q σε πρώτους:

$P = p_1 ... p_k$ και $Q = q_1 ... q_l$, με $p_i, q_j \in \mathbb{P}$ και $(p_i, q_j) = 1$.

Τότε $(\frac{P}{Q}) = \prod (\frac{p_i}{q_j})$, με $i = 1, ..., k$ και $j = 1, ..., l$

και $(\frac{Q}{P}) = \prod (\frac{q_j}{p_i})$, με $i = 1, ..., k$ και $j = 1, ..., l$.

Άρα $(\frac{P}{Q})(\frac{Q}{P}) = \prod (\frac{p_i}{q_j})(\frac{q_j}{p_i})$, με $i = 1, ..., k$ και $j = 1, ..., l$.

Από τον τετραγωνικό νόμο αντιστροφής έχουμε ότι $(\frac{p_i}{q_j})(\frac{q_j}{p_i}) = (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}$.

Τότε

$$(\frac{P}{Q})(\frac{Q}{P}) = (-1)^{\sum \frac{p_i-1}{2}\frac{q_j-1}{2}},$$

καθώς τα i και j διατρέχουν τις τιμές $1, ..., k$ και $1, ..., l$ αντίστοιχα.

Από το λήμμα 2.6.2 έχουμε ότι:

$$\sum \frac{p_i-1}{2} \equiv \frac{P-1}{2} \pmod 2 \ \ \kappa\alpha\iota \ \ \sum \frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2,$$

άρα

$$\sum \frac{p_i-1}{2}\frac{q_j-1}{2} \equiv \frac{P-1}{2}\frac{Q-1}{2} \pmod 2$$

και άρα έχουμε

$$(\frac{P}{Q})(\frac{Q}{P}) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Παρατήρηση:

Από τη σχέση $(\frac{a}{b}) = (\frac{a}{-b})$, έχουμε ότι η γενίκευση του τετραγωνικού νόμου αντιστροφής ισχύει και όταν ένας από τους P και Q είναι αρνητικός και $(P,Q)=1$.

Απόδειξη:

Έστω P,Q με $(P,Q)=1$. Χωρίς βλάβη της γενικότητας θεωρώ ότι $Q<0$ και $P>0$, τότε $P,-Q>0$ και ισχύει $(\frac{P}{-Q})(\frac{-Q}{P}) = (-1)^{\frac{P-1}{2}\frac{-Q-1}{2}}$.

Θα δείξουμε ότι

$$(\frac{P}{Q})(\frac{Q}{P}) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Είναι

$$(\frac{P}{Q})(\frac{Q}{P}) = (\frac{P}{-Q})(\frac{(-1)\cdot(-Q)}{P}) =$$

$$= (\frac{P}{-Q})(-1)^{\frac{P-1}{2}}(\frac{-Q}{P}) = (\frac{P}{-Q})(\frac{-Q}{P})(-1)^{\frac{P-1}{2}} =$$

$$= (-1)^{\frac{P-1}{2}\frac{-Q-1}{2}}(-1)^{\frac{P-1}{2}} = (-1)^{\frac{P-1}{2}(\frac{-Q-1}{2}+1)} =$$

$$= (-1)^{\frac{P-1}{2}\frac{-Q+1}{2}} = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

□

2.7 Modulus δυνάμεων πρώτων

Επόμενος στόχος είναι να δώσουμε την πρώτη απόδειξη του Gauss για τον τετραγωνικό νόμο αντιστροφής. Όπως είδαμε ο Legendre δεν μπόρεσε να αποδείξει ότι αν q πρώτος, με $q \equiv 1 \pmod 4$, τότε υπάρχει ένας τουλάχιστον πρώτος p, μικρότερος του q τ.ω. $(\frac{q}{p}) = -1$ και για αυτό το λόγο δεν κατάφερε να αποδείξει πλήρως τον τετραγωνικό νόμο αντιστροφής. Σε αυτό το κεφάλαιο θα προσπαθήσουμε να αποδείξουμε την παραπάνω πρόταση.

Αρχικά θα αποδείξουμε δύο βοηθητικά λήμματα.

Λήμμα 2.7.1:

Έστω p περιττός πρώτος και D θετικός ακέραιος, με $(p, D) = 1$, αν η ισοτιμία $x^2 \equiv D \pmod p$ έχει λύση, τότε έχει λύση και η ισοτιμία $x^2 \equiv D \pmod{p^r}$, για κάθε $r \geq 1$.

Απόδειξη:

Θα αποδείξουμε ότι αν η ισοτιμία $x^2 \equiv D \pmod{p^\omega}$ έχει λύση τότε έχει λύση και η $x^2 \equiv D \pmod{p^{\omega+1}}$ με $\omega \geq 1$. Έστω a η λύση της $x^2 \equiv D \pmod{p^\omega}$, τότε $a^2 \equiv D \pmod{p^\omega} \Rightarrow a^2 - D = hp^\omega$, για κάποιο $h \in \mathbb{Z}$. Θέτουμε $x = a + p^\omega y$, τότε $x^2 - D = a^2 + 2ap^\omega y + p^{2\omega}y^2 - D = hp^\omega + 2ap^\omega y + p^{2\omega}y^2 \equiv p^\omega(h + 2ay) \pmod{p^{\omega+1}}$

Για να έχει λύση η $x^2 \equiv D \pmod{p^{\omega+1}}$ θα πρέπει $h + 2ay \equiv 0 \pmod p$, δηλαδή $h \equiv 2ay \pmod p$. Όμως $(p, D) = 1$, άρα και $(a, p) = 1$ και αφού p περιττός πρώτος $(2a, p) = 1$, τότε από το θεώρημα **2.2.5** η $2ay \equiv h \pmod p$ έχει λύση, έστω y_0. Οπότε η $x_0 = a + p^\omega y_0$ είναι λύση της $x^2 \equiv D \pmod{p^{\omega+1}}$.

□

Λήμμα 2.7.2:

Αν $D \equiv 1 \pmod 8$, τότε η ισοτιμία $x^2 \equiv D \pmod{2^r}$ έχει λύση για κάθε $r \geq 1$.

Απόδειξη:

Η ισοτιμία $x^2 \equiv D \pmod 2$ έχει πάντα λύση (άρα και όταν $D \equiv 1 \pmod 8$).

Θα δείξουμε ότι η $x^2 \equiv D \pmod 4$ έχει λύση αν και μόνο αν $D \equiv 1 \pmod 4$.

($\Rightarrow$)

Η ρίζα της $x^2 \equiv D \pmod 4$ θα πρέπει να είναι περιττός, δηλαδή της μορφής $2n+1$, τότε το τετράγωνό της θα είναι $4n^2+4n+1 \equiv 1 \pmod 4$, άρα $D \equiv 1 \pmod 4$.

($\Leftarrow$)

Αν $D \equiv 1 \pmod 4$ έχουμε ότι το $x = 1$ είναι ρίζα της $x^2 \equiv D \pmod 4$, τότε τα $1, -1$ είναι ρίζες της $x^2 \equiv D \pmod 4$ και αφού από $Lagrange$ έχουμε το πολύ 2 λύσεις, αυτές θα είναι και οι μοναδικές.

Πάμε τώρα να δούμε ότι η ισοτιμία $x^2 \equiv D \pmod 8$ έχει λύση αν και μόνο αν $D \equiv 1 \pmod 8$.

($\Rightarrow$)

Οι λύσεις της θα είναι και λύσεις της $x^2 \equiv D \pmod 4$, οι οποίες είναι $\pm 1 \pmod 4$, άρα θα ψάξουμε για λύσεις στους αριθμούς της μορφής $4n \pm 1$. Το τετράγωνό τους είναι $16n^2 \pm 8n + 1 \equiv 1 \pmod 8$, άρα η ισοτιμία $x^2 \equiv D \pmod 8$ έχει λύση αν $D \equiv 1 \pmod 8$.

($\Leftarrow$)

Αν $D \equiv 1 \pmod 8$ έχουμε ότι το $x = 1$ είναι ρίζα της $x^2 \equiv D \pmod 8$.

Τέλος για να ολοκληρωθεί η απόδειξη θα δείξουμε ότι αν η ισοτιμία $x^2 \equiv D \pmod 8$ έχει λύση, το ίδιο θα πρέπει να ισχύει και για την $x^2 \equiv D \pmod{2^r}$, με $r \geq 3$.

Αν η ισοτιμία $x^2 \equiv D \pmod 8$ έχει λύση είδαμε ότι θα πρέπει $D \equiv 1 \pmod 8$. Όπως και στο προηγούμενο λήμμα θα αποδείξουμε ότι αν η $x^2 \equiv D \pmod{2^r}$ έχει λύση, θα έχει λύση και η $x^2 \equiv D \pmod{2^{r+1}}$. Έστω a λύση της ισοτιμίας $x^2 \equiv D \pmod{2^r}$, τότε $a^2 - D = h2^r$. Θέτουμε $x = a + 2^{r-1}y$, τότε $x^2 - D = h2^r + 2^r ay + 2^{2r-2}y^2$

Αφού $r \geq 3,\ 2r-2 \geq r+1$, άρα $x^2 - D \equiv 2^r(h+ay) \pmod{2^{r+1}}$. Για να έχουμε $x^2 \equiv D \pmod{2^{r+1}}$ αρκεί η $ay \equiv -h \pmod 2$ να έχει λύση, όμως αυτό ισχύει από το θεώρημα 2.2.5, αφού ο a περιττός.

□

Πρόταση 2.7.3:

Έστω q πρώτος, με $q \equiv 1 \pmod 4$, τότε υπάρχει ένας τουλάχιστον πρώτος p, μικρότερος του q τ.ω. $(\frac{q}{p}) = -1$.

Απόδειξη:

Θα χωρίσουμε την απόδειξη σε δυο περιπτώσεις, αν $q \equiv 1 \pmod 8$ και αν $q \equiv 5 \pmod 8$.

i) Έστω $q \equiv 5 \pmod 8$, τότε $q-2 \equiv 3 \pmod 8$, άρα ο $q-2$ έχει πρώτο παράγοντα $p \equiv 3$ ή $5 \pmod 8$.

(Αφου p πρώτος θα είναι $\equiv \pm 1, \pm 3 \pmod 8$, θέλουμε να δείξουμε ότι $p \equiv \pm 3 \pmod 8$, θα υποθέσω λοιπόν ότι $p \equiv \pm 1 \pmod 8$ και θα δείξουμε ότι ο q θα έχει αναγκαστικά παράγοντα $\equiv \pm 3 \pmod 8$, άρα επαγωγικά ο q θα έχει αναγκαστικά πρώτο παράγοντα $\equiv \pm 3 \pmod 8$. Έστω λοιπόν ότι $p \equiv \pm 1 \pmod 8$, τότε $q-2 \equiv 3 \pmod 8 \Rightarrow pk \equiv 3 \pmod 8 \Rightarrow k \equiv \pm 3 \pmod 8$).

Δηλαδή $q \equiv 2 \pmod p$ με $p \equiv \pm 3 \pmod 8$ και τότε $(\frac{q}{p}) = (\frac{2}{p}) = 2^{\frac{p^2-1}{8}} \equiv -1$ (πόρισμα 2.4.4).

ii) Έστω $q \equiv 1 \pmod 8$ και $2m+1$ ένας περιττός πρώτος $< q$. Ας θεωρήσουμε ότι το λήμμα δεν ισχύει (και θα οδηγηθούμε σε αντίφαση), τότε για κάθε πρώτο $p \leq 2m+1$ ο q είναι τετραγωνικό ισοϋπόλοιπο $\pmod p$, δηλαδή η $x^2 \equiv q \pmod p$ έχει λύση, το ίδιο και η $x^2 \equiv q \pmod 8$, (για x=1).

Από τα λήμματα 2.7.1 και 2.7.2 έχουμε ότι το q είναι τετραγωνικό ισοϋπόλοιπο για κάθε αριθμό με πρώτους παράγοντες $p \leq 2m+1$.

Έστω $M = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (2m) \cdot (2m+1)$, ο M έχει πρώτους διαιρέτες $\leq 2m+1$, άρα $(\frac{q}{M}) = 1$, τότε η $x^2 \equiv q \pmod M$ έχει λύση, έστω k. Είναι $(q, M) = 1$, αφού $2m+1 < q$, άρα $(k, M) = 1$.

Έχουμε $k(q-1^2)(q-2^2)\ldots(q-m^2) \equiv k(k^2-1^2)(k^2-2^2)\ldots(k^2-m^2)) \equiv (k+m)(k+m-1)\ldots(k+1)k(k-1)\ldots(k-m+1)(k-m) \pmod M$

Το τελευταίο είναι γινόμενο $2m+1$ διαδοχικών όρων, όμως κάθε τέτοιο γινόμενο διαιρείται από το $(2m+1)! = M$, (δείτε παράρτημα 4.3), τότε το M διαιρεί και το $k(q-1^2)(q-2^2)\ldots(q-m^2)$ και αφού $(k, M) = 1$, το M θα διαιρεί το $(q-1^2)(q-2^2)\ldots(q-m^2)$.

Το M μπορούμε να το δούμε και σαν $M = (m+1) \cdot ((m+1)^2-1^2) \cdot ((m+1)^2-2^2) \cdot \ldots \cdot ((m+1)^2-m^2)$, άρα το γινόμενο:

$$\frac{1}{m+1} \cdot \frac{q-1^2}{(m+1)^2-1^2} \cdot \ldots \cdot \frac{q-m^2}{(m+1)^2-m^2}$$

είναι ακέραιος.

Στη συνέχεια θα δείξουμε ότι στην περίπτωση μας αυτό το γινόμενο δεν μπορεί να είναι ακέραιος, τότε οδηγούμαστε σε άτοπο και η υπόθεση που κάναμε στην αρχή, ότι το λήμμα δεν ισχύει είναι λανθασμένη και η απόδειξη τελείωσε.

Είναι φανερό ότι το γινόμενο αυτό δεν είναι ακέραιος όταν ο m είναι ο μεγαλύτερος ακέραιος μικρότερος του $\sqrt{q}$, δηλαδή όταν $m < \sqrt{q} < m+1$, αφού τότε όλα τα

κλάσματα που αποτετελούν το γινόμενο είναι μικρότερα της μονάδας. Αρκεί λοιπόν να μπορούμε να επιλέξουμε το m τέτοιο ώστε $m < \sqrt{q} < m + 1$.

Το $q \equiv 1 \pmod 8$, για την περίπτωση $q = 9$ είναι εύκολο να δούμε ότι το λήμμα είναι αληθές, οπότε μπορούμε να περιοριστούμε στη περίπτωση που $q \geq 17$, τότε $2\sqrt{q} + 1 < q$. Ο μόνος περιορισμός που έχουμε για το m είναι ότι $2m + 1 < q$ και αφού $2\sqrt{q} + 1 < q$, έπεται ότι μπορούμε να επιλέξουμε το m ώστε $m < \sqrt{q} < m + 1$.

□

2.8 Τρίτη απόδειξη του τετραγωνικού νόμου αντιστροφής

Τώρα είμαστε έτοιμοι να δούμε την πρώτη απόδειξη που έδωσε ο Gauss για τον τετραγωνικό νόμο αντιστροφής. Με τη βοήθεια του συμβόλου Legendre η απόδειξη γίνεται πιο απλή και σύντομη, αφού μπορούμε να συνδιάσουμε τις πολλές περιπτώσεις που είχε διακρίνει ο Gauss.

Αυτό που θα αποδείξουμε είναι ότι αν ο τετραγωνικός νόμος ισχύει για κάθε ζεύγος πρώτων p, p' οι οποίοι είναι μικρότεροι από ένα πρώτο q (επαγωγική υπόθεση), τότε θα ισχύει και για κάθε ζευγάρι ενός πρώτου $p < q$ με το q. Από αυτό και από το γεγονός ότι το θεώρημα ισχύει για τους αρχκούς δύο περιττούς πρώτους 3 και 5 προκύπτει η γενική ισχύ του θεωρήματος.

Αν ο τετραγωνικός νόμος αντιστροφής ισχύει για κάθε ζευγάρι πρώτων p, p', με $p' < q$, τότε και η γενίκευση του θα ισχύει για κάθε P, Q, πρώτους μεταξύ τους, οι οποίοι έχουν πρώτους παράγοντες μικρότερους από q.

Για να αποδείξουμε ότι ο τετραγωνικός νόμος ισχύει για κάθε ζευγάρι ενός πρώτου $p < q$ με το q, θα διακρίνουμε δυο περιπτώσεις:

(I) Αν $q = 4n + 1$ και $(\frac{p}{q}) = -1$, τότε αρκεί να αποδείξουμε ότι $(\frac{q}{p}) = -1$ (ο τετραγωνικός νόμος αντιστροφής λέει ότι $(\frac{p}{q}) = (\frac{q}{p})$ αν q ή $p \equiv 1 \pmod 4$).

(II) Τη δεύτερη περίπτωση θα τη χωρίσουμε σε δύο υποπεριπτώσεις:

(II_1) $q = 4n + 1$ και $(\frac{p}{q}) = 1$.

(II_2) $q = 4n + 3$.

Για τη (II_1) θέτουμε $\omega = p$, άρα $(\frac{\omega}{q}) = 1$, αρκεί λοιπόν να αποδείξουμε ότι $(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{q-1}{2}}$.

Για τη (II_2) είναι $(\frac{-1}{q}) = (-1)^{\frac{q-1}{2}} = (-1)^{2n+1} = -1$, τότε:

-Αν $(\frac{p}{q}) = 1$, θέτουμε $\omega = p$ και έχουμε $(\frac{\omega}{q}) = 1$, αρκεί λοιπόν να αποδείξουμε πάλι ότι $(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{q-1}{2}}$.

-Αν $(\frac{p}{q}) = -1$, τότε θέτουμε $\omega = -p$ και έχουμε $(\frac{\omega}{q}) = (\frac{-p}{q}) = (-1)^{\frac{q-1}{2}}(\frac{p}{q}) = (-1)(-1) = 1$, αρκεί λοιπόν πάλι να αποδείξουμε ότι $(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{q-1}{2}}$.

Βλέπουμε δηλαδή ότι στην περίπτωση (II) μπορούμε να θέσουμε $\omega = \pm p$, έτσι ώστε το ω να είναι τετραγωνικό ισοϋπόλοιπο $\pmod q$, για τουλάχιστον ένα πρόσημο και μένει όπως είδαμε να αποδείξουμε ότι $(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{q-1}{2}}$.

Για την περίπτωση (II)**:**

Έστω $\omega = p$ ή$-p$, τετραγωνικό ισοϋπόλοιπο $\pmod q$. Τότε η ισοτιμία $x^2 \equiv \omega \pmod q$ έχει δύο ρίζες μεταξύ των 0 και q και το άθροισμά τους είναι ίσο με q (είδαμε ότι αν α μία ρίζα τότε η άλλη είναι η q-α).

Οπότε μία από αυτές, ας τη θέσουμε e θα είναι άρτιος (περιττός = άρτιος +περιττός). Συνεπώς $e^2 \equiv \omega \pmod q$, δηλαδή $e^2 - \omega = qf$, με $f \in \mathbb{Z} - \{0\}$,(αν $f = 0$ τότε θα έπρεπε ο πρώτος αριθμός ω να είναι τετράγωνο, άτοπο).

Επίσης ο f δεν μπορεί να είναι αρνητικός, αν ήταν θα έπρεπε να είναι $-\omega = qf_e^2 < 0$, άρα $\omega = +p$ και τότε $p - e^2 = p - qf - p = -qf > 0$, θετικός ακέραιος που διαιρείται από το q, όμως $p - e^2 < p < q$, αντίφαση.

Ο f πρέπει να είναι περιττός, (αφού ο e είναι άρτιος τότε ο $e^2 - \omega$ είναι περιττός και άρα και ο f σαν διαιρέτης του πρέπει να είναι περιττός).

Τέλος, ο περιττός θετικός ακέραιος f πρέπει να είναι $< q - 1$, επειδή $e \leq q - 1$ και $p < q - 1$ έχουμε ότι $qf = e^2 - \omega < (q-1)^2 + (q-1) = q^2 - q$, άρα $qf < q(q-1) \Rightarrow f < q - 1$.

Θα διακρίνουμε 2 περιπτώσεις:

1. Αν το f δε διαιρείται από το p, από τη σχέση $e^2 - \omega = qf$ έπεται ότι $e^2 \equiv \omega \pmod f$, δηλαδή $(\frac{\omega}{f}) = +1 \quad (1)$

Επίσης $qf \equiv e^2 \pmod \omega$, άρα $(\frac{qf}{\omega}) = +1$, δηλαδή $(\frac{q}{\omega}) = (\frac{f}{\omega}) \quad (2)$.

Τώρα αφού οι περιττοί θετικοί ακέραιοι f και ω είναι μεταξύ τους πρώτοι, μικρότεροι του q θα ικανοποιούν τη γενίκευση του τετραγωνικού νόμου αντιστροφής (επαγωγική υπόθεση), δηλαδή $(\frac{f}{\omega})(\frac{\omega}{f}) = (-1)^{\frac{\omega-1}{2}\frac{f-1}{2}}$.

Τότε αντικαθιστώντας από τις (1) και (2) έχουμε:

$$(\frac{q}{\omega}) \cdot 1 = (-1)^{\frac{\omega-1}{2}\frac{f-1}{2}}$$

$$(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{f-1}{2}} \quad (3)$$

Αφού ο e είναι άρτιος θα ισχύει $e^2 \equiv 0 \pmod 4$, άρα $-\omega \equiv qg \pmod 4$, εύκολα βλέπουμε ότι:

$$-\frac{\omega+1}{2} \equiv \frac{qf-1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod 2$$

(Για την πρώτη ισοτιμία: $-\frac{\omega+1}{2} - \frac{qf-1}{2} = 2k \Leftrightarrow -\omega - 1 - qf + 1 = 4k \Leftrightarrow -\omega \equiv qf$

$(\mathrm{mod}\ 4)$, που ισχύει.

Για τη δεύτερη ισοτιμία: $\frac{qf-1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod 2 \Leftrightarrow -qf+q+f \equiv 1 \pmod 4$, όμως q και f περιττοί, άρα $q = 2k+1$ και $f = 2l+1$, τότε $-(2k+1)(2l+1) + 2k + 1 + 2l + 1 \equiv 1 \pmod 4 \Leftrightarrow 0 \equiv 0 \pmod 4$, που ισχύει).

Τότε

$$-\frac{\omega+1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod 2$$

$$-\frac{\omega+1}{2}\frac{\omega-1}{2} \equiv (\frac{q-1}{2} + \frac{f-1}{2})\frac{\omega-1}{2} \pmod 2$$

Το $\frac{\omega+1}{2}\frac{\omega-1}{2}$ είναι γινόμενο δυο διαδοχικών ακεραίων, άρα άρτιος, έπεται λοιπόν ότι:

$$\frac{q-1}{2} \cdot \frac{\omega-1}{2} \equiv \frac{f-1}{2} \cdot \frac{\omega-1}{2} \pmod 2$$

Τότε η (3) δίνει: $(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{q-1}{2}}$.

2. Έστω ότι το p διαιρεί το f, τότε $f = \omega\phi$, όπου ο ϕ είναι περιττός ακέραιος με πρόσημο ίδιο με αυτό του ω και απόλυτη τιμή $< q$.

Αφού $e^2 - \omega = q\omega\phi$, έχουμε ότι το ω διαιρεί το e^2 και αφού ω πρώτος, έχουμε ότι το ω διαιρεί το e, τότε $e = \varepsilon\omega$, όπου ε ένας περιττός ακέραιος. Οπότε:

$$\varepsilon^2\omega^2 - \omega = q\omega\phi$$

$$\varepsilon^2\omega - 1 = q\phi$$

και έπεται ότι το ϕ δεν διαιρείται από το ω (διαφορετικά το ω θα διαιρεί το 1, το οποίο είναι άτοπο). Αφού όμως το ω είναι τετραγωνικό ισοϋπόλοιπο $mod\ \ f = \omega\phi$ ($e^2 - \omega = q\omega\phi$), θα είναι και τετραγωνικό ισοϋπόλοιπο $(\mathrm{mod}\ \phi)$, $((\omega, \phi) = 1)$. Δηλαδή $(\frac{\omega}{\phi}) = (\frac{\omega}{-\phi}) = +1$ (4).

Επίσης $-q\phi = 1 - \varepsilon^2\omega \Rightarrow -q\phi \equiv 1 \pmod \omega$, άρα το $-q\phi$ είναι τετραγωνικό ισοϋπόλοιπο $(\mathrm{mod}\ \omega)$, δηλαδή $(\frac{-q\phi}{\omega}) = 1 \Rightarrow (\frac{q}{\omega}) = (\frac{-\phi}{\omega})$ (5).

Τελικά, αφού ένας από τους δυο περιττούς αριθμούς, $-\phi$ και ω, είναι θετικός και αφού είναι πρώτοι μεταξύ τους $< q$, από τη γενίκευση του τετραγωνικού νόμου αντιστροφής έχουμε:

$$(\frac{-\phi}{\omega})(\frac{\omega}{-\phi}) = (-1)^{\frac{\omega-1}{2}\frac{\phi+1}{2}}.$$

Τότε αντικαθιστώντας από τις (4) και (5): $(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{\phi+1}{2}} \quad (6)$.

Όμως ο ε είναι άρτιος, άρα $q\phi = \varepsilon^2\omega - 1 \equiv -1 \pmod 4$, ένας από τους q και ϕ πρέπει να είναι της μορφής $4n+1$ και ο άλλος της μορφής $4n+3$. Τότε

$$\frac{\phi+1}{2} \equiv \frac{q-1}{2} \pmod 2$$

και τότε η (6) δίνει: $(\frac{q}{\omega}) = (-1)^{\frac{\omega-1}{2}\frac{q-1}{2}}$.

Για την περίπτωση (I)**:**

Αν $q = 4n+1$ και για $p < q$ ισχύει $(\frac{p}{q}) = -1$, τότε αρκεί να αποδείξουμε ότι $(\frac{q}{p}) = -1$ (ο τετραγωνικός νόμος αντιστροφής λέει ότι $(\frac{p}{q}) = (\frac{q}{p})$ αν q ή $p \equiv 1 \pmod 4$).

Από την πρόταση 2.7.3 έχουμε ότι αν $q \equiv 1 \pmod 4$, τότε υπάρχει κάποιος πρώτος $p' < q$, τέτοιος ώστε $(\frac{q}{p'}) = -1$.

Αν $(\frac{p'}{q}) = -1$ τότε η προς απόδειξη σχέση ισχύει για τα p' και q. Θα δείξουμε ότι δεν γίνεται να είναι $(\frac{p'}{q}) = 1$, αφού αν ίσχυε θα είχαμε $(\frac{q}{p'}) = (-1)^{\frac{p'-1}{2}\frac{q-1}{2}} = (-1)^{\frac{p'-1}{2}\cdot(2n)} = 1$, το οποίο είναι άτοπο.

Άρα ο τετραγωνικός νόμος αντιστροφής ισχύει για τα p' και q. Μένει να δείξουμε ότι αν υπάρχουν και άλλοι πρώτοι p μικρότεροι του q, με $(\frac{p}{q}) = -1$ τότε θα ισχύει ότι $(\frac{q}{p}) = -1$, ισοδύναμα αρκεί να δείξουμε ότι:

$$(\frac{q}{pp'}) = +1.$$

Αφού λοιπόν για τα p και p' έχουμε ότι είναι τετραγωνικά ανισοϋπόλοιπα $\pmod q$, έχουμε ότι το pp' είναι τετραγωνικό ισοϋπόλοιπο $\pmod q$, οπότε θα υπάρχει κάποιος άρτιος αριθμός $e < q$, τ.ω. $e^2 - pp' = q\phi$, (η μία από τις δυο ρίζες της $x^2 \equiv pp' \pmod q$ είναι άρτια, αφού το άθροισμα των δυο ριζών είναι ίσο με q), για κάποιο ακέραιο ϕ.

Το αριστερό μέλος της ισότητας αναπαριστά έναν περιττό αριθμό μικρότερο του q^2, τότε θα πρέπει και ο ϕ να είναι ένας περιττός μικρότερος του q.

Τώρα, ανάλογα με τη διαιρετότητα του ϕ από τα p και p', διακρίνουμε τις ακόλουθες περιπτώσεις:

1. Αν το ϕ δεν διαιρείται από τα p και p', δηλαδή $(\phi, pp') = 1$. Από τη σχέση $e^2 - pp' = q\phi$ θα έχουμε ότι $q\phi$ είναι τετραγωνικό ισοϋπόλοιπο $\pmod{pp'}$, δηλαδή $(\frac{q\phi}{pp'}) = 1$ και συνεπάγεται ότι $(\frac{q}{pp'}) = (\frac{\phi}{pp'})$.

Όμως η $e^2 - pp' = q\phi$ μας λέει επίσης ότι το pp' είναι τετραγωνικό ισοϋπόλοιπο $\pmod{\phi}$, δηλαδή $(\frac{pp'}{\phi}) = 1$.

Οι ϕ και pp' είναι δύο περιττοί αριθμοί, πρώτοι μεταξύ τους, με τον ένα από αυτούς να είναι σίγουρα θετικός (ο pp') και έχουν πρώτους παράγοντες μικρότερους του q. Άρα από τη γενίκευση του τετραγωνικού νόμου αντιστροφής έχουμε:

$$(\frac{\phi}{pp'})(\frac{pp'}{\phi}) = (-1)^{\frac{\phi-1}{2}\frac{pp'-1}{2}}$$

και, αντικαθιστώντας από τις σχέσεις $(\frac{pp'}{\phi}) = 1$ και $(\frac{q}{pp'}) = (\frac{\phi}{pp'})$, παίρνουμε ότι:

$$(\frac{q}{pp'}) = (-1)^{\frac{\phi-1}{2}\frac{pp'-1}{2}}.$$

Στη συνέχεια θα βρούμε αν ο εκθέτης του -1 είναι άρτιος ή περιττός.

Ο e είναι άρτιος, οπότε η $e^2 - pp' = q\phi$ μας δίνει ότι $-pp' \equiv q\phi \pmod 4$ και αφού $q \equiv 1 \pmod 4$ έχουμε

$$\phi \equiv -pp' \pmod 4 \Rightarrow \frac{\phi-1}{2} \equiv -\frac{pp'+1}{2} \pmod 2$$

και τότε θα πρέπει

$$\frac{\phi-1}{2} \cdot \frac{pp'+1}{2} \equiv 0 \pmod 2.$$

Άρα ο ζητούμενος εκθέτης είναι άρτιος και έχουμε $(\frac{q}{pp'}) = 1$.

2. Αν $p'|\phi$ και $p \not| \phi$.

Το $p'|\phi$, τότε $p'|q\phi + pp' = e^2$ και αφού p' πρώτος, το p' διαιρεί το e, οπότε θα έχουμε $\phi = p'\psi$ και $e = p'\varepsilon$. Το $\psi < q$ είναι ένας περιττός που δεν διαιρείται από το p, (αφού $p|\phi$) και το ε είναι ένας άρτιος, (αφού e άρτιος), τότε από τη σχέση $e^2 - pp' = q\phi$ παίρνουμε

$$p'\varepsilon^2 - p = q\psi.$$

Όμως $(\psi, pp') = 1$ (είδαμε ότι $p \not| \psi$, αν τώρα $p'|\psi$, από την παραπάνω σχέση θα είχαμε ότι $p'|p$, άτοπο), άρα από τη σχέση $e^2 - pp' = q\phi = qp'\psi$ έχουμε

$$(\frac{pp'}{\psi}) = +1.$$

Επίσης $(\frac{q\psi}{p}) = (\frac{p'}{p})$, αφού από τη σχέση $p'\varepsilon^2 - p = q\psi$ βλέπουμε ότι το $q\psi$ είναι τετραγωνικό ισοϋπόλοιπο $\pmod p$ αν και μόνο αν το p' είναι τετραγωνικό ισοϋπόλοιπο $\pmod p$, τότε

$$(\frac{q}{p})(\frac{\psi}{p}) = (\frac{p'}{p}) \Rightarrow (\frac{q}{p}) = (\frac{p'}{p})(\frac{\psi}{p}). \quad (I)$$

Πάλι από τη σχέση $p'\varepsilon^2 - p = q\psi$ έχουμε ότι $-p \equiv q\psi \pmod{p'}$, άρα

$$(\frac{q\psi}{p'}) = (\frac{-p}{p'}) \Rightarrow (\frac{q}{p'}) = (\frac{-p}{p'})(\frac{\psi}{p'}). \quad (II)$$

Πολλαπλασιάζοντας τις (I) και (II):

$$(\frac{q}{pp'}) = (\frac{p'}{p})(\frac{-p}{p'})(\frac{\psi}{pp'}) = (\frac{p'}{-p})(\frac{-p}{p'})(\frac{\psi}{pp'}) = (-1)^{\frac{p+1}{2}\frac{p'-1}{2}}(\frac{\psi}{pp'}) \quad (*)$$

Τώρα αφού τα ψ και pp' έχουν πρώτους παράγοντες μικρότερους του q, από τη γενίκευση του τετραγωνικού νόμου αντιστροφής έχουμε:

$$(\frac{\psi}{pp'})(\frac{pp'}{\psi}) = (-1)^{\frac{\psi-1}{2}\frac{pp'-1}{2}},$$

όμως δείξαμε ότι $(\frac{pp'}{\psi}) = 1$, άρα $(\frac{\psi}{pp'}) = (-1)^{\frac{\psi-1}{2}\frac{pp'-1}{2}}$.

Αντικαθιστώντας στην $(*)$ παίρνουμε:

$$(\frac{q}{pp'}) = (-1)^{\frac{p+1}{2}\frac{p'-1}{2}+\frac{\psi-1}{2}\frac{pp'-1}{2}}.$$

Στη συνέχεια θα δείξουμε ότι ο εκθέτης είναι $\equiv 0 \pmod 2$.

Ξέρουμε ότι $\varepsilon^2 \equiv 0 \pmod 4$ και $q \equiv 1 \pmod 4$, τότε από τη σχέση $p'\varepsilon^2 - p = q\psi$ έπεται ότι $\psi \equiv -p \pmod 4$, άρα

$$\frac{\psi - 1}{2} \equiv \frac{p+1}{2} \pmod 2,$$

τότε

$$\frac{p+1}{2}\frac{p'-1}{2}+\frac{\psi-1}{2}\frac{pp'-1}{2}\equiv\frac{p+1}{2}[\frac{p'-1}{2}+\frac{pp'-1}{2}] \pmod 2$$

Από το λήμμα 2.6.2 έχουμε ότι

$$\frac{pp'-1}{2}\equiv\frac{p-1}{2}+\frac{p'-1}{2},$$

άρα

$$\frac{p+1}{2}\frac{p'-1}{2}+\frac{\psi-1}{2}\frac{pp'-1}{2}\equiv\frac{p+1}{2}\frac{p-1}{2}\equiv 0 \pmod 2$$

(αφού τα $\frac{p+1}{2}$, $\frac{p-1}{2}$ είναι διαδοχικοί ακέραιοι ο ένας αναγκαστικά θα είναι άρτιος) και τότε έχουμε την προς απόδειξη σχέση $(\frac{q}{pp'})=1$.

Αν $p|\phi$ και $p' \not| \phi$, η απόδειξη είναι όμοια.

3.Αν τα p και p' διαιρούν το ϕ, αφού οι p και p' είναι πρώτοι διαφορετικοί μεταξύ τους, θα πρέπει και το pp' να διαιρεί το ϕ και τότε γράφουμε $\phi=pp'\psi$, όπου ψ ένας περιττός μικρότερος του q. Από τη σχέση $e^2-pp'=q\phi$ έχουμε ότι και ο e διαιρείται από το pp' και τότε μπορεί να γραφτεί σαν $e=pp'\varepsilon$, όπου ε ένας άρτιος αριθμός, τότε

$$pp'\varepsilon^2-1=q\psi.$$

Τα $pp'e^2$ και ψ είναι πρώτα μεταξύ τους, διαφορετικά αν ένας πρώτος τους διαιρεί, θα πρέπει από την παραπάνω σχέση να διαιρεί και το 1, άτοπο.

Επίσης έχουμε ότι $pp'\varepsilon^2\equiv 1 \pmod\psi$, τότε η $x^2\equiv pp'\varepsilon^2 \pmod\psi$ έχει λύση, τη $x=1$. Δηλαδή το $pp'\varepsilon^2$ είναι τετραγωνικό ισοϋπόλοιπο $\pmod\psi$, άρα

$$(\frac{pp'\varepsilon^2}{\psi})=1\Rightarrow(\frac{pp'}{\psi})(\frac{\varepsilon^2}{\psi})=1,$$

όμως $(\frac{\varepsilon^2}{\psi})=1$, άρα

$$(\frac{pp'}{\psi})=1.$$

Έχουμε όμως ότι και $-q\psi\equiv 1 \pmod{pp'}$, άρα $(\frac{-q\psi}{pp'})=1$ και συνεπάγεται ότι

$$(\frac{q}{pp'})=(\frac{\psi}{pp'}).$$

Οι αριθμοί $-\psi$ και pp' είναι πρώτοι μεταξύ τους, με pp' σίγουρα θετικό και πρώτους παράγοντες μικρότερους του q, άρα από τη γενίκευση του τετραγωνικού νόμου αντιστροφής θα έχουμε ότι

$$(\frac{-\psi}{pp'})(\frac{pp'}{\psi}) = (-1)^{\frac{pp'-1}{2}\frac{\psi+1}{2}}.$$

Ο ε είναι άρτιος, άρα $\varepsilon^2 \equiv 0 \pmod 4$ και $q \equiv 1 \pmod 4$, τότε από τη σχέση $pp'\varepsilon^2 - 1 = q\psi$ έχουμε ότι $\psi \equiv -1 \pmod 4$, τότε ο $\frac{\psi+1}{2}$ είναι άρτιος και έπεται ότι

$$(\frac{q}{pp'}) = 1$$

και η απόδειξη ολοκληρώθηκε.

□

2.9 Αθροίσματα Gauss

Οι μέθοδοι που χρησιμοποιήσαμε ως τώρα για να αποδείξουμε τον τετραγωνικό νόμο αντιστροφής μπορεί να είναι ιδιαίτερα ευφυείς, αλλά δε μπορούν να χρησιμοποιηθούν εύκολα σε πιο γενικές περιπτώσεις (νόμος κυβικής αντιστροφής κ.τ.λ.). Σε αυτό το κεφάλαιο θα δώσουμε μία νέα απόδειξη, βασιζόμενη σε μια μέθοδο που μπορεί να γενικευτεί και να χρησιμοποιηθεί για την απόδειξη υψηλότερης τάξης νόμων αντιστροφής.

Αρχικά θα εισάγουμε τις έννοιες των αλγεβρικών αριθμών και των αλγεβρικών ακεραίων.

Ορισμός:

Ένας μιγαδικός αριθμός a ο οποίος είναι ρίζα ενός πολυωνύμου $a_0x^n+a_1x^{n-1}+...+a_{n-1}x+a_n$, με $a_0,a_1,...,a_n\in\mathbb{Q}$ και $a_0\neq 0$ λέγεται **αλγεβρικός αριθμός**.

Ένας μιγαδικός αριθμός ω ο οποίος είναι ρίζα ενός πολυωνύμου $x^n+b_1x^{n-1}+...+b_{n-1}x+b_n$, με $b_1,...,b_n\in\mathbb{Z}$ λέγεται **αλγεβρικός ακέραιος**.

Προφανώς κάθε αλγεβρικός ακέραιος είναι αλγεβρικός αριθμός.

Πρόταση 2.9.1:

Ένας ρητός αριθμός $r\in\mathbb{Q}$ είναι αλγεβρικός ακέραιος αν και μόνο αν $r\in\mathbb{Z}$.

Απόδειξη:

Αν $r\in\mathbb{Z}$ τότε είναι ρίζα του πολυωνύμου $x-r=0$, που έχει ακέραιους συντελεστές, άρα ο r είναι αλγεβρικός ακέραιος. Έστω τώρα ότι $r\in\mathbb{Q}$ και r αλγεβρικός ακέραιος. Τότε από τον ορισμό έχουμε ότι ο r ικανοποιεί την εξίσωση $x^n+b_1x^{n-1}+...+b_n=0$, με $b_1,...,b_n\in\mathbb{Z}$.

Ο r όμως είναι ρητός αριθμός, άρα υπάρχουν ακέραιοι c,d με $d\neq 0$ και $(c,d)=1$ τέτοιοι ώστε $r=\frac{c}{d}$. Αντικαθιστώντας στην εξίσωση έχουμε

$$c^n+b_1c^{n-1}d+...+b_nd^n=0.$$

Θα δείξουμε ότι $d=1$. Έστω ότι $d>1$, τότε θα υπάρχει p πρώτος διαιρέτης του b. Από την πάνω σχέση θα πρέπει ο p να διαιρεί και το c^n και αφού p πρώτος θα πρέπει να διαιρεί το c, τότε όμως $p|(c,d)=1$, άτοπο, άρα $d=1$.

□

Στη συνέχεια θα δείξουμε ότι οι αλγεβρικοί αριθμοί αποτελούν σώμα, ενώ οι αλγεβρικοί ακέραιοι δακτύλιο.

Ορισμός:

Ένα υποσύνολο $V \subset \mathbb{C}$ των μιγαδικών θα λέγεται $\mathbb{Q} - module$ αν :

α)Για $\gamma_1, \gamma_2 \in V$ συνεπάγεται ότι $\gamma_1 + \gamma_2, \gamma_1 - \gamma_2 \in V$.

β)Για $\gamma \in V$ και $r \in \mathbb{Q}$ συνεπάγεται ότι $r\gamma \in V$.

γ)Υπάρχουν στοιχεία $\gamma_1, ..., \gamma_l \in V$, τέτοια ώστε κάθε $\gamma \in V$ να γράφεται σαν $\sum_{i=1}^{l} r_i\gamma_i$, με $r_i \in \mathbb{Q}$.

Αν $\gamma_1, ..., \gamma_l \in \mathbb{C}$, το σύνολο όλων των στοιχείων της μορφής $\sum_{i=1}^{l} r_i\gamma_i$, με $r_i \in \mathbb{Q}$ είναι προφανές από τον ορισμό ότι είναι $\mathbb{Q} - module$ και θα το συμβολίζουμε με $[\gamma_1, ..., \gamma_l]$.

Πρόταση 2.9.2:

Έστω $V = [\gamma_1, ..., \gamma_l]$ και ένα $a \in \mathbb{C}$ τέτοιο ώστε για κάθε $\gamma \in V$ να ισχύει $a\gamma \in V$, τότε ο a είναι αλγεβρικός αριθμός.

Απόδειξη:

Έχουμε $a\gamma_i \in V$ για κάθε $i = 1, ..., l$, τότε $a\gamma_i = \sum_{j=1}^{l} a_{ij}\gamma_j$, όπου $a_{ij} \in \mathbb{Q}$.

Θεωρούμε τώρα τον $l \times l$ πίνακα $A = (a_{ij})$, τότε

$$(A - Ia)(\gamma_1, ..., \gamma_l)^T = (0, ..., 0)^T$$

Αν η ορίζουσα $|A - Ia|$ είναι διαφορετική του μηδενός το ομογενές σύστημα θα είχε ως λύση μόνο τη μηδενική, επειδή όμως τα γ_i δεν είναι όλα μηδέν, έχουμε ότι $|A - Ia| = 0$.

Όμως η $|A - Ia|$ είναι πολυωνυμική έκφραση του a της μορφής $a^n + c_{n-1}a^{n-1} + ... + c_0$, όπου τα $c_i \in \mathbb{Q}$, (αφού παράγονται από γινόμενα των $a_{ij} \in \mathbb{Q}$).

Άρα ο a είναι αλγεβρικός αριθμός.

□

Θεώρημα 2.9.3:

Το σύνολο των αλγεβρικών αριθμών αποτελεί σώμα.

Απόδειξη:

Έστω a_1 και a_2 αλγεβρικοί αριθμοί. Θα δείξουμε ότι και οι a_1a_2 και a_1+a_2 είναι αλγεβρικοί αριθμοί. Αφού a_1 και a_2 αλγεβρικοί αριθμοί θα ισχύουν οι παρακάτω εξισώσεις

$a_1^n + r_1a_1^{n-1} + ... + r_n = 0 \quad (1)$

$a_2^m + s_1a_2^{m-1} + ... + s_m = 0 \quad (2)$

για κάποια $r_i, s_j \in \mathbb{Q}$.

Έστω V ένα $\mathbb{Q} - module$, με γεννήτορες τα στοιχεία $a_1^i a_2^j$, όπου $0 \leq i < n$ και $0 \leq j < m$. Για κάθε $\gamma \in V$ έχουμε $a_1\gamma \in V$, $a_2\gamma \in V$ και $a_1a_2\gamma \in V$ (αφού $\gamma \in V$ έχουμε $\gamma = \sum q_{ij}a_1^i a_2^j$ με $q_{ij} \in \mathbb{Q}$, τότε $a_1\gamma = a_1 \sum q_{ij}a_1^i a_2^j = \sum q_{ij}a_1^{i+1}a_2^j$. Αν η δύναμη $i+1$ είναι ίση με n τότε μπορούμε να τη μειώσουμε με τη βοήθεια της (1), άρα το $a_1\gamma$ θα γράφετε σαν $\sum q'_{ij}a_1^i a_2^j$ με $0 \leq i < n$ και $0 \leq j < m$, άρα $a_1\gamma \in V$. Όμοια για τα $a_2\gamma \in V$ και $a_1a_2\gamma \in V$).

Από τον ορισμό του $\mathbb{Q} - module$ έχουμε ότι αφού $a_1\gamma \in V$, $a_2\gamma \in V$ τότε $(a_1 + a_2)\gamma \in V$. Δείξαμε δηλαδή ότι για κάθε $\gamma \in V$ έχουμε $(a_1 + a_2)\gamma \in V$ και $a_1a_2\gamma \in V$. Τότε από την πρόταση 2.9.2 οι a_1+a_2 και a_1a_2 είναι αλγεβρικοί ακέραιοι.

Τέλος έμεινε να δείξουμε ότι αν ο a είναι αλγεβρικός ακέραιος, διαφορετικός του μηδενός, το ίδιο ισχύει για τον a^{-1}. Ο a σαν αλγεβρικός ακέραιος πρέπει να ικανοποιεί την εξίσωση $a_0a^n + a_1a^{n-1} + ... + a_n = 0$, όπου $a_i \in \mathbb{Q}$, τότε $a_na^{-n} + a_{n-1}a^{n-1} + ... + a_0 = 0$, άρα και ο a^{-1} είναι αλγεβρικός ακέραιος.

□

Ορισμός:

Ένα υποσύνολο $W \subset \mathbb{C}$ των μιγαδικών θα λέγεται $\mathbb{Z} - module$ αν :

α)Για $\gamma_1, \gamma_2 \in W$ συνεπάγεται ότι $\gamma_1 + \gamma_2, \gamma_1 - \gamma_2 \in W$.

β)Υπάρχουν στοιχεία $\gamma_1, ..., \gamma_l \in W$, τέτοια ώστε κάθε $\gamma \in W$ να γράφεται σαν $\sum_{i=1}^{l} b_i\gamma_i$, με $b_i \in \mathbb{Z}$.

Πρόταση 2.9.4:

Έστω W ένα $\mathbb{Z} - module$ και $\omega \in \mathbb{C}$ τέτοιο ώστε $\omega\gamma \in W$ για κάθε $\gamma \in W$, τότε ο ω είναι αλγεβρικός ακέραιος.

Η απόδειξη είναι όμοια με αυτή της πρότασης 2.9.2.

□

Πρόταση 2.9.5:

Το σύνολο των αλγεβρικών ακεραίων αποτελεί δακτύλιο.

Η απόδειξη είναι όμοια με αυτή της πρότασης 2.9.3.

□

Έστω Ω ο δακτύλιος των αλγεβρικών ακεραίων. Αν $\omega_1, \omega_2, \gamma \in \Omega$, θα λέμε ότι $\omega_1 \equiv \omega_2 \pmod{\gamma}$ αν $\omega_1 - \omega_2 = \gamma a$, με $a \in \Omega$.

Η επόμενη πρόταση θα μας χρησιμεύσει στη συνέχεια.

Πρόταση 2.9.6:

Αν $\omega_1, \omega_2 \in \Omega$ και $p \in \mathbb{Z}$ (άρα ανήκει και στο Ω) πρώτος, τότε:

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

Απόδειξη:

Έχουμε $(\omega_1 + \omega_2)^p = \sum_{k=o}^{p} \binom{p}{k} \omega_1^k \omega_2^{p-k}$ και $p | \binom{p}{k}$ για κάθε $1 \leq k \leq p-1$, ($\binom{p}{k} = \frac{p!}{k!(p-k)!}$, άρα $p! = \binom{p}{k} k!(p-k)!$. Όμως $p|p!$, άρα έχουμε ότι $p|\binom{p}{k}k!(p-k)!$, όμως $p \not| k!(p-k)!$ αφού το γινόμενο περιέχει όρους μικρότερους από το p, άρα $p|\binom{p}{k}$, τότε $(\omega_1 + \omega_2)^p = \omega_1^p + \sum_{k=1}^{p-1} \binom{p}{k} \omega_1^k \omega_2^{p-k} + \omega_2^p \equiv \omega_1^p + \omega_2^p \pmod{p}$

□

Οι n ρίζες της μονάδας είναι λύσεις της εξίσωσης $x^n - 1$, άρα είναι αλγεβρικοί ακέραιοι. Ας θεωρήσουμε μία πρωταρχική p ρίζα της μονάδας $\zeta = e^{\frac{2\pi i}{p}}$.

Λήμμα 2.9.7:

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p, \text{ αν } a \equiv 0 \pmod{p} \\ 0, \text{ αν } a \not\equiv 0 \pmod{p} \end{cases}$$

Απόδειξη:

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

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 2.9.8:

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

Η απόδειξη είναι άμεση από το λήμμα 2.9.7.

□

Λήμμα 2.9.9:

$\sum_{t=0}^{p-1} (\frac{t}{p}) = 0$, όπου $(\frac{t}{p})$ το σύμβολο *Legendre*.

Απόδειξη:

Το $(\frac{0}{p})$ είναι ίσο με το μηδέν εξ' ορισμού. Από τους υπόλοιπους $p - 1$ όρους του αθροίσματος, όπως είδαμε στο κεφάλαιο 2.3, οι μισοί έχουν τιμή 1 και οι άλλοι μισοί έχουν τιμή -1, άρα το άθροισμα είναι μηδέν.

□

Ορισμός:

Το $g_a = \sum_{t=0}^{p-1} (\frac{t}{p})\zeta^{at}$ λέγεται τετραγωνικό άθροισμα του Gauss.

Πρόταση 2.9.10:

$g_a = (\frac{a}{p})g_1$

Απόδειξη:

Αν $a \equiv 0 \pmod{p}$, τότε $\zeta^{at} = 1$ για κάθε t και άρα έχουμε $g_a = \sum_{t=0}^{p-1} (\frac{t}{p}) = 0$ από το λήμμα 2.9.9. Όμως $(\frac{a}{p}) = 0$, άρα δείξαμε ότι η σχέση ισχύει για $a \equiv 0 \pmod{p}$.

Αν $a \not\equiv 0 \pmod{p}$ τότε $(\frac{a}{p})g_a = \sum_{t=0}^{p-1} (\frac{at}{p})\zeta^{at} = \sum_{x=0}^{p-1} (\frac{x}{p})\zeta^{x} = g_1$ (στην αλλαγή της μεταβλητής του αθροίσματος κάναμε χρήση του θεωρήματος 2.2.3, που στην περίπτωση αυτή μας λέει ότι καθώς το t διατρέχει τις κλάσεις $\pmod{p}$, το ίδιο κάνει και το $x = at$, $(a, p) = 1$).

Αφού $(\frac{a}{p})^2 = 1$ όταν $a \not\equiv 0 \pmod{p}$, πολλαπλασιάζουμε την $(\frac{a}{p})g_a = g_1$ με $(\frac{a}{p})$ και έχουμε ότι $g_a = (\frac{a}{p})g_1$.

□

Προκύπτει από την πρόταση 2.9.10 ότι $g_a^2 = g_1^2$ αν $a \not\equiv 0 \pmod{p}$. Θέτουμε $g = g_1$ και στη συνέχεια θα υπολογίσουμε την κοινή αυτή τιμή.

Πρόταση 2.9.11:

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

Απόδειξη:

Η ιδέα της απόδειξης είναι να εκφράσουμε το άθροισμα $\sum_{a=0}^{p-1} g_a g_{-a}$ με δύο διαφορετικούς τρόπους.

Αν $a \not\equiv 0 \pmod{p}$, τότε $g_a g_{-a} = (\frac{a}{p})g(\frac{-a}{p})g = (\frac{-a^2}{p})g^2 = (\frac{-1}{p})g^2$,

δηλαδή

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1} (\frac{-1}{p}) g^2 = (\frac{-1}{p})(p-1)g^2 \quad (1).$$

Επίσης

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

αθροίζοντας για $a = 0$ μέχρι $p-1$ και από το πόρισμα 2.9.8 έχουμε:

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} (\frac{x}{p})(\frac{y}{p}) \delta(x,y) p$$

με $\delta(x,y) = 1$ αν $x \equiv y \pmod p$ και $\delta(x,y) = 0$ αν $x \not\equiv y \pmod p$,

άρα

$$\sum_{x=0}^{p-1} \sum_{y=0}^{p-1} (\frac{x}{p})(\frac{y}{p}) \delta(x,y) = \sum_{x \equiv y \pmod p} (\frac{x^2}{p}) \cdot 1 + \sum_{x \not\equiv y \pmod p} (\frac{x}{p})(\frac{y}{p}) \cdot 0 = p-1$$

Οπότε θα έχουμε

$$\sum_{a=0}^{p-1} g_a g_{-a} = p(p-1) \quad (2)$$

Από τις (1),(2):

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

□

2.10 Τέταρτη απόδειξη του τετραγωνικού νόμου αντιστροφής

Έστω $p^* = (-1)^{\frac{p-1}{2}}p = g^2$ και $q \neq p$ περιττός πρώτος. Έχουμε $g^{q-1} = (g^2)^{\frac{q-1}{2}} = {p^*}^{\frac{q-1}{2}} \equiv (\frac{p^*}{q}) \pmod q$ (από το θεώρημα 2.4.1), δηλαδή $g^q \equiv (\frac{p^*}{q})g \pmod q$ (1).

Ο g είναι αλγεβρικός ακέραιος (δείξαμε ότι οι αλγεβρικοί ακέραιοι αποτελούν δακτύλιο και αφού ο ζ είδαμε ότι είναι αλγεβρικός ακέραιος, το ίδιο θα ισχύει και για το $\sum_{t=0}^{p-1}(\frac{t}{p})\zeta^t = g$), άρα από την πρόταση 2.9.6 θα έχουμε:

$$g^q = (\sum_{t=0}^{p-1}(\frac{t}{p})\zeta^t)^q \equiv \sum_{t=0}^{p-1}(\frac{t}{p})^q\zeta^{qt} \equiv \sum_{t=0}^{p-1}(\frac{t}{p})\zeta^{qt} \equiv g_q \equiv (\frac{q}{p})g \pmod q \quad (2).$$

Από τις (1) και (2) έχουμε:

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

πολλαπλασιάζοντας και τα δυο μέλη με g και με τη βοήθεια της σχέσης $g^2 = p^*$ βρίσκουμε ότι:

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

και αφού $(p^*, q) = 1$ θα είναι:

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

επειδή $1 \not\equiv -1 \pmod q$ έπεται ότι:

$$(\frac{q}{p}) = (\frac{p^*}{q})$$

όμως από τον ορισμό του p^* έχουμε $(\frac{p^*}{q}) = (\frac{-1}{q})^{\frac{p-1}{2}}(\frac{p}{q}) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}(\frac{p}{q})$

άρα

$$(\frac{q}{p}) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}(\frac{p}{q}) \Rightarrow (\frac{q}{p})(\frac{p}{q}) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$$

□

Κεφάλαιο 3

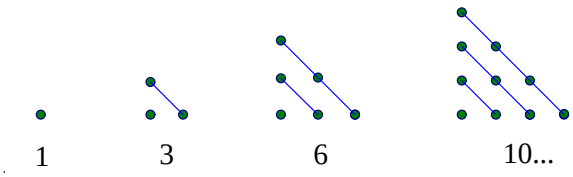
Πολύγωνοι αριθμοί

3.1 Εισαγωγή

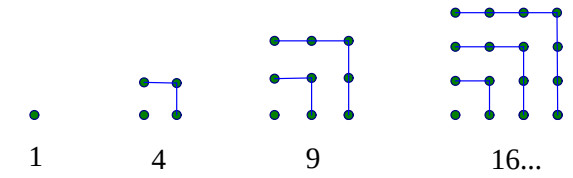
Ένα από τα πρώτα υποσύνολα των φυσικών αριθμών που μελετήθηκαν από τους αρχαίους Έλληνες ήταν οι πολύγωνοι αριθμοί. Δίνεται ένας φυσικός αριθμός m, με $m > 1$, οι φυσικοί αριθμοί της μορφής $m\frac{n^2-n}{2} + n$, με $n \in \mathbb{N} \cup \{0\}$ θα λέγονται (m+2)-γωνοι αριθμοί.

Οι αριθμοί αυτοί αποτέλεσαν μία γέφυρα μεταξύ της γεωμετρίας και της θεωρίας αριθμών. Πρώτος ο Πυθαγόρας μελέτησε τον 6ο αιώνα π.Χ. τους τρίγωνους και τους τετράγωνους αριθμούς.

Τρίγωνοι αριθμοί $t_n = \frac{n(n+1)}{2}$ $(m = 1)$:



Τετράγωνοι αριθμοί $s_n = n^2$ $(m = 2)$:



Η ακριβής ημερομηνία της γέννησης του Πυθαγόρα δεν μπορεί να καθοριστεί, αλλά μια κοινή παράδοση την τοποθετεί στο 569 π.Χ. Το όνομα του σημαίνει αυτός που μιλάει (αγορεύειν) με τις ευλογίες του Πύθιου Απόλλωνα. Για τον Πυθαγόρα τα μαθηματικά ήταν η γέφυρα ανάμεσα στον ορατό και τον αόρατο κόσμο. Επεδίωξε την μελέτη των μαθηματικών όχι μόνο ως έναν τρόπο κατανόησης και διαχείρισης της Φύσης, αλλά επίσης ως έναν τρόπο να φύγει ο νους μακριά από τον φυσικό κόσμο, τον οποίο θεωρούσε πρόσκαιρο και ψεύτικο.

Οι Πυθαγόρειοι γνώριζαν ότι το n-οστό τετράγωνο είναι ίσο με το άθροισμα των n πρώτων περιττών ακεραίων. Δηλαδή ότι $n^2 = 1+3+5+...+(2n-1)$, για κάθε θετικό ακέραιο n. Η ιδιότητα αυτή των φυσικών εμφανίζεται επίσης, πολύ αργότερα στο έργο Liber quadratorum (Το βιβλίο των τετραγώνων) του Leonardo Pisano, γνωστότερου ως Fibonacci.

Μία άλλη ενδιαφέρουσα ιδιότητα, που ήταν γνωστή στους Πυθαγορείους εμφανίζεται στις Πλατωνικές ερωτήσεις του Πλούταρχου. Ο Πλούταρχος αναφέρει ότι οχτώ φορές ένας τρίγωνος αριθμός συν ένα μας δίνει τετράγωνο. Με σημερινούς συμβολισμούς έχουμε $8t_n + 1 = 8\frac{n(n+1)}{2} + 1 = (2n+1)^2 = s_{2n+1}$.

Ο όρος πολύγωνοι αριθμοί εισάγεται πρώτη φορά από τον Έλληνα μαθηματικό και αστρονόμο Υψικλή (2ος αι. μ.Χ.), συγγραφέα του έργου "Περί πολυέδρων", που αποτελεί συνέχεια παρόμοιων ερευνών του Απολλώνιου και έχει συμπεριληφθεί στα Στοιχεία του Ευκλείδη, ως το δέκατο τέταρτο βιβλίο τους.

Σημαντικά έργα εκείνης της εποχής, στα οποία συναντάμε ιδιότητες των πολύγωνων αριθμών είναι η Αριθμητική Εισαγωγή του Νικομάχου (100 μ.Χ.) και τα Αριθμητικά του Διόφαντου.

Το 1636 ο Pierre de Fermat γράφει ότι έχει ανακαλύψει ένα πολύ όμορφο θεώρημα, ότι κάθε θετικός ακέραιος είναι άθροισμα το πολύ τριών τρίγωνων αριθμών, τεσσάρων τετράγωνων αριθμών, πέντε πενταγώνων αριθμών κ.ο.κ. Προσθέτει όμως πως δεν θα μπορέσει να δώσει και την απόδειξη, αφού αυτή στηρίζεται σε "πολυάριθμα και δυσνόητα μυστήρια των αριθμών". Σχεδίαζε να αφιερώσει ένα βιβλίο σε αυτά τα μυστήρια, αλλά δυστυχώς ποτέ δεν το δημοσίευσε.

Το 1798 στο $Théorie$ des nombres, ο Ιταλός μαθηματικός και αστρονόμος Joseph Louis Lagrange, χρησιμοποιώντας μία ταυτότητα που ανακάλυψε ο Leonhard Euler απέδειξε την εικασία του Fermat για την περίπτωση των τετραγώνων.

Στις 10 Ιουλίου 1796, ο Gauss αποδεικνύει το αποτέλεσμα για την περίπτωση των τρίγωνων αριθμών, σε ηλικία μόλις 19 χρονών και στο ημερολόγιο του έγραψε

$$\varepsilon\acute{\upsilon}\rho\eta\kappa\alpha!\ \ num = \triangle + \triangle + \triangle$$

Δύο χρόνια αργότερα το αποτέλεσμα του Gauss αποδεικνύεται ανεξάρτητα από τον Γάλλο μαθηματικό Adrien Marie Legendre. Το 1815 ο Augustin Louis Cauchy αποδεικνύει πλήρως την εικασία (*Oeuvres complètes*, τόμος 6).

Σε αυτό το κεφάλαιο θα αποδείξουμε το θεώρημα των πολύγωνων αριθμών, βασιζόμενοι στη δουλειά των Gauss και Cauchy.

3.2 Μορφές Gauss

Έστω D αρνητικός ακέραιος και ισότιμος με $1 \pmod 4$. Έστω επίσης ακέραιοι a, b και c, ανά δύο πρώτοι μεταξύ τους τ.ω. $a, c > 0$ και $b^2 - 4ac = D$.

Υπάρχουν πάντα τέτοιοι ακέραιοι, για παράδειγμα αφού $D \equiv 1 \pmod 4$, υπάρχει κάποιος αρνητικός ακέραιος n τ.ω. $D = 4n + 1$. Μια τέτοια τριάδα είναι $a = -n > 0$, $b = 1$ και $c = 1$.

Το πολυώνυμο $ax^2+bxy+cy^2$ θα λέγεται **μορφή Gauss** και θα τη συμβολίζουμε με $[a, b, c]$. Κάθε μορφή Gauss θα αντιστοιχεί σε ένα πίνακα

$$M = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$$

Παρατηρούμε ότι ισχύει

$$[a, b, c] = (x\ y)M(x\ y)^T$$

Ο D λέγεται διακρίνουσα της μορφής Gauss $[a, b, c]$ και του αντίστοιχου πίνακα.

Υπόλογίζοντας την ορίζουσα του πίνακα έχουμε $detM = ac - \frac{b^2}{4} = -\frac{D}{4}$, δηλαδή

$$D = -4detM.$$

Πρόταση 3.2.1:

Αν ο D, στην ανάλυση του σε γινόμενο πρώτων παραγόντων, έχει r διακεκριμένους πρώτους παράγοντες, τότε ο αριθμός των μορφών Gauss με $b = a$, δηλαδή των $[a, a, c]$ είναι 2^r.

Απόδειξη:

Το $ax^2 + axy + cy^2$ είναι μία από τις ζητούμενες μορφές Gauss αν και μόνο αν $a^2 - 4ac = a(a - 4c) = D$, με a θετικό και περιττό (ο a είναι θετικός εξ' ορισμού και περιττός αφού D περιττός), $a - 4c$ αρνητικό και περιττό και ΜΚΔ($a, a - 4c$)=1 (έστω p πρώτος με $p|a$ και $p|a - 4c$, τότε θα διαιρεί και τη διαφορά τους, δηλαδή $p|4c$, το p σαν περιττός πρώτος δε μπορεί να διαιρεί το 4, άρα το $p|c$, άτοπο αφού οι a και c είναι πρώτοι μεταξύ τους).

Επομένως κάθε πρώτος παράγοντας του D στη μέγιστη δύναμη που διαιρεί τον D θα εμφανίζεται είτε στο a είτε στο $a-4c$. Όταν στη συνέχεια θα αναφερόμαστε στους

r αυτούς πρώτους θα τους θεωρούμε στη δύναμη που εμφανίζονται στην ανάλυση του D. Τότε τα πιθανά a είναι 2^r, αφού έχουμε r πρώτους παράγοντες (πάντα στη δύναμη που αναφέραμε παραπάνω) και κάθε ένας από αυτούς έχει 2 επιλογές, να διαιρεί ή να μην διαιρεί το a. Για κάθε επιλογή του a ορίζεται και το $c = \frac{a^2-D}{4a}$. Άρα έχουμε 2^r μορφές Gauss $[a, a, c]$.

□

Για παράδειγμα ας υποθέσουμε ότι το $D = -143 \equiv 1 \pmod 4$, η ανάλυση του D σε πρώτους παράγοντες είναι $D = 11 \cdot 13$ και τότε οι επιλογές του a είναι 1,11,13 ή 143. Έστω $a = 11$, τότε $a - 4c = -\frac{143}{11} = -13$ και έχουμε $c = \frac{a+13}{4} = 6$.

$SL_2(\mathbb{Z})$: η πολλαπλασιαστική ομάδα των δύο επί δύο πινάκων με ακέραια στοιχεία και ορίζουσα ίση με 1.

Αν $G = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL_2(\mathbb{Z})$, ορίζουμε την πράξη:

$G*[a,b,c] = (x\ y)GMG^T(x\ y)^T = [ar^2+brs+cs^2, 2art+b(ru+st)+2csu, at^2+btu+cu^2]$, όπου Μ ο πίνακας που αντιστοιχεί στη μορφή Gauss $[a, b, c]$.

Θεώρημα 3.2.2:

Αν $[a, b, c]$ μία μορφή Gauss και $G \in SL_2(\mathbb{Z})$, τότε το $G * [a, b, c]$ είναι επίσης μορφή Gauss (με την ίδια διακρίνουσα D).

Απόδειξη:

Έστω Μ ο πίνακας που αντιστοιχεί στη $[a, b, c]$ και M' ο πίνακας που αντιστοιχεί στην

$$G * [a, b, c] = [a', b', c'], \quad \text{με} \quad G = \begin{bmatrix} r & s \\ t & u \end{bmatrix}.$$

Θα πρέπει να δείξουμε ότι: (1) οι a', b' και c' είναι πρώτοι μεταξύ τους, (2) η μορφή $[a', b', c']$ έχει διακρίνουσα D και (3) $a', b' > 0$.

Έχουμε λοιπόν:

1)Κάθε πρώτος διαιρέτης των a, b και c διαιρεί επίσης και τα

$$a' = ar^2 + brs + cs^2$$

$$b' = 2art + b(ru + st) + 2csu$$

$$c' = at^2 + btu + cu^2$$

Επίσης αφού $(G^{-1}) * [a', b', c'] = G^{-1} * (G * [a, b, c]) = [a, b, c]$, έχουμε από τις αντίστοιχες σχέσεις ότι κάθε πρώτος διαιρέτης των a', b' και c' διαιρεί τα a, b και c (ο G^{-1} υπάρχει αφού $detG = 1 \neq 0$). Έπεται λοιπόν ότι αφού τα a, b και c είναι ανά δύο πρώτοι μεταξύ τους το ίδιο θα ισχύει και για τα a', b' και c'.

2) Η διακρίνουσα της μορφής $[a', b', c']$ είναι $-4detM' = -4det(GMG^T) = -4detG \cdot detM \cdot detG^T = -4detM = D \ \ (detG = detG^T = 1)$.

3)Έχουμε ότι $D < 0$, δηλαδή $b^2 - 4ac < 0$, οπότε $b^2 < 4ac$ και αφού $ac > 0$ έχουμε

$$|b| < 2\sqrt{ac}$$

Επίσης

$$(\sqrt{a}|r| - \sqrt{c}|s|)^2 \geq 0$$

$$ar^2 - 2\sqrt{ac}|r| \cdot |s| + cs^2 \geq 0$$

$$ar^2 - |brs| + cs^2 \geq 0$$

Επομένως $a' = ar^2 + bsr + cs^2 > 0$, (αφού $bsr \geq -|bsr|$) και επείδη $b'^2 - 4a'c' = D < 0$ έχουμε ότι και $c' > 0$.

□

Θεώρημα 3.2.3:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} * [a, b, c] = [c, -b, a]$$

$$\begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} * [a, a, c] = [c, 2c - a, c]$$

$$\begin{bmatrix} -1 & 2 \\ -1 & 1 \end{bmatrix} * [a, a, c] = [4c - a, 4c - a, c]$$

$$\begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} * [a, b, c] = [a, b + 2an, an^2 + bn + c]$$

Παρατήρηση: αν $a \neq 0$ και n ο κοντινότερος ακέραιος στο $-\frac{b}{2a}$, τότε $|b+2an| \leq a$. (Αφού ο n είναι ο κοντινότερος ακέραιος στο $-\frac{b}{2a}$, τότε η απόσταση τους θα είναι μικρότερη από το $\frac{1}{2}$, δηλαδή $|n-(-\frac{b}{2a})| \leq \frac{1}{2} \Rightarrow |n+\frac{b}{2a}| \leq \frac{1}{2}$ και επειδή $a > 0$ πολλαπλασιάζουμε με $2a$ και έχουμε το αποτέλεσμα).

Απόδειξη:

Για την πρώτη ισότητα έχουμε

$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} * [a,b,c] = [a',b',c']$, με

$a' = ar^2 + brs + cs^2 = a \cdot 0 + b \cdot 0 \cdot 1 + c \cdot 1^2 = c$

$b' = 2art + b(ru+st) + 2csu = 2a \cdot 0 \cdot (-1) + b(0+(-1)) + 2c \cdot 1 \cdot 0 = -b$

$c' = at^2 + btu + cu^2 = a \cdot (-1)^2 + b(-1) \cdot 0 + c \cdot 0 = a$

Ομοίως τα υπόλοιπα.

□

Μια μορφή Gauss $[a,b,c]$ (ή ο αντίστοιχος πίνακας) θα λέγεται **ανηγμένη (reduced)** αν

i) $|b| \leq a \leq c$

ii) $b \geq 0$, αν $|b| = a$ ή $c = a$.

Θεώρημα 3.2.4:

Αν $[a,b,c]$ ανηγμένη μορφή Gauss, τότε $a \leq \sqrt{-\frac{D}{3}}$.

Απόδειξη:

$4a^2 \leq 4ac = b^2 - D \leq a^2 - D$, άρα $3a^2 \leq -D$.

□

Για παράδειγμα υπάρχει μόνο μία ανηγμένη μορφή Gauss για $D = -3$, η $[1,1,1]$. Από το παραπάνω θεώρημα έχουμε ότι $a \leq \sqrt{-\frac{-3}{3}} = 1$ και αφού $a > 0$ θα πρέπει $a = 1$, τότε από τον ορισμό της ανηγμένης μορφής έχουμε $|b| \leq 1$, δηλαδή $b = 0, -1$ ή 1.

Αν $b = 0$ τότε $D = 4ac$ και $D \equiv 1 \pmod 4$, άτοπο.

Αν $b = -1$ τότε $|b| = a$ και από τον ορισμό της ανηγμένης μορφής θα έπρεπε $b > 0$, άτοπο.

Άρα $b = 1$ και τότε $c = \frac{b^2-D}{4a} = \frac{1+3}{4} = \frac{4}{4} = 1$.

Θεώρημα 3.2.5:

Έστω a και c δύο σχετικά πρώτοι θετικοί ακέραιοι.

Αν $a \leq c$ τότε η μορφή Gauss $[a, a, c]$ είναι ανηγμένη.

Αν $c < a < 2c$ τότε η μορφή Gauss $[c, 2c - a, c]$ είναι ανηγμένη.

Αν $2c < a \leq 3c$ τότε η μορφή Gauss $[c, -(2c - a), c]$ είναι ανηγμένη.

Αν $3c < a < 4c$ τότε η μορφή Gauss $[4c - a, 4c - a, c]$ είναι ανηγμένη.

Όλες οι παραπάνω μορφές Gauss έχουν τη ίδια διακρίνουσα $D = a^2 - 4ac$.

Απόδειξη:

Θα δούμε την δεύτερη περίπτωση. Από το θεώρημα 3.2.2 είδαμε ότι η πράξη $G * [a, b, c]$ μας δίνει μορφή Gauss αν η $[a, b, c]$ είναι μορφή Gauss και $G \in SL_2(\mathbb{Z})$. Τότε η $[c, 2c - a, c]$ είναι μορφή Gauss, αφού όπως είδαμε από το θεώρημα 3.2.3 προκύπτει από την πράξη ανάμεσα στον πίνακα $\begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$ και τη μορφή $[a, a, c]$.

Θα δείξουμε τώρα ότι ισχύει η ανισότητα $|b| \leq a \leq c$. Η ανισότητα $|b| \leq a$ στην $[c, 2c - a, c]$ μεταφράζεται στην $|2c - a| \leq c$, δηλαδή

$$-c \leq 2c - a \leq c \Leftrightarrow -3c \leq -a \leq -c \Leftrightarrow c \leq a \leq 3c$$

που ισχύει αφού $c < a < 2c$. Όμοια η σχέση $a \leq c$ στην περίπτωση μας μεταφράζεται στην $c \leq c$, που προφανώς ισχύει. Τέλος το b, δηλαδή το $2c - a$ είναι θετικό αφού $2c > a$ και είμαστε στην περίπτωση που $a = c$ (το a στην $[c, 2c - a, c]$ είναι το c).

□

Δύο μορφές Gauss F και F' (ή οι αντίστοιχοι πίνακες) θα λέγονται **γνήσια ισοδύναμες** αν και μόνο αν για κάποιο $G \in SL_2(\mathbb{Z})$, ισχύει $F' = G * F$ (και αντίστοιχα $M' = GMG^T$).

Θα δείξουμε ότι η παραπάνω σχέση είναι σχέση ισοδυναμίας.

1) Είναι ανακλαστική, αφού $F = G * F$ για $G = I \in SL_2(\mathbb{Z})$

2) Είναι συμμετρική. Πράγματι αν $F' \sim F$ τότε $F' = G * F$ για κάποιο $G \in SL_2(\mathbb{Z})$ και $M' = GMG^T$. Όμως $detG = 1 \neq 0$, άρα υπάρχει ο αντίστροφος του G και πολλαπλασιάζοντας με αυτόν την παραπάνω σχέση, έχουμε

$$G^{-1}M' = MG^T$$
$$G^{-1}M'(G^T)^{-1} = M$$
$$G^{-1}M'(G^{-1})^T = M$$

άρα θέτοντας $G' = G^{-1}$ έχουμε $M = G'M'G'^T$, δηλαδή $F \sim F'$ (η $SL_2(\mathbb{Z})$ είναι ομάδα, άρα $G^{-1} \in SL_2(\mathbb{Z})$).

3) Είναι μεταβατική. Αν $F'' \sim F'$ και $F' \sim F$ τότε $M'' = G'M'G'^T$ και $M' = GMG^T$ για κάποιους $G, G' \in SL_2(\mathbb{Z})$, άρα

$$M'' = G'GMG^TG'^T = (G'G)M(G'G)^T$$

προφανώς $G'G \in SL_2(\mathbb{Z})$, επομένως $F'' \sim F$.

Θεώρημα 3.2.6:

Κάθε μορφή Gauss είναι γνήσια ισοδύναμη με μια ανηγμένη μορφή Gauss.

Απόδειξη:

Από το θεώρημα 3.2.3 η $[a, b, c]$ είναι γνήσια ισοδύναμη με την $[c, -b, a]$ και την $[a, b + 2an, an^2 + bn + c]$. Με τη βοήθεια της πρώτης ισοδυναμίας μπορούμε να ικανοποιήσουμε την συνθήκη $a \leq c$ και παράλληλα η απόλυτη τιμή του b να μην αλλάζει, ενώ με τη δεύτερη, για κατάλληλο n μπορούμε να ικανοποιήσουμε την $|b| \leq a$ (από παρατήρηση του θεωρήματος 3.2.3).

Έτσι μπορούμε να κατασκευάσουμε μία ακολουθία μορφών Gauss, με πρώτο όρο τη δοσμένη μορφή και τέτοια ώστε ο πρώτος όρος a των μορφών να φθίνει.

Για παράδειγμα έστω ότι η δοσμένη μορφή είναι η $[10, 14, 5]$, τότε θα έχουμε:

$[10, 14, 5]$, εδώ το a είναι μεγαλύτερο από το c οπότε χρησιμοποιούμε την πρώτη ισοδυναμία και θα έχουμε τη γνήσια ισοδύναμη μορφή $[5, -14, 10]$. Τώρα θέλουμε να κάνουμε το απόλυτο του b μικρότερο ή ίσο από το a, από τη δεύτερη ισοδυναμία για $n = 1$ έχουμε $[5, -4, 1]$. Χρησιμοποιούμε πάλι την πρώτη και φτάνουμε στη μορφή $[1, -4, 1]$ και πάλι τη δεύτερη για $n = 2$ και έχουμε $[1, 0, 1]$.

Αφού οι όροι a είναι θετικοί ακέραιοι, μία τέτοια διαδικασία δε μπορεί να συνεχίσει επ' άπειρο χωρίς να φτάσουμε σε μια μορφή Gauss που να ισχύει $|b| \leq a \leq c$.

Μένει να δείξουμε τη δεύτερη συνθήκη της ανηγμένης μορφής, δηλαδή ότι αν $|b| = a$ ή $a = c$ είναι $b \geq 0$.

Αν $b = a$, τότε $b > 0$, αφού $a > 0$.

Αν $b = -a$, τότε από το θεώρημα 3.2.3 για $n = 1$ έχουμε ότι η $[a, -a, c]$ είναι γνήσια ισοδύναμη με την $[a, -a + 2a, a - a + c] = [a, a, c]$ και το νέο b είναι ίσο με το a που είναι θετικός ακέραιος (και η ανισότητα $|b| \leq a \leq c$ συνεχίζει να ισχύει).

Αν $b < 0$ και $a = c$ χρησιμοποιώντας την πρώτη πρόταση του θεωρήματος 3.2.3 φτάνουμε σε μία γνήσια ισοδύναμη μορφή με $0 \leq b \leq a = c$.

□

Θεώρημα 3.2.7:

Δύο ανηγμένες μορφές Gauss δε μπορεί να είναι γνήσια ισοδύναμες.

Απόδειξη:

Έστω ότι οι μορφές $[a, b, c]$ και $[a', b', c']$ είναι ανηγμένες και γνήσια ισοδύναμες, τότε θα υπάρχει πίνακας

$$G = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL_2(\mathbb{Z})$$

τέτοιος ώστε $G * [a, b, c] = [a', b', c']$ και $a' = ar^2 + brs + cs^2$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $a' \leq a$ (αν δεν ήταν, αφού ισχύει η συμμετρικά ιδιότητα θα θεωρούσαμε πίνακα G', ώστε $G' * [a', b', c'] = [a, b, c]$).

Επομένως

$$a(r + \frac{bs}{2a})^2 + (-\frac{D}{4a})s^2 = ar^2 + bsr + \frac{ab^2s^2}{4a^2} + \frac{(4ac - b^2)s^2}{4a} =$$

$$= ar^2 + bsr + \frac{ab^2s^2}{4a^2} + \frac{4acs^2}{4a} - \frac{b^2s^2}{4a} = ar^2 + brs + cs^2 = a' \leq a.$$

Άρα $a(r + \frac{bs}{2a})^2 + (-\frac{D}{4a})s^2 \leq a$, δηλαδή $(-\frac{D}{4a})s^2 \leq a$, τότε $-Ds^2 \leq 4a^2$. Επίσης από το θεώρημα 3.2.4 έχουμε ότι $4a^2 \leq \frac{-4D}{3}$, άρα

$$-Ds^2 \leq \frac{-4D}{3}$$

Οπότε $s = 0, 1$ ή -1. Διακρίνουμε τις ακόλουθες περιπτώσεις:

i)Ας υποθέσουμε ότι $s = 0$. Θα δείξουμε ότι $a' = a$, $b' = b$ και $c' = c$. Από τη σχέση $a(r + \frac{bs}{2a})^2 \leq a$, έχουμε ότι $r^2 \leq 1$. Δηλαδή $r = 0$ ή $r^2 = 1$, το r όμως δε μπορεί να είναι ίσο με το μηδέν, αφού τότε σε συνδιασμό με το ότι το $s = 0$ η ορίζουσα του πίνακα G είναι μηδέν, που δεν ισχύει, αφού $G \in SL_2(\mathbb{Z})$, άρα $r^2 = 1$ και τότε $a' = a$.

Επίσης έχουμε ότι $b' = 2art + bru$. Αφού $G \in SL_2(\mathbb{Z})$ η ορίζουσα του G θα είναι ίση με ένα, δηλαδή $ru = 1$, τότε $b' = 2art + b$ και αυτό συναπάγεται ότι $b' - b = 2art$. Επειδή οι δύο μορφές είναι ανηγμένες, ισχύουν οι ανισότητες $|b| \leq a$ και $|b'| \leq a' = a$, δηλαδή $-a \leq b$ και $b' \leq a$, άρα $-b \leq a$ και $b' \leq a$. Προσθέτοντας τώρα τις δύο ανισότητες κατά μέλη παίρνουμε ότι $b' - b \leq 2a$, άρα $2art \leq 2$ και αυτό συνεπάγεται ότι $rt \leq 1$ με r, t ακεραίους.

Αν το t είναι μηδέν, έχουμε ότι και $b' = b$ (το r δε μπορεί να είναι μηδέν αφού τότε η ορίζουσα του G θα ήταν ίση με μηδέν).

Μένει να εξετάσουμε την περίπτωση που $|rt| = 1$ και $rt < -1$.

Ας υποθέσουμε ότι $rt = 1$ και θα οδηγηθούμε σε άτοπο. Είναι $b' = 2a + b$ και η τριπλή ανισότητα $-a \leq b' \leq a$, μας δίνει ότι $-a \leq 2a + b \leq a$, δηλαδή $-3a \leq b \leq -a$. Όμως $-a \leq b \leq a$, άρα $b = -a < 0$, αλλά τότε $|b| = a$ και από τη συνθήκη ανηγμένης μορφής θα έπρεπε το b να είναι θετικό, εμείς όμως δείξαμε ότι είναι αρνητικό, αντίφαση. Ομοίως εργαζόμαστε και στην περίπτωση που $rt = -1$.

Ας υποθέσουμε τώρα ότι $rt < -1$, άρα $b' - b = 2art < -2a$. Από τις ανισότητες $-a \leq b \leq a$ και $-a \leq -b' \leq a$ έχουμε ότι $-2a \leq b - b' \leq 2a$, αντίφαση.

Τέλος έχουμε $c' = \frac{b'^2 - D}{4a'} = \frac{b^2 - D}{4a} = c$.

ii)Ας υποθέσουμε τώρα ότι $s = \pm 1$, τότε $a' = ar^2 \pm br + c \leq a$, δηλαδή $ar^2 \pm br \leq a - c \leq 0$ (αφού $a \leq c$). Επομένως

$$ar^2 \pm br \leq 0.$$

Αυτό συνεπάγεται ότι $r = 0$ ή $a|r| \leq |b|$. (Αν $r > 0$, η σχέση μας δίνει ότι $0 < ar \leq \pm b$, δηλαδή $a|r| \leq |b|$. Αν $r < 0$, τότε η σχέση μας δίνει ότι $0 < -ar \leq \pm b$, δηλαδή $a|r| \leq |b|$).

-Έστω ότι $r = 0$, τότε $a' = ar^2 + brs + cs^2 = c$. Αφού $c = a' \leq a \leq c$, συνεπάγεται ότι $a = c$, δηλαδή $a' = a = c$. Οπότε από τη δεύτερη συνθήκη της

ανηγμένης μορφής έχουμε ότι $b \geq 0$. Επίσης αν $r = 0$ το $st = -1$ (για να έχουμε $detG = 1$) και τότε $b' = -b + 2csu$. Όμως $b \leq c$ και $b' \leq a' = c$, προσθέτοντας τις δύο ανισότητες έχουμε $b' + b = 2csu$, δηλαδή $2csu \leq 2c$, όμως $c > 0$, άρα $su \leq 1$ με s και u ακεραίους. Αν εργαστούμε όπως στην προηγούμενη περίπτωση που είχαμε $rt \leq 1$ με r, t ακεραίους, θα φτάσουμε στο αποτέλεσμα ότι $su = 0$, όμως $s = \pm 1$, άρα $u = 0$. Συνεπώς $c' = at^2 + btu + cu^2 = at^2$ και επειδή $st = -1$, έχουμε $|t| = 1$. Έπεται λοιπόν ότι $c' = a$, δηλαδή $c' = a = a'$ και τότε από ορισμό της ανηγμένης μορφής έχουμε $b \geq 0$. Έχουμε δηλαδή ότι $b' = -b + 2csu = -b$ και $b, b' \geq 0$, άρα $b' = b = 0$. Τέλος $c' = \frac{b'^2 - D}{4a'} = \frac{b^2 - D}{4a} = c$.

-Αν $r = \pm 1$, τότε από τη σχέση $a|r| \leq |b|$ έχουμε $a \leq |b|$. Όμως επειδή η μορφή είναι ανηγμένη ισχύει ότι $|b| \leq a$. Άρα $a = |b|$, τότε όμως, από τη δεύτερη συνθήκη της ανηγμένης μορφής θα πρέπει $b \geq 0$, άρα τελικα $a = b$.

Επίσης $a' \leq a \Rightarrow ar^2 \pm br + c \leq a \Rightarrow a \pm a + c \leq a$.

Αν $a + a + c \leq a$, τότε $a + c \leq 0$, άτοπο αφού $a, c > 0$.

Αν $a - a + c \leq a$, τότε $c \leq a$, όμως $a \leq c$, άρα $a = c$.

Δηλαδή $a = b = c$, επειδή όμως οι a, b και c είναι ανά δύο πρώτοι μεταξύ τους, θα είναι $a = b = c = 1$. Τότε $D = b^2 - 4ac = 1 - 4 = -3$, που όπως είδαμε σε προηγούμενο παράδειγμα υπάρχει μία μόνο ανηγμένη μορφή Gauss με διακρίνουσα -3.

□

Πρόβλημα:

Να βρεθούν οι ανηγμένες μορφές Gauss με διακρίνουσα $D = -23$.

Λύση:

Έστω $[a, b, c]$ μία τέτοια μορφή, τότε από θεώρημα **3.2.4** $0 < a \leq \sqrt{-\frac{-23}{3}} = 2,7688...$, δηλαδή $a = 1$ ή **2**.

Αν $a = 1$ τότε $b = -1, 0, 1,$ (αφού $|b| \leq a$). Το b δεν μπορεί να είναι ίσο με 0 αφού τότε το $D = -4ac$ δεν θα είναι ισότιμο με $1 \pmod 4$. Επίσης το b δεν μπορεί να είναι ίσο με -1, αφού τότε $|b| = a$ και από τον ορισμό της ανηγμένης μορφής θα έπρεπε $b \geq 0$. Άρα $b = 1$ και τότε $c = \frac{b^2 - D}{4a} = \frac{1+23}{4} = 6$. Πράγματι η μορφή Gauss $[1, 1, 6]$ είναι ανηγμένη.

Αν $a = \pm 2$, τότε όπως πριν έχουμε $b = \pm 1$ (είδαμε ότι το b δε μπορεί να είναι ίσο με 0) και $c = 3$. Οι μορφές $[2, 1, 3]$ και $[2, -1, 3]$ είναι ανηγμένες.

Υπάρχουν λοιπόν τρεις ανηγμένες μορφές και λέμε ότι ο αριθμός κλάσεων για τον -23 είναι 3.

□

Οι μορφές Gauss της μορφής $[a, a, c]$ (με διακρίνουσα D) λέγονται **ειδικές ασαφείς μορφές (special ambiguous forms)**. Στο θεώρημα 3.2.1 είδαμε ότι αν οι διακεκριμένοι πρώτοι διαιρέτες είναι r το πλήθος, τότε υπάρχουν 2^r ειδικές ασαφείς μορφές. Από το θεώρημα 3.2.3 έχουμε ότι οι ειδικές ασαφείς μορφές $[a, a, c]$ και $[4c - a, 4c - a, c]$ είναι γνήσια ισοδύναμες. (Αυτές δεν μπορεί να είναι ίδιες, αν ήταν θα είχαμε $4c - a = a$, δηλαδή $2c = a$, επειδή όμως οι a και c είναι πρώτοι μεταξύ τους θα είναι $c = 1$ και $a = 2$, οπότε $b = 2$, άτοπο αφού ο b είναι περιττός). Στις ειδικές ασαφείς μορφές $[a, a, c]$ ισχύει $a \neq 2c$ και $a < 4c$ (αφού $a^2 - 4ac = D < 0$). Από τα θεωρήματα 3.2.3 και 3.2.5 έπεται ότι η $[a, a, c]$ είναι γνήσια ισοδύναμη με μία ανηγμένη μορφή $[*, *, c]$. Άρα αν δύο μορφές $[a, a, c]$ και $[a', a', c']$ είναι γνήσια ισοδύναμες με την ίδια ανηγμένη μορφή, θα πρέπει $c' = c$ και τότε, αφού

$$a^2 - 4ac = D = a'^2 - 4a'c'$$

έχουμε $(a' - 2c)^2 = (a - 2c)^2$, όπου $a' = a$ ή $4c - a$. Δηλαδή κάθε ειδική ασαφή μορφής $[a, a, c]$ είναι γνήσια ισοδύναμη με ακριβώς μία άλλη ειδική ασαφή μορφή, την $[4c - a, 4c - a, c]$. Για παράδειγμα η $[1, 1, 1,]$ είναι γνήσια ισοδύναμη με την $[3, 3, 1]$, και με καμία άλλη ειδική ασαφή μορφή.

Η σχέση ισοδυναμίας που έχουμε ορίσει (γνήσια ισοδυναμία) χωρίζει τις μορφές Gauss σε κλάσεις ισοδυναμίας. Άρα αφού οι ειδικές ασαφείς μορφές βρίσκονται σε " ισοδύναμα ζευγάρια ", θα βρίσκουμε τις 2^r ειδικές ασαφείς μορφές σε 2^{r-1} κλάσεις. Δηλαδή αν μία κλάση περιέχει την $[a, a, c]$, θα περιέχει και την $[4c - a, 4c - a, c]$ και καμία άλλη ειδική ασαφή μορφή.

Για παράδειγμα, αν $D = -23$ υπάρχουν τρεις κλάσεις ισοδυναμίας, όσες και οι ανηγμένες μορφές, που όπως είδαμε είναι οι $[1, 1, 6]$ και $[2, \pm 1, 3]$. Εδώ το $r = 1$ και οι ειδικές ασαφείς μορφές είναι οι $[1, 1, 6]$ και $[23, 23, 6]$, οι οποίες βρίσκονται στην κλάση που ορίζει η ανηγμένη μορφή $[1, 1, 6]$.

Έστω $[\left[a, b, c\right]]$ η κλάση ισοδυναμίας που περιέχει την μορφή $[a, b, c]$. Μία κλάση ισοδυναμίας που περιέχει μία ειδική ασαφή μορφή θα λέγεται ειδική ασαφής κλάση. Από τα παραπάνω έπεται ότι υπάρχουν 2^{r-1} ειδικές ασαφείς κλάσεις (όπου r το πλήθος των διακεκριμένων πρώτων διαιρετών του D).

3.3 Τριαδικές τετραγωνικές μορφές πινάκων

Για να αποδείξουμε ότι κάθε θετικός ακέραιος γράφεται σαν άθροισμα τριών τρίγωνων αριθμών, θα χρειαστεί να μελετήσουμε τρία επί τρία πίνακες.

Έστω $M = \begin{bmatrix} a & b & c \\ d & e & f \\ h & i & j \end{bmatrix}$ ένας αντιστρέψιμος τρία επί τρία πίνακας. Ορίζουμε

$$\overline{M} = \begin{bmatrix} ej - fi & fh - dj & di - eh \\ ci - bj & aj - ch & bh - ai \\ bf - ce & cd - af & ae - bd \end{bmatrix}.$$

Τότε

$$M \cdot \overline{M}^T = (detM)I.$$

Απόδειξη:

Το στοιχείο της πρώτης γραμμής και πρώτης στήλης είναι ίσο με $a(ej - fi) - b(dj - fi) + c(di - eh)$, που είναι ίσο με την ορίζουσα $detM$, αν τη δούμε ανεπτυγμένη ως προς την πρώτη στήλη.

Το στοιχείο της πρώτης γραμμής και δεύτερης στήλης είναι ίσο με $a(ci - bj) + b(aj - ch) + c(bh - ai) = aci - abj + abj - bch + bch - aci = 0$.

Ομοίως και για τα υπόλοιπα στοιχεία.

□

Επομένως

$$\overline{M}^T = (detM)M^{-1}$$

και

$$det\overline{M} = |(detM)M^{-1}| = (detM)^3 \cdot det(M^{-1}) = (detM)^3 \cdot \frac{1}{detM} = (detM)^2$$

Επίσης

$$M\overline{M}^T = (detM)I \Rightarrow$$

$$(M\overline{M}^T)^T = ((detM)I)^T \Rightarrow$$

$$\overline{M}M^T = (detM)I \Rightarrow$$

$$\overline{M} = (detM)(M^T)^{-1} \Rightarrow$$

$$\overline{M} = (detM)(M^{-1})^T \Rightarrow$$

$$\overline{\overline{M}} = (detM^2)\overline{M^{-1}}^T \Rightarrow$$

$$\overline{\overline{M}} = (detM)^2(detM)^{-1}M = (detM)M.$$

Στις παραπάνω ισοδυναμίες χρησιμοποιήσαμε τις σχέσεις:

$i)$ $\overline{MM'} = \overline{M} \cdot \overline{M'}$

$ii)$ $\overline{M^T} = \overline{M}^T$

$iii)$ $\overline{sM} = s^2\overline{M}$

$iv)$ $(detM)^{-1}M = \overline{M^{-1}}^T$

Τις οποίες και θα αποδείξουμε:

$i)$

$$\overline{MM'} = \overline{\begin{bmatrix} a & b & c \\ d & e & f \\ h & i & j \end{bmatrix} \cdot \begin{bmatrix} a' & b' & c' \\ d' & e' & f' \\ h' & i' & j' \end{bmatrix}} =$$

$$\overline{\begin{bmatrix} aa'+bd'+ch' & ab'+be'+ci' & ac'+bf'+cj' \\ a'd+ed'+fh' & db'+ee'+fi' & dc'+ef'+fj' \\ ha'+id'+jh' & hb'+ie'+ji' & c'h+f'i+jj' \end{bmatrix}}$$

Το στοιχείο της πρώτης γραμμής και της πρώτης στήλη θα είναι το:

$(db'+ee'+fi')(c'h+f'i+jj')+(dc'+ef'+fj')(hb'+ie'+ji') = db'c'h+db'f'i+db'jj'+ee'c'h+ee'f'i+ee'jj'+fi'c'h+fi'f'i+fi'jj'-dc'hb'-dc'ie'-dc'ji'-ef'hb'-ef'ie'-ef'ji'-fj'hb'-fj'ie'-fj'ji' = db'f'i+db'jj'+ee'c'h+ee'jj'+fi'c'h+fi'f'i-dc'ie'-dc'ji'-ef'hb'-ef'ji'-fj'hb'-fj'ie'.$

Το δεύτερο μέλος της ισότητας μας δίνει:

$$\overline{M}\cdot\overline{M'}=\begin{bmatrix} ej-fi & fh-dj & di-eh \\ ci-bj & aj-ch & bh-ai \\ bf-ce & cd-af & ae-bd \end{bmatrix}\cdot\begin{bmatrix} e'j'-f'i' & f'h'-d'j' & d'i'-e'h' \\ c'i'-b'j' & a'j'-c'h' & b'h'-a'i' \\ b'f'-c'e' & c'd'-a'f' & a'e'-b'd' \end{bmatrix}$$

Τώρα το στοιχείο της πρώτης γραμμής και της πρώτης στήλη είναι το:

$(ej-fi)(e'j'-f'i')+(fh-dj)(c'i'-b'j')+(di-eh)(b'f'-c'e')=eje'j'-ejf'i'-fie'j'+fif'i'+fhc'i'-fhb'j'-djc'i'+djb'j'+dib'f'-dic'e'-ehb'f'+ehc'e'$.

Παρατηρώντας τα δύο αθροίσματα βλέπουμε ότι είναι τα ίδια. Όμοια εργαζόμαστε για τα άλλα στοιχεία του πίνακα.

ii)

$$\overline{M^T}=\overline{\begin{bmatrix} a & d & h \\ b & e & i \\ c & f & j \end{bmatrix}}=\begin{bmatrix} ej-fi & ci-bj & bf-ce \\ fh-dj & aj-ch & cd-af \\ di-eh & bh-ai & ae-bd \end{bmatrix}=$$

$$\begin{bmatrix} ej-fi & fh-dj & di-eh \\ ci-bj & aj-ch & bh-ai \\ bf-ce & cd-af & ae-bd \end{bmatrix}^T=\overline{M}^T.$$

iii)

$$\overline{sM}=\overline{\begin{bmatrix} sa & sb & sc \\ sd & se & sf \\ sh & si & sj \end{bmatrix}}=\begin{bmatrix} s^2ej-s^2fi & s^2fh-s^2dj & s^2di-s^2eh \\ s^2ci-s^2bj & s^2aj-s^2ch & s^2bh-s^2ai \\ s^2bf-s^2ce & s^2cd-s^2af & s^2ae-s^2bd \end{bmatrix}=$$

$$=s^2\begin{bmatrix} ej-fi & fh-dj & di-eh \\ ci-bj & aj-ch & bh-ai \\ bf-ce & cd-af & ae-bd \end{bmatrix}=s^2\overline{M}$$

iv) Έχουμε ότι $\overline{M}^T=(detM)M^{-1}$, αν θέσουμε όπου M το M^{-1}, θα έχουμε $\overline{M^{-1}}^T=(det(M^{-1}))M=(detM)^{-1}M$

□

Αν έχουμε τον πίνακα $M=\begin{bmatrix} 1 & 0 & 0 \\ 0 & e & f \\ 0 & f & j \end{bmatrix}$, τότε $\overline{M}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & j & -f \\ 0 & -f & e \end{bmatrix}$

και αν

$$F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix},$$

με $detF \neq 0$, τότε

$$\overline{F} = \begin{bmatrix} bc - \frac{v^2}{4} & \frac{vw}{4} - \frac{cu}{2} & \frac{uv}{4} - \frac{bw}{2} \\ \frac{vw}{4} - \frac{cu}{2} & ac - \frac{w^2}{4} & \frac{uw}{4} - \frac{av}{2} \\ \frac{uv}{4} - \frac{bw}{2} & \frac{uw}{4} - \frac{av}{2} & ab - \frac{u^2}{4} \end{bmatrix}.$$

Αν $a, b, c, u, v, w \in \mathbb{Z}$, τότε πίνακες της μορφής του F θα λέγονται πίνακες **ακέραιας τριαδικής τετραγωνικής μορφής (integral ternary quadratic form matrices)** ή για συντομία απλά **τριαδικοί (ternary)**.

Με τον συμβολισμό $GL_3(\mathbb{Z})$ θα εννοούμε την πολλαπλασιαστική ομάδα των τρία επί τρία πινάκων με ακέραια στοιχεία και ορίζουσα ± 1.

Αν $G \in GL_3(\mathbb{Z})$ τότε και $\overline{G} \in GL_3(\mathbb{Z})$ (να θυμηθούμε ότι $det\overline{G} = (detG)^2$).

Αν ο F είναι τριαδικός το ίδιο θα ισχύει και για τον GFG^T. Θα λέμε ότι δύο τριαδικοί πίνακες F και F' είναι ισοδύναμοι αν υπάρχει κάποιος πίνακας $G \in GL_3(\mathbb{Z})$ τέτοιος ώστε $F' = GFG^T$. Η σχέση που ορίσαμε είναι σχέση ισοδυναμίας.

Έστω πίνακας $G \in GL_3(\mathbb{Z})$ της μορφής

$$\begin{bmatrix} r & s & 0 \\ t & q & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

με την "πάνω αριστερά ορίζουσα" $rq - st$, ίση με 1, τότε ο G θα λέγεται top left heavy πίνακας. Το σύνολο των top left heavy πινάκων αποτελεί υποομάδα της $GL_3(\mathbb{Z})$.

(Έυκολα βλέπουμε ότι η προσεταιριστική ιδιότητα ισχύει, το ουδέτερο στοιχείο είναι ο I και ο αντίστροφος του G υπάρχει, αφού $detG = 1 \neq 0$ και είναι ο $\begin{bmatrix} q & -s & 0 \\ -t & r & 0 \\ 0 & 0 & 1 \end{bmatrix}$, ο οποίος ανήκει στην $GL_3(\mathbb{Z})$).

Μία παρατήρηση που θα μας φανεί χρήσιμη είναι ότι αν ο $G = \begin{bmatrix} r & s & 0 \\ t & q & 0 \\ 0 & 0 & 1 \end{bmatrix}$

είναι top left heavy πίνακας, τότε και ο $\overline{G} = \begin{bmatrix} q & -t & 0 \\ s & r & 0 \\ 0 & 0 & qr-st \end{bmatrix} = \begin{bmatrix} q & -t & 0 \\ s & r & 0 \\ 0 & 0 & 1 \end{bmatrix}$ είναι top left heavy πίνακας.

Όμοια ορίζουμε τους bottom right heavy πίνακες, να είναι της μορφής

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & r & s \\ 0 & t & q \end{bmatrix}$$

με την "κάτω δεξιά ορίζουσα" $rq - st$ να είναι ίση με 1, επίσης αποτελούν υποομάδα της $GL_3(\mathbb{Z})$. Πάλι έχουμε ότι αν ο G είναι bottom right heavy πίνακας, το ίδιο θα ισχύει και για τον $\overline{G}$.

Αν ο F είναι τριαδικός και ο G είναι top left heavy πίνακας, τότε ο GFG^T έχει τη μορφή:

$$\begin{bmatrix} \begin{bmatrix} r & s \\ t & q \end{bmatrix} \begin{bmatrix} a & \frac{u}{2} \\ \frac{u}{2} & a \end{bmatrix} \begin{bmatrix} r & t \\ s & q \end{bmatrix} & * \\ * & c \end{bmatrix}$$

με τον κάτω δεξιά όρο c του GFG^T ίδιο με αυτό του F.

Επίσης η πάνω αριστερά δύο επί δύο ορίζουσα των GFG^T και F παραμένει ίδια, αφού στον F είναι

$$det \begin{bmatrix} a & \frac{u}{2} \\ \frac{u}{2} & a \end{bmatrix} = ab - \frac{u^4}{4}$$

και στον GFG^T είναι $det(\begin{bmatrix} r & s \\ t & q \end{bmatrix} \begin{bmatrix} a & \frac{u}{2} \\ \frac{u}{2} & a \end{bmatrix} \begin{bmatrix} r & t \\ s & q \end{bmatrix}) = (rq-st)\cdot(ab-\frac{u^4}{4})\cdot(rq-st) = 1 \cdot (ab - \frac{u^4}{4}) \cdot 1 = ab - \frac{u^4}{4}$.

Αντίστοιχα αν ο G είναι bottom right heavy πίνακας τότε ο GFG^T έχει τη μορφή:

$$\begin{bmatrix} a & * \\ * & \begin{bmatrix} r & s \\ t & q \end{bmatrix} \begin{bmatrix} b & \frac{v}{2} \\ \frac{v}{2} & c \end{bmatrix} \begin{bmatrix} r & t \\ s & q \end{bmatrix} \end{bmatrix}$$

με τον πάνω αριστερά όρο a, ίδιο στους F και GFG^T. Επίσης η κάτω δεξιά δύο επί δύο ορίζουσα είναι ίδια στους δύο πίνακες.

Με την βοήθεια των δύο θεωρημάτων που ακολουθούν θα μπορέσουμε να χρησιμοποιήσουμε τους top left heavy και bottom right heavy πίνακες για να φτάσουμε

τους τριαδικούς πίνακες σε ανηγμένες μορφές, με τρόπο όμοιο όπως φτάναμε σε ανηγμένη μορφή μία δοσμένη μορφή Gauss.

Θεώρημα 3.3.1:

Αν

$$F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

είναι τριαδικός πίνακας και

$$G = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

τότε

$$GFG^T = \begin{bmatrix} b & -\frac{u}{2} & * \\ -\frac{u}{2} & a & * \\ * & * & c \end{bmatrix}$$

όπου τα * είναι ακέραιοι ή μισά ακεραίων. Επιπλέον, αν

$$G' = \begin{bmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

τότε

$$G'FG'^T = \begin{bmatrix} a & an + \frac{u}{2} & * \\ an + \frac{u}{2} & an^2 + un + b & * \\ * & * & c \end{bmatrix}$$

Να σημειώσουμε ότι $a(an^2 + un + b) - (an + \frac{u}{2})^2 = ab - (\frac{u}{2})^2$ (δηλαδή η πάνω αριστερά δύο επί δύο ορίζουσα παραμένει ίδια) και ότι αν $a \neq 0$ και n ο κοντινότερος ακέραιος στο $\frac{-u}{2a}$ τότε $|2an + u| \leq |a|$ (δηλαδή το νέο u είναι απολύτως μικρότερο του $|a|$).

Απόδειξη:

$$GFG^T = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} \frac{u}{2} & b & \frac{v}{2} \\ -a & -\frac{u}{2} & -\frac{w}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} b & -\frac{u}{2} & \frac{v}{2} \\ -\frac{u}{2} & a & -\frac{w}{2} \\ \frac{v}{2} & -\frac{w}{2} & c \end{bmatrix}$$

και

$$G'FG'^T = \begin{bmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix} \cdot \begin{bmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$\begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ an + \frac{u}{2} & \frac{un}{2} + b & \frac{nw}{2} + \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix} \cdot \begin{bmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a & an + \frac{u}{2} & \frac{w}{2} \\ an + \frac{u}{2} & an^2 + un + b & \frac{nw}{2} + \frac{v}{2} \\ \frac{w}{2} & \frac{nw}{2} + \frac{v}{2} & c \end{bmatrix}$$

□

Θεώρημα 3.3.2:

Αν

$$F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

είναι τριαδικός πίνακας και

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

τότε

$$GFG^T = \begin{bmatrix} a & * & * \\ * & c & -\frac{v}{2} \\ * & -\frac{v}{2} & b \end{bmatrix}$$

όπου τα * είναι ακέραιοι ή μισά ακεραίων. Επιπλέον, αν

$$G' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{bmatrix}$$

τότε

$$G'FG'^T = \begin{bmatrix} a & * & * \\ * & cn^2+vn+b & cn+\frac{v}{2} \\ * & cn+\frac{v}{2} & c \end{bmatrix}$$

Να σημειώσουμε ότι η κάτω δεξιά δύο έπι δύο ορίζουσα των F ($bc-\frac{v^2}{4}$) και $G'FG'^T$ ($c(cn^2+vn+b)-(cn+\frac{v}{2})^2 = c^2n^2+cvn+cb-c^2n^2-\frac{v^2}{4}-cvn = cb-\frac{v^2}{4}$) παραμένει ίδια. Επίσης αν ο n είναι ο κοντινότερος ακέραιος στο $-\frac{v}{2c}$, τότε $|2cn+v| \leq |c|$ (δηλαδή το νέο v είναι απόλυτα μικρότερο ίσο του $|c|$).

Η απόδειξη είναι όμοια με την προηγούμενη.

Θεώρημα 3.3.3:

Έστω

$$F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

τριαδικός πίνακας, τότε υπάρχει ένας top left heavy πίνακας G τέτοιος ώστε:

(1) Η πάνω αριστερά δύο επί δύο ορίζουσα j του F να είναι ίση με αυτή του GFG^T.

(2) Η απόλυτη τιμή του πάνω αριστερά όρου του GFG^T να είναι $\leq \sqrt{\frac{4|j|}{3}}$.

(3) Ο κάτω δεξιά όρος του $\overline{F}$(δηλαδή το $j = ab-\frac{u^2}{4}$) να είναι ίσος με τον κάτω δεξιά όρο του πίνακα $\overline{GFG^T}$.

Απόδειξη:

Είδαμε από το θεώρημα 3.3.1 ότι μπορούμε να φτάσουμε σε ισοδύναμο πίνακα του F (με τη βοήθεια του $\begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$) που να ισχύει $|a| \leq |b|$ (ενώ το u αλλάζει μόνο πρόσημο, δηλαδή το $|u|$ παραμένει σταθερό). Μπορούμε επίσης να φτάσουμε σε ισοδύναμο πίνακα του F με $|u| \leq |a|$ (με τη βοήθεια του πίνακα $\begin{bmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, για n τον κοντινότερο ακέραιο στο $\frac{-u}{2a}$). Όμοια με τη λογική του θεωρήματος 3.2.6, μπορούμε να φτάσουμε σε έναν ισοδύναμο πίνακα του F ώστε να ισχύει

$$|u| \leq |a| \leq |b|.$$

Δηλαδή υπάρχει πίνακας G τέτοιος ώστε για τον GFG^T να ισχύει $|u| \leq |a| \leq |b|$.

Τότε όπως σημειώσαμε στο θεώρημα 3.3.1 κατά την μετάβαση του F στον MFM^T (με $M = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ ή $\begin{bmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$), η πάνω αριστερά δύο επί δύο ορίζουσα δεν αλλάζει. Άρα και κατά τη μετάβαση του F στον GFG^T (με G ένα γινόμενο πινάκων Μ) η πάνω αριστερά δύο επί δύο ορίζουσα δε θα αλλάζει. Επομένως και ο κάτω δεξιά όρος του $\overline{F}$ είναι ίδιος με αυτόν του $\overline{GFG^T}$ (αν έχουμε έναν πίνακα Α, τότε από τον ορισμό του $\overline{A}$ ο κάτω δεξιά όρος του $\overline{A}$ είναι ίσος με την πάνω αριστερά ορίζουσα του Α). Μένει να αποδείξουμε το (2).

Αν $a = 0$, σταματάμε εδώ αφού $0 \leq \sqrt{\frac{4|j|}{3}}$. Έστω λοιπόν ότι $a \neq 0$. Έχουμε ότι

$$|u| \leq |a| \leq |b|,$$

άρα

$$4a^2 \leq u^2 - u^2 + 4|ab| \leq a^2 - u^2 + 4|ab|,$$

δηλαδή

$$3a^2 \leq -u^2 + 4|ab|.$$

Αν $ab \geq 0$, έχουμε $3a^2 \leq -u^2 + 4ab$, δηλαδή $a^2 \leq \frac{4}{3}(ab - \frac{u^2}{4})$. Έχουμε $|a|, |b| \geq u$, άρα $|ab| \geq u^2$, και αφού $ab \geq 0$ είναι $ab - \frac{u^2}{4} \geq 0$, τότε $a \leq \sqrt{\frac{4}{3}(ab - \frac{u^2}{4})}$. Όμως η πάνω αριστερά ορίζουσα του GFG^T (η οποία είναι η $ab - \frac{u^2}{4}$) είναι ίση με αυτή του F (δηλαδή τη j), άρα $j = ab - \frac{u^2}{4}$, τότε $a \leq \sqrt{\frac{4}{3}j} = \sqrt{\frac{4}{3}|j|}$ (αφού $j = ab - \frac{u^2}{4} \geq 0$).

Αν $ab < 0$, έχουμε

$$3a^2 \leq -4ab - u^2 \leq -4ab + u^2.$$

Δηλαδή

$$a^2 \leq -\frac{4}{3}(ab - \frac{u^2}{4}).$$

Όμως $ab - \frac{u^2}{4} < 0$, άρα $-\frac{4}{3}(ab - \frac{u^2}{4}) > 0$ και η παραπάνω σχέση μας δίνει $a \leq \sqrt{-\frac{4}{3}(ab - \frac{u^2}{4})}$. Επίσης $j = ab - \frac{u^2}{4} < 0$, άρα $a \leq \sqrt{\frac{4}{3}|j|}$.

□

Θεώρημα 3.3.4:

Έστω

$$F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

τριαδικός πίνακας, τότε υπάρχει ένας bottom right heavy πίνακας G τέτοιος ώστε:

(1) Η κάτω δεξιά δύο επί δύο ορίζουσα k του $\overline{F}$ να είναι ίση με αυτή του $H\overline{F}H^T$.

(2) Η απόλυτη τιμή του κάτω δεξιά όρου του $H\overline{F}H^T$ να είναι $\leq \sqrt{\frac{4|k|}{3}}$.

(3) Ο πάνω αριστερά όρος του $\overline{H}F\overline{H}^T$ να είναι ίσος με αυτόν του F (ο όρος αυτός είναι ο $\frac{k}{detF}$).

Απόδειξη:

Έχουμε $F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$ τριαδικός πίνακας, τότε

$$\overline{F} = \begin{bmatrix} bc - \frac{v^2}{4} & \frac{vw}{4} - \frac{cu}{2} & \frac{uv}{4} - \frac{bw}{2} \\ \frac{vw}{4} - \frac{cu}{2} & ac - \frac{w^2}{4} & \frac{uw}{4} - \frac{av}{2} \\ \frac{uv}{4} - \frac{bw}{2} & \frac{uw}{4} - \frac{av}{2} & ab - \frac{u^2}{4} \end{bmatrix}.$$

Έστω ότι ο $\overline{F}$ είναι τριαδικός. Από το θεώρημα 3.3.2 και όπως προηγουμένως, υπάρχει ένας bottom right heavy πίνακας H τέτοιος ώστε για τον $H\overline{F}H^T$ να ισχύει

$$|v| \leq |c| \leq |b|.$$

(1) Από το θεώρημα 3.3.2 είδαμε ότι κάτα την πράξη $H\overline{F}H^T$ με H bottom right heavy πίνακα, η τιμή της κάτω δεξιάς ορίζουσας του $\overline{F}$ και του $H\overline{F}H^T$ δεν αλλάζει.

(2) Με τη βοήθεια της σχέσης $|v| \leq |c| \leq |b|$, έχουμε:

$$4c^2 \leq v^2 - v^2 + 4|cb| \leq c^2 - v^2 + |4cb|$$

δηλαδή

$$3c^2 \leq -v^2 + |4cb|.$$

Έστω $cb \geq 0$, τότε $3c^2 \leq -v^2 + 4cb$, δηλαδή

$$c^2 \leq \frac{4}{3}(bc - \frac{v^2}{4}).$$

Έχουμε ότι $|b|, |c| \geq |\frac{v}{2}|$, άρα $|bc| \geq \frac{v^2}{4}$ και επειδή $cb \geq 0$ έπεται ότι $bc \geq \frac{v^2}{4}$.

Άρα

$$c \leq \sqrt{\frac{4}{3}(bc - \frac{v^2}{4})}.$$

Όμως $k = bc - \frac{v^2}{4} \geq 0$, άρα

$$c \leq \sqrt{\frac{4}{3}|k|}.$$

Όμοια για $bc < 0$.

(3) Ο H είναι bottom right heavy πίνακας, όπως είδαμε το ίδιο θα ισχύει και για τον $\overline{H}$ και τότε ο F και ο $\overline{H}F\overline{H}^T$ έχουν το ίδιο πάνω αριστερά στοιχείο.

(Ας θυμηθούμε ότι αν ο G είναι bottom right heavy πίνακας τότε ο GFG^T έχει τη μορφή:

$$\begin{bmatrix} a & & * & \\ & \begin{bmatrix} r & s \\ t & q \end{bmatrix} & \begin{bmatrix} b & \frac{v}{2} \\ \frac{v}{2} & c \end{bmatrix} & \begin{bmatrix} r & t \\ s & q \end{bmatrix} \\ * & & & \end{bmatrix}$$

με τον πάνω αριστερά όρο a, ίδιο στους πίνακες F και GFG^T).

Ποιό είναι όμως αυτό το στοιχείο;

Ονομάσαμε k την κάτω δεξιά δύο επί δύο ορίζουσα του $\overline{F}$, η οποία είναι ίδια με αυτή του $H\overline{F}H^T$.

Το πάνω αριστερά στοιχείο $\overline{H\overline{F}H^T}$ είναι αυτή η ορίζουσα k.

Όμως

$$\overline{H\overline{F}H^T} = \overline{H} \cdot \overline{\overline{F}} \cdot \overline{H}^T = detF \cdot \overline{H}F\overline{H}^T$$

άρα το πάνω αριστερά στοιχείο του $\overline{H}F\overline{H}^T$ είναι το $\frac{k}{detF}$.

Έστω ότι ο πίνακας $\overline{F}$ δεν είναι τριαδικός. Όλοι οι όροι του $4\overline{F}$ είναι ακέραιοι, άρα είναι τριαδικός και για τον $2F$ ισχύει το θεώρημα (ο πίνακας $2F$ είναι τριαδικός

και αποδείξαμε το θεώρημα στην περίπτωση που και ο $\overline{2F} = 4\overline{F}$ είναι τριαδικός πίνακας). Θα δείξουμε τώρα ότι το θεώρημα θα ισχύει και για τον F.

(1) Έχουμε ότι η κάτω δεξιά ορίζουσα του $4\overline{F}$ είναι ίση με την αντίστοιχη του $4H\overline{F}H^T$ (το θεώρημα ισχύει για τον $2F$) . Όμως η κάτω δεξιά ορίζουσα του $4\overline{F}$ είναι τέσσερις φορές η κάτω δεξιά ορίζουσα του $\overline{F}$ και επίσης η κάτω δεξιά ορίζουσα του $4H\overline{F}H^T$ είναι τέσσερις φορές η κάτω δεξιά ορίζουσα του $H\overline{F}H^T$, άρα και η κάτω δεξιά ορίζουσα του $\overline{F}$ είναι ίση με την αντίστοιχη του $H\overline{F}H^T$.

(2) Αν c ο κάτω δεξιά όρος του $H\overline{F}H^T$, τότε ο αντίστοιχος του $4H\overline{F}H^T$ θα είναι ο $4c$. Δείξαμε ότι το θεώρημα ισχύει για τον $2F$, δηλ $4|c| \leq \sqrt{\frac{4|k|}{3}}$, τότε όμως $|c| \leq 4|c| \leq \sqrt{\frac{4|k|}{3}}$.

(3) Η απόδειξη του τρία είναι ίδια με πριν.

□

Έστω

$$F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

τριαδικός πίνακας. Ξεκινώντας με την F θα φτιάξουμε μια ακολουθία F_1,F_2,F_3,... από τριαδικούς πίνακες, ισοδύναμους με την F (άρα η διακρίνουσα D είναι κοινή για τους πίνακες τις ακολουθίας). Το a_n θα συμβολίζει τον πάνω αριστερά όρο του πίνακα F_n, ενώ το j_n θα συμβολίζει την δύο επί δύο πάνω αριστερά ορίζουσα του F_n, το οποίο είναι και το κάτω δεξιά στοιχείο c_n του $\overline{F_n}$.

Με k_n θα συμβολίζουμε την κάτω δεξιά ορίζουσα του $\overline{F_n}$, οπότε θα ισχύει $k_n = a_n D$, όπου D η διακρίνουσα του F_n (και των άλλων πινάκων της ακολουθίας).

$$(k_n = (ac - \frac{w^2}{4})(ab - \frac{u^2}{4}) - (\frac{uw}{4} - \frac{av}{2})^2$$

$$= a^2bc - \frac{acu^2}{4} - \frac{abw^2}{4} + \frac{w^2u^2}{16} - \frac{w^2u^2}{16} - \frac{a^2v^2}{4} + \frac{avuw}{4} =$$

$$= a(abc - \frac{cu^2}{4} - \frac{bw^2}{4} - \frac{av^2}{4} + \frac{vuw}{4}) =$$

$$= a(a(bc - \frac{v^2}{4}) - \frac{u}{2}(\frac{uc}{2} - \frac{vw}{4}) + \frac{w}{2}(\frac{uv}{4} - \frac{bw}{2})) =$$

$$= a(a \cdot \begin{bmatrix} b & \frac{v}{2} \\ \frac{v}{2} & c \end{bmatrix} - \frac{u}{2} \cdot \begin{bmatrix} \frac{u}{2} & \frac{v}{2} \\ \frac{w}{2} & c \end{bmatrix} + \frac{w}{2} \cdot \begin{bmatrix} \frac{u}{2} & b \\ \frac{w}{2} & \frac{v}{2} \end{bmatrix}) =$$

$$= a \cdot detF = a_n \cdot D)$$

Αν $|a| \leq \sqrt{\frac{4|j|}{3}}$, όπου $j = ab - \frac{u^2}{4}$, θέτουμε $F_1 = F$.

Αν όχι, θεωρούμε τον πίνακα G όπως στο θεώρημα 3.3.3 και θέτουμε $F_1 = GFG^T$, τώρα αν a_1 ο πάνω αριστερά όρος του F_1, έχουμε $|a_1| \leq \sqrt{\frac{4|j|}{3}}$.

Αν c_1 ο κάτω δεξιά όρος του $\overline{F_1}$ και c ο κάτω δεξιά όρος του $\overline{F}$, τότε $c_1 = c$ και οι δύο ίσοι με j (αν $F_1 = F$ προφανώς ισχύει, αν $F_1 = GFG^T$ ισχύει από το θεώρημα 3.3.3 (3)).

Έστω k_1 η κάτω δεξιά ορίζουσα του F_1. Αν $|c_1| \leq \sqrt{\frac{4|k_1|}{3}}$, σταματάμε τη διαδικασία. Διαφορετικά θεωρούμε πίνακα H σαν αυτό του θεωρήματος 3.3.4 και θέτουμε $F_2 = \overline{H}F_1\overline{H}^T$. Τώρα αν ο c_2 ο κάτω δεξιά όρος του $H\overline{F_1}H^T$, έχουμε

$$|c_2| \leq \sqrt{\frac{4|k_1|}{3}} \leq |c_1|.$$

Αν a_2 ο πάνω αριστερά όρος του F_2, τότε $a_2 = a_1$ (από θεώρημα 3.3.4). Να σημειώσουμε ότι $\overline{F_2} = H\overline{F_1}H^T$ ($\overline{F_2} = \overline{\overline{H}F_1\overline{H}^T} = \overline{\overline{H}} \cdot \overline{F_1} \cdot \overline{\overline{H^T}}$, όμως $\overline{\overline{H}} = H$ (αφού ο H είναι bottom right heavy πίνακας θα ανήκει στο $SL_2(\mathbb{Z})$, άρα $detH = 1$, τότε από τη σχέση $\overline{\overline{M}} = detM \cdot M$ έχουμε $\overline{\overline{H}} = H$)).

Έστω j_2 η πάνω αριστερά ορίζουσα του F_2. Αν $|a_1| \leq \sqrt{\frac{4|j_2|}{3}}$ σταματάμε τη διαδικασία. Διαφορετικά έστω πίνακας G όπως στο θεώρημα 3.3.3 και θέτουμε $F_3 = GF_2G^T$, τότε αν a_3 ο πάνω αριστερά όρος του F_3, έχουμε

$$|a_3| \leq \sqrt{\frac{4|j_2|}{3}} < |a_2|.$$

Με τον κάτω δεξιά όρο του $\overline{F_3}$ ίσο με αυτόν του $\overline{F_2}$, δηλαδή $c_3 = c_2$.

Συνεχίζοντας αυτή τη διαδικασία κατασκευάζουμε μία ακολουθία από ισοδύναμους τριαδικούς πίνακες, F,F_1,F_2,F_3,... με

$$|a_1| = |a_2| > |a_3| = |a_4| > ...$$

και

$$|c| = |c_1| > |c_2| = |c_3| > |c_4| = ...$$

Η διαδικασία αυτή κάποια στιγμή πρέπει να σταματήσει, αφού τα a είναι ακέραιοι και τα c μισά ακεραίων. Άρα για κάποιο n θα έχουμε $|a_n| \leq \sqrt{\frac{4|j_n|}{3}}$ και $|c_n| \leq \sqrt{\frac{4|k_n|}{3}}$.

Άρα κάθε τριαδικός πίνακας F είναι ισοδύναμος με έναν τριαδικό πίνακα με

$$|a| \leq \sqrt{\frac{|u^2 - 4ab|}{3}}$$

και αν D η ορίζουσα του F, ισχύει

$$|c| = |ab - \frac{u^2}{4}| \leq \sqrt{\frac{4|(ac - \frac{w^2}{4})(ab - \frac{u^2}{4}) - (\frac{uw}{4} - \frac{av}{2})^2|}{3}} \leq \sqrt{\frac{4|aD|}{3}}.$$

Έπεται το ακόλουθο θεώρημα

Θεώρημα 3.3.5:

Κάθε τριαδικός πίνακας F είναι ισοδύναμος με έναν τριαδικό πίνακα

$$F = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

τέτοιο ώστε

$$|a| \leq \sqrt{\frac{|u^2 - 4ab|}{3}} \text{ και } |u^2 - 4ab| \leq 8\sqrt{\frac{|aD|}{3}}$$

και συνεπάγεται ότι $|a| \leq \frac{4}{3}\sqrt[3]{|D|}$, όπου D η ορίζουσα του F.

Απόδειξη:

$3a^2 \leq 8\sqrt{\frac{|aD|}{3}}$, άρα $9a^4 \leq 64\frac{|aD|}{3}$.

□

Παράδειγμα:

Ας θεωρήσουμε τον πίνακα

$$F = \begin{bmatrix} 3 & 2 & -1 \\ 2 & 32 & -4 \\ -1 & -4 & 7 \end{bmatrix},$$

τότε

$$\overline{F} = \begin{bmatrix} 208 & -10 & 24 \\ -10 & 20 & 10 \\ 24 & 10 & 92 \end{bmatrix}.$$

Έχουμε $a_1 = 3$ και $j_1 = 3 \cdot 32 - 2 \cdot 2 = 92$, ισχύει ότι $|a_1| \leq \sqrt{\frac{4|j_1|}{3}}$ και θέτουμε $F = F_1$, με $c_1 = 92$.

Επίσης $k_1 = 20 \cdot 92 - 10 \cdot 10 = 1740$ και $|c_1| = 92 > \sqrt{\frac{4|k_1|}{3}} \simeq 48,1$, δεν ισχύει η δεύτερη ανισότητα και σύμφωνα με την παραπάνω διαδικασία πρέπει να βρούμε τον πίνακα H όπως στο θεώρημα 3.3.4 και να θέσουμε $F_2 = \overline{H} F_1 \overline{H}^T$. Από το θεώρημα 3.3.4, αν c_2 ο κάτω δεξιά όρος του $\overline{H} F_1 \overline{H}^T$, θα έχουμε

$$|c_2| \leq \sqrt{\frac{4|k_1|}{3}} < |c_1|.$$

Τώρα θα υπολογίσουμε τον H. Είδαμε στην απόδειξη του θεωρήματος 3.3.4 ότι ο ζητούμενος πίνακας H, είναι ένας ισοδύναμος του

$$\overline{F} = \begin{bmatrix} 208 & -10 & 24 \\ -10 & 20 & 10 \\ 24 & 10 & 92 \end{bmatrix}$$

τέτοιος ώστε να ισχύει η ανισότητα $|v| \leq |c| \leq |b|$.

Στον $\overline{F}$ έχουμε $v = 20, c = 92, b = 20$ και δεν ισχύει η τριπλή ανισότητα. Αρχικά θα βρούμε έναν ισοδύναμό του με $|c| \leq |b|$.

Σύμφωνα με το θεώρημα 3.3.2 θεωρούμε τον πίνακα

$$G_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

και έχουμε

$$G_1\overline{F}G_1^T = \begin{bmatrix} 208 & 24 & 10 \\ 24 & 92 & -10 \\ 10 & -10 & 20 \end{bmatrix}$$

τώρα $v = -20, c = 20, b = 92$ και η τριπλή ανισότητα $|v| \leq |c| \leq |b|$ ισχύει. Έχουμε δηλαδή $H = G_1$ και θέτουμε

$$F_2 = \overline{H}F_1\overline{H}^T = \begin{bmatrix} 3 & -1 & -2 \\ -1 & 7 & 4 \\ -2 & 4 & 32 \end{bmatrix}$$

Θα δούμε ότι πράγματι οι ανισότητες $|a_2| \leq \sqrt{\frac{4|j_2|}{3}}$ και $|c_2| \leq \sqrt{\frac{4|k_2|}{3}}$ ισχύουν. Το $|a_2| = 3 \leq \sqrt{\frac{4|j_2|}{3}} = \sqrt{\frac{4(3\cdot 7-(-1)(-1))}{3}} = \sqrt{\frac{4\cdot 20}{3}} \simeq 5,16$ και ο $\overline{F_2}$ είναι ο

$$\begin{bmatrix} 208 & 24 & 10 \\ 24 & 92 & -20 \\ 10 & -20 & 20 \end{bmatrix}$$

Άρα $k_2 = 92 \cdot 20 - (-20) \cdot (-20) = 1440$ και $c_2 = 20$ και η ανισότητα $|c_2| \leq \sqrt{\frac{4|k_2|}{3}} \simeq 43,81$ ισχύει. Ο F_2 λοιπόν είναι ο ζητούμενος πίνακας.

□

Θεώρημα 3.3.6:

Κάθε τριαδικός πίνακας F με ορίζουσα $-\frac{1}{4}$ είναι ισοδύναμος με τον πίνακα

$$\begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix}$$

Απόδειξη :

Από το θεώρημα 3.3.5 ο F είναι ισοδύναμος με έναν τριαδικό πίνακα F' με $|a| \leq \frac{4}{3}\sqrt[3]{|D|} = \frac{4}{3}\sqrt[3]{\frac{1}{4}}$, δηλαδή $|a| \leq 0.9$ και αφού ο a είναι ακέραιος, πρέπει $a = 0$.

Πάλι από το θεώρημα 3.3.5. η σχέση $|u^2 - 4ab| \leq 8\sqrt{\frac{|aD|}{3}}$, μας δίνει $|u^2| \leq 0$, δηλαδή $u = 0$ (u ακέραιος).

Έστω

$$F' = \begin{bmatrix} a & \frac{u}{2} & \frac{w}{2} \\ \frac{u}{2} & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

αντικαθιστώντας τα $a = 0$ και $u = 0$ έχουμε

$$F' = \begin{bmatrix} 0 & 0 & \frac{w}{2} \\ 0 & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix}$$

και $detF' = \frac{w}{2}(-\frac{bw}{2})$, όμως ο F' είναι ισοδύναμος με τον F, άρα $detF' = detF = -\frac{1}{4}$. Δηλαδή $-\frac{bw^2}{4} = -\frac{1}{4}$, άρα $bw^2 = 1$. Όμως οι b και w είναι ακέραιοι, άρα $b = 1$ και $w^2 = 1$.

Θεωρούμε τον πίνακα

$$G = \begin{bmatrix} 1 & 0 & 0 \\ -wv & 1 & 0 \\ -wc & 0 & 1 \end{bmatrix} \in GL_3(\mathbb{Z})$$

τότε

$$GF'G^T = \begin{bmatrix} 0 & 0 & \frac{w}{2} \\ 0 & 1 & 0 \\ \frac{w}{2} & 0 & 1 \end{bmatrix}.$$

Ας ονομάσουμε τον παραπάνω πίνακα H. Αν $w = -1$ τότε ο H είναι της ζητούμενης μορφής και το θεώρημα αποδείχθηκε. Έστω ότι $w = 1$, θεωρούμε τον πίνακα

$$G' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \in GL_3(\mathbb{Z})$$

τότε

$$G'HG'^T = \begin{bmatrix} 0 & 0 & -\frac{w}{2} \\ 0 & 1 & 0 \\ -\frac{w}{2} & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix}$$

και φτάσαμε στο ζητούμενο πίνακα.

□

Θεώρημα 3.3.7:

Κάθε τριαδικός πίνακας F με ακέραιους όρους και ορίζουσα ίση με 1 είναι ισοδύναμος με έναν εκ των

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ ή } \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Απόδειξη :

Έστω τριαδικός πίνακας F με ακεραίους όρους, αυτό σημαίνει ότι $\frac{u}{2}, \frac{v}{2}, \frac{w}{2} \in \mathbb{Z}$. Από το θεώρημα 3.3.5 ο F είναι ισοδύναμος με έναν τριαδικό πίνακα F' με ακέραιους όρους (αυτό γιατί ο F έχει ακέραιους όρους και κατά τον πολλαπλασιασμό με πίνακες από το $GL_3(\mathbb{Z})$ οι όροι παραμένουν ακέραιοι) έτσι ώστε:

$$|a| \leq \sqrt{\frac{|u^2 - 4ab|}{3}}$$

$$|u^2 - 4ab| \leq 8\sqrt{\frac{|a|}{3}}$$

$$|a| \leq \frac{4}{3}, \quad (\text{αφού } |a| \leq \frac{4}{3}\sqrt[3]{|D|} \text{ και } D = 1)$$

Από την τελευταία ανισότητα έχουμε $-\frac{4}{3} \leq a \leq \frac{4}{3}$, άρα $a = 0, 1$ ή -1.

Περίπτωση 1. $a = \pm 1$**.**

Μπορούμε να θεωρήσουμε ότι $\frac{u}{2} = 0$ (από το θεώρημα 3.3.1 αν $a = 1$ θέτουμε $n = -\frac{u}{2} \in \mathbb{Z}$, τότε κατά την πράξη $GF'G^T$ με $G = \begin{bmatrix} 1 & 0 & 0 \\ n & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ φτάνουμε στον πίνακα $\begin{bmatrix} 1 & 0 & * \\ 0 & -\frac{u^2}{4} + b & * \\ * & * & c \end{bmatrix}$, ο οποίος είναι ισοδύναμος με τον F, έχει $\frac{u}{2} = 0$ και το

ερώτημα είναι αν ισχύουν ακόμα οι ανισότητες. Αρκεί το $|u'^2 - 4a'b'|$ να είναι ίσο με $|u^2 - 4ab| = |u^2 - 4b|$, πράγματι $|u'^2 - 4a'b'| = |0 - 4 \cdot 1 \cdot (-\frac{u^2}{4} + b)| = |u^2 - 4b|$, όμοια για $a = -1$ θέτουμε $n = \frac{u}{2} \in \mathbb{Z}$).

Αφού

$$3 \leq |u^2 \pm 4b| \leq 4$$

(προκύπτει εύκολα από τις δύο πρώτες ανισότητες), συνεπάγεται ότι $3 \leq | \pm 4b| \leq 4$ και επειδή $b \in \mathbb{Z}$, θα πρέπει $b = \pm 1$.

Έστω

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{1}{2}wa & 0 & 1 \end{bmatrix}$$

αφού ο $\frac{w}{2}$ είναι ακέραιος και $a = \pm 1$, έπεται ότι $G \in GL_3(\mathbb{Z})$ και

$$GF'G^T = \begin{bmatrix} a & 0 & 0 \\ 0 & b & \frac{v}{2} \\ 0 & \frac{v}{2} & c - \frac{w^2}{4a} \end{bmatrix}.$$

Αν

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -\frac{1}{2}vb & 1 \end{bmatrix}$$

έχουμε

$$(HG)f'(HG)^T = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c' \end{bmatrix}.$$

Άρα $detHGF'G^TH^T = a \cdot b \cdot c'$, δηλαδή $1 = abc'$ και αφού $a = \pm 1$, $b = \pm 1$ έχουμε $c' = \pm 1$. Αν οι a, b, c είναι όλοι θετικοί, είναι ίσοι με ένα και ο πίνακας είναι ο μοναδιαίος. Διαφορετικά θα πρέπει ακριβώς δύο από αυτούς να είναι ίσοι με -1 (αφού το γινόμενο τους είναι ίσο με 1).

Αν $a = 1$, θέτουμε

$$G_1 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Αν $b = 1$, θέτουμε

$$G_2 = \begin{bmatrix} -1 & 1 & 0 \\ -1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Αν $c = 1$, θέτουμε

$$G_2 = \begin{bmatrix} 0 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{bmatrix}$$

Σε κάθε περίπτωση για το αντίστοιχο i, ο πίνακας $G_i HGF'(G_i HG)^T$ είναι ο

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Περίπτωση 2. $a = 0$**.**

Από τη σχέση $|u^2 - 4ab| \leq 8\sqrt{\frac{|a|}{3}}$, έχουμε ότι $u = 0$, τότε

$$detF' = det \begin{bmatrix} 0 & 0 & \frac{w}{2} \\ 0 & b & \frac{v}{2} \\ \frac{w}{2} & \frac{v}{2} & c \end{bmatrix} = -\frac{bw^2}{4} = 1$$

και $b, w \in \mathbb{Z}$, δηλαδή $b = -1$ και $w = \pm 2$. Αφού ο v είναι άρτιος (διαφορετικά ο F' δε θα είχε ακέραιους όρους), έχουμε ότι ο $\frac{v}{w}$ είναι ακέραιος, άρα ο παρακάτω πίνακας G ανήκει στο $GL_3(\mathbb{Z})$.

$$G = \begin{bmatrix} 1 & 0 & 0 \\ -\frac{v}{w} & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Επομένως

$$GF'G^T = \begin{bmatrix} 0 & 0 & \frac{w}{2} \\ 0 & -1 & 0 \\ \frac{w}{2} & 0 & c \end{bmatrix} \quad (I)$$

Αν θεωρήσουμε τον πίνακα $H = \begin{bmatrix} 1 & 0 & 0 \\ \frac{w}{2} & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ ο οποίος ανήκει στο $GL_3(\mathbb{Z})$ (αφού $w = \pm 2$), έχουμε:

$$HGF'G^TH^T = \begin{bmatrix} 0 & 0 & \frac{w}{2} \\ 0 & -1 & 0 \\ \frac{w}{2} & 0 & c-1 \end{bmatrix} \quad (II)$$

Άρα ο δοθείς πίνακας F είναι ισοδύναμος με τον

$$F'' = \begin{bmatrix} 0 & 0 & \frac{w}{2} \\ 0 & -1 & 0 \\ \frac{w}{2} & 0 & c \end{bmatrix},$$

με c άρτιο (αν το c είναι άρτιο έχουμε τον πίνακα από την ισότητα (I), αν c περιττό έχουμε τον πίνακα από την ισότητα (II) με $c' = c-1$ άρτιο).

Αφού το c είναι άρτιος ο πίνακας $J = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{c}{w} & 0 & 1 \end{bmatrix}$ ανήκει στο $GL_3(\mathbb{Z})$ και παίρνουμε

$$JF''J^T = \begin{bmatrix} 0 & 0 & \frac{w}{2} \\ 0 & -1 & 0 \\ \frac{w}{2} & 0 & 0 \end{bmatrix}.$$

Αν $w = 2$ ο παραπάνω πίνακας είναι ο $\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.

Αν $w = -2$, θέτουμε $J' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \in GL_3(\mathbb{Z})$ και τότε

$$J'JF''J^TJ'^T = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

και το θεώρημα αποδείχτηκε.

□

Θεώρημα 3.3.8:

Έστω T_1, T_2, T_3 και X ακέραιοι, με $X \neq 0$. Αν ΜΚΔ(T_1, T_2, T_3)=1, τότε υπάρχουν ακέραιοι U και V, πρώτοι μεταξύ τους, τέτοιοι ώστε:

$$ΜΚΔ(T_1V^2 - T_2UV + T_3V^2, 2X) = 1$$

Απόδειξη:

Έστω $u_1, ..., u_h$ οι διακεκριμένοι πρώτοι που διαιρούν το $2X$, αλλά όχι το T_1 και U το γινόμενο τους (ή $U = 1$, αν δεν υπάρχουν τέτοιοι πρώτοι).

Έστω $v_1, ..., v_i$ οι διακεκριμένοι πρώτοι που διαιρούν το $2X$ και το T_1, αλλά όχι το T_3 και V το γινόμενο τους (ή $V = 1$, αν δεν υπάρχουν τέτοιοι πρώτοι).

Έστω $w_1, ..., w_k$ οι διακεκριμένοι πρώτοι που διαιρούν τα $2X$,T_1 και T_3,τότε κανένα w δε διαιρεί το $Y = T_1V^2 - T_2UV + T_3U^2$, (αν ένα w διαιρούσε το Y, τότε αφού διαιρεί και τα T_1, T_3 θα πρέπει να διαιρεί και το UVT_2, όμως από τον ορισμό των U, V το w δε μπορεί να τα διαιρεί, άρα $w|T_2$, τότε όμως $w|ΜΚΔ(T_1, T_2, T_3) = 1$, αντίφαση).

Από τον ορισμό των U και V έχουμε ΜΚΔ$(U, V) = 1$ και ΜΚΔ$(Y, 2X) = 1$ (αν $p|2X$ τότε ο p είναι ένας από τους u, v ή w. Αν είναι u τότε δε διαιρεί το T_1 και διαιρεί το U, δηλαδή διαιρεί το $T_2UV - T_3U^2$. Αν το p διαιρεί και το Y τότε το p διαιρεί το $Y + T_2UV - T_3U^2 = T_1V^2$, όμως $p \not| V$ (αφού το p είναι ένα από τα u), άρα $p|T_1$, άτοπο. Όμοια αν το p είναι v ή w).

□

Θεώρημα 3.3.9:

Έστω τριαδικός πίνακας

$$A = \begin{bmatrix} a & \frac{b}{2} & \frac{k}{2} \\ \frac{b}{2} & c & \frac{m}{2} \\ \frac{k}{2} & \frac{m}{2} & n \end{bmatrix}$$

με $detA = -\frac{1}{4}$, $a, c > 0$ και b περιττό. Έστω ότι $b^2 - 4ac < 0$ και ΜΚΔ(a, b, c)=1, τότε ο πίνακας

$$\begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$$

είναι γνήσια ισοδύναμος με έναν πίνακα της μορφής

$$\begin{bmatrix} N^2 & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix},$$

όπου ΜΚΔ$(N, 2(b^2 - 4ac)) = 1$.

Απόδειξη:

Από το θεώρημα 3.3.6 υπάρχει πίνακας $T \in GL_3(\mathbb{Z})$ τέτοιο ώστε $A = TMT^T$, με

$$M = \begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix}.$$

Έστω $[t_1\ t_2\ t_3]$ η κάτω σειρά του πίνακα T και $[T_1\ T_2\ T_3]$ η κάτω σειρά του πίνακα $\overline{T}$, τότε

$$\pm 1 = detT = t_1T_1 + t_2T_2 + t_3T_3$$

(από τον ορισμό του $\overline{T}$ το T_i στοιχείο είναι το αλγεβρικό συμπλήρωμα του στοιχείου t_i) και έπεται ότι ΜΚΔ$(T_1, T_2, T_3) = 1$. Από το θεώρημα 3.3.8 υπάρχουν ακέραιοι U και V, πρώτοι μεταξύ τους, τέτοιοι ώστε:

$$MK\Delta(T_1V^2 - T_2UV + T_3V^2, 2(b^2 - 4ac)) = 1.$$

Έστω $H, J \in \mathbb{Z}$ τέτοιοι ώστε $UJ - VH = 1$ (τέτοιοι ακέραιοι υπάρχουν αφού $(U, V) = 1$). Θεωρούμε τον πίνακα

$$S = \begin{bmatrix} U^2 & UH & H^2 \\ 2UV & UJ + VH & 2HJ \\ V^2 & VJ & J^2 \end{bmatrix}$$

Ισχύει ότι $detS = 1$ και $SMS^T = M$ (δείτε παράρτημα). Επίσης η δεξιά στήλη του πίνακα $\overline{S}$ είναι (δείτε παράρτημα):

$$\begin{bmatrix} V^2 \\ -UV \\ U^2 \end{bmatrix},$$

άρα ο κάτω δεξιά όρος του πίνακα $\overline{T} \cdot \overline{S}$ είναι

$$[T_1\ T_2\ T_3] \begin{bmatrix} V^2 \\ -UV \\ U^2 \end{bmatrix} = T_1V^2 - T_2UV + U^2T_3,$$

δηλαδή είναι ο (μη μηδενικός) ακέραιος σχετικά πρώτος με το $2(b^2 - 4ac)$ που είδαμε παραπάνω.

Έστω

$$TS = \begin{bmatrix} r_1 & r_2 & r_3 \\ s_1 & s_2 & s_3 \\ * & * & * \end{bmatrix}$$

Από τη σχέση $SMS^T = M$, έχουμε ότι $TSMS^TT^T = TMT^T$ και άρα $TSM(TS)^T = A$. Συγκρίνοντας λοιπόν τους πίνακες $TSM(TS)^T$ και A, παίρνουμε τις σχέσεις:

$$a = r_2^2 - r_1r_3$$

$$\frac{b}{2} = r_2s_2 - \frac{r_1s_3}{2} - \frac{r_3s_1}{2}$$

$$c = s_2^2 - s_1s_3$$

Με απλή αντικατάσταση των a, $\frac{b}{2}$ και c από τις παραπάνω σχέσεις (δείτε παράρτημα), έχουμε

$$as_1^2 - bs_1r_1 + cr_1^2 = (r_1s_2 - r_2s_1)^2.$$

Το $r_1s_2 - r_2s_1$ είναι η κάτω δεξιά είσοδος του $\overline{TS}$, η οποία όπως δείξαμε είναι ίση και με $T_1V^2 - T_2UV + U^2T_3$ (στην πραγματικότητα δείξαμε ότι είναι ο κάτω δεξιά όρος του $\overline{T} \cdot \overline{S}$, αλλά όπως έχουμε δει παραπάνω $\overline{T} \cdot \overline{S} = \overline{TS}$). Άρα ο $r_1s_2 - r_2s_1$ είναι μη μηδενικός ακέραιος και σχετικά πρώτος με τον $2(b^2 - 4ac)$. Θέτουμε

$$s'' = \frac{s_1}{MK\Delta(s_1, r_1)} \quad \text{και} \quad r'' = \frac{r_1}{MK\Delta(s_1, r_1)}.$$

Οι s'' και r'' από τον ορισμό τους είναι πρώτοι μεταξύ τους, άρα υπάρχουν ακέραιοι t'' και u'' τέτοιοι ώστε:

$$-s''t'' - r''u'' = 1$$

και έπεται ότι ο πίνακας

$$G = \begin{bmatrix} -s'' & r'' \\ u'' & t'' \end{bmatrix}$$

ανήκει στο $SL_2(\mathbb{Z})$, τότε

$$G \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} G^T \begin{bmatrix} N^2 & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix}$$

όπου ο $N = \frac{r_1 s_2 - r_2 s_1}{MK\Delta(s_1, r_1)} \in \mathbb{Z}$ είναι πρώτος με τον $2(b^2 - 4ac)$ (αφού ο $r_1 s_2 - r_2 s_1$ είναι πρώτος με τον $2(b^2 - 4ac)$).

□

3.4 Omega Kernel ή Τετραγωνικές Μορφές

Έστω D αρνητικός ακέραιος ισότιμος με $1 \pmod 4$. Έστω H το σύνολο των κλάσεων ισοδυναμίας $x \pmod D$, ώστε $(x, D) = 1$ και η $z^2 \equiv x \pmod D$ να έχει λύση, τότε το H είναι πολλαπλασιαστική ομάδα. Επίσης αν $x \in H$ τότε και $x^2 \in H$.

Θεώρημα 3.4.1:

Το σύνολο H έχει $\frac{\phi(|D|)}{2^r}$ στοιχεία, όπου r το πλήθος των διακεκριμένων πρώτων διαιρετών του D.

Απόδειξη:

Η $z^2 \equiv x \pmod D$, με $(x, D) = 1$, είτε δεν έχει λύση, είτε έχει 2^r λύσεις (δείτε παράρτημα για την ισοτιμία $x^2 \equiv R \pmod C$).

Αν $x \in H$ (δηλαδή αν η $z^2 \equiv x \pmod D$ έχει τουλάχιστον μία λύση), τότε σύμφωνα με το παραπάνω θα έχει 2^r λύσεις. Όλες αυτές οι λύσεις είναι ανάμεσα στις $\phi(|D|)$ κλάσεις που είναι σχετικά πρώτες με το D.

Αν x_1, x_2 διαφορετικά στοιχεία του H, τότε καμία λύση της $z^2 \equiv x_1 \pmod D$ δεν είναι λύση της $z^2 \equiv x_2 \pmod D$ (διαφορετικά θα έπρεπε τα x_1 και x_2 να ανήκουν στην ίδια κλάση, άτοπο).

Άρα για κάθε στοιχείο του H (δηλαδή για κάθε $x \in H$) ορίζεται ένα σύνολο (το σύνολο των λύσεων της $z^2 \equiv x \pmod D$), το οποίο περιέχει 2^r ισοϋπόλοιπα σχετικά πρώτα με το D και ξένα μεταξύ τους. Το ερώτημα είναι αν με αυτό τον τρόπο παίρνουμε και τις $\phi(|D|)$ κλάσεις ή λιγότερες.

Αν δείξουμε ότι κάθε κλάση που είναι σχετικά πρώτη με το D ανήκει σε ένα τέτοιο σύνολο, τότε $2^r \cdot |H| = \phi(|D|)$ και το θεώρημα αποδείχθηκε.

Πράγματι αν u μία κλάση, με $(u, D) = 1$, τότε $u^2 \in H$ και το u ανήκει στο σύνολο των λύσεων που ορίζεται από το u^2.

□

Θα λέμε ότι η μορφή Gauss $F = [a, b, c]$ αναπαριστά έναν ακέραιο m αν και μόνο αν υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε:

$$ax^2 + bxy + cy^2 = m.$$

Αν η F αναπαριστά έναν ακέραιο m και F' είναι γνήσια ισοδύναμη με την F, τότε και η F' αναπαριστά τον m.

Εφόσον η F αναπαριστά έναν ακέραιο m, θα υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $(x\ y)M(x\ y)^T = m$. Όμως η F' είναι γνήσια ισοδύναμη με την F, άρα θα υπάρχει πίνακας $G \in SL_2(\mathbb{Z})$ τέτοιος ώστε $M' = GMG^T$.

Για $(x'\ y') := (x\ y)G^{-1}$, έχουμε $(x'\ y')M'(x'\ y')^T = (x\ y)G^{-1}GMG^T((x\ y)G^{-1})^T$ $= (x\ y)MG^T(G^T)^{-1}(x\ y)^T = (x\ y)M(x\ y)^T = m$, δηλαδή η F' αναπαριστά τον m.

Άρα αν η μορφή $[a, b, c]$ αναπαριστά έναν ακέραιο m, λέμε ότι η κλάση ισοδυναμίας $[\![a, b, c]\!]$ αναπαριστά το m. Θα συμβολίζουμε με C το σύνολο αυτών των κλάσεων ισοδυναμίας και θα δείξουμε στο επόμενο κεφάλαιο ότι το C είναι ομάδα.

Έστω $x \in H$, τότε η $z^2 \equiv x \pmod D$ έχει λύση, έστω z και για $D = b^2 - 4ac$, έχουμε:

$$z^2 + bz \cdot 0 + \frac{b^2 - D}{4} \cdot 0^2 = x + QD$$

για κάποιο ακέραιο Q. Έτσι αν $x \in H$, η μορφή Gauss $[1, b, \frac{b^2-D}{4}]$ αναπαριστά ακέραιο ισότιμο με το $x \pmod D$. Μία μορφή Gauss που αναπαριστά έναν ακέραιο της μορφής $x + QD$, με $x \in H$ θα λέγεται μορφή omega kernel. Σύμφωνα με τα παραπάνω, αν δύο μορφές Gauss είναι γνήσια ισοδύναμες και η μία είναι μορφή omega kernel, τότε θα είναι και η άλλη. Άρα έχει νόημα να ορίσουμε ως omega kernel κλάση την κλάση του C που να περιέχει μία μορφή omega kernel (δηλαδή μία που να αναπαριστά έναν ακέραιο της μορφής $x + QD$, με $x \in H$). Έστω λοιπόν K το σύνολο των omega kernel κλάσεων.

Στο κεφάλαιο 3.6 θα ορίσουμε μία συνάρτηση ω με πεδίο ορισμού το C και σύνολο τιμών το U/H, όπου U το σύνολο των κλάσεων ισοδυναμίας που είναι σχετικά πρώτες με το D. Αυτή η συνάρτηση αναπαριστά την κλάση $[f]$ των μορφών Gauss, στο σύμπλοκο mH, όπου m ισοϋπόλοιπο του U ώστε ένας αριθμός της μορφής $m + QD$ να αναπαρίσταται από την κλάση $[f]$. Θα δούμε ότι ο πυρήνας της ω (δηλαδή το υποσύνολο του C που απεικονίζεται μέσω της ω στο H) είναι το σύνολο των omega kernel κλάσεων.

Τώρα θα ορίσουμε τις τετραγωνικές μορφές.

Δύο μορφές Gauss $F_1 = [a_1, b_1, c_1]$ και $F_2 = [a_2, b_2, c_2]$ θα λέμε ότι βρίσκονται σε **αρμονία (concordant)** αν και μόνο αν $b_1 = b_2$ και $a_2|c_1$.

Να σημειώσουμε ότι αφού $b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$ (οι μορφές έχουν ίδια διακρίνουσα D), έχουμε $\frac{c_1}{a_2} = \frac{c_2}{a_1}$, άρα και $a_1|c_2$.

Ορίζουμε τη σύνθεση $F_1 \circ F_2$ δύο αρμονικών μορφών να είναι η μορφή

$$[a_1a_2, b_1, \frac{c_1}{a_2}]$$

Βλέπουμε ότι η σύνθεση των μορφών έχει την ίδια διακρίνουσα με αυτές ($b_1^2 - 4a_1a_2\frac{c_1}{a_2} = b_1^2 - 4a_1c_1 = D$).

Για παράδειγμα η μορφή $[N, b, Nc]$ είναι σε αρμονία με τον εαυτό της.

Η μορφή $[a, b, c]$ είναι τετραγωνική μορφή αν και μόνο αν υπάρχουν δύο γνήσια ισοδύναμες μορφές Gauss, F και F', οι οποίες βρίσκονται σε αρμονία, τέτοιες ώστε η $[a, b, c]$ να είναι γνήσια ισοδύναμη με την $F \circ F'$.

Για παράδειγμα η $[N^2, b, c] = [N, b, Nc] \circ [N, b, Nc]$ είναι τετραγωνική μορφή.

Θεώρημα 3.4.2:

Αν οι μορφές F_1 και F_2 βρίσκονται σε αρμονία και αναπαριστούν ακεραίους m_1 και m_2 αντίστοιχα, τότε η $F_1 \circ F_2$ αναπαριστά τον m_1m_2.

Απόδειξη:

Έστω $F_1 = [a_1, b, c_1]$ και $F_2 = [a_2, b, c_2]$. Οι μορφές F_1 και F_2 αναπαριστούν ακεραίους m_1 και m_2 αντίστοιχα, άρα θα υπάρχουν ακέραιοι x_1, y_1, x_2 και y_2 έτσι ώστε:

$$m_1 = a_1x_1^2 + bx_1y_1 + c_1y_1^2$$

$$m_2 = a_2x_2^2 + bx_2y_2 + c_2y_2^2$$

Έστω $c = \frac{c_2}{a_1} = \frac{c_1}{a_2}$, τότε $F_1 \circ F_2 = [a_1a_2, b, c]$.

Θέτουμε

$$X = x_1x_2 - cy_1y_2$$

και

$$Y = a_1x_1y_2 + a_2y_1x_2 + by_1y_2,$$

τότε, όπως ανακάλυψε ο Gauss (παράρτημα) είναι

$m_1m_2 = (a_1x_1^2 + bx_1y_1 + c_1y_1^2)(a_2x_2^2 + bx_2y_2 + c_2y_2^2) = a_1a_2X^2 + bXY + cY^2$

□

Θεώρημα 3.4.3:

Μία μορφή Gauss είναι μορφή omega kernel αν και μόνο αν είναι τετραγωνική μορφή.

Απόδειξη:

(⇐)

Αν είναι τετραγωνική μορφή, θα υπάρχουν δύο γνήσια ισοδύναμες μορφές F και F', οι οποίες βρίσκονται σε αρμονία τ.ω. η $[a, b, c]$ να είναι γνήσια ισοδύναμη με την $F \circ F'$. Αν η F αναπαριστά ακέραιο x, τότε και η F' θα αναπαριστά τον ίδιο ακέραιο x και τότε από το προηγούμενο θεώρημα θα έχουμε ότι η $F \circ F'$ αναπαριστά τον x^2. Όμως $x^2 \in H$, άρα η $[a, b, c]$ είναι μορφή omega kernel.

(⇒)

Έστω ότι η $[a, b, c]$ είναι μορφή omega kernel, δηλαδή αναπαριστά κάποιον ακέραιο $h + QD$, με $h \in H$.

Το $h^{-1} \in H$ και η μορφή Gauss

$$[1, b, \frac{b^2 - D}{4}],$$

όπως είδαμε παραπάνω, αναπαριστά έναν ακέραιο j, ισότιμο με το $h^{-1} \pmod D$.

Οι μορφές $[a, b, c]$ και $[1, b, \frac{b^2-D}{4}]$ βρίσκονται σε αρμονία και η σύνθεση τους $[a \cdot 1, b, \frac{c}{1}] = [a, b, c]$ αναπαριστά τον ακέραιο hj, που είναι ισότιμος με $1 \pmod D$.

Άρα υπάρχουν ακέραιοι m, k και Q τ.ω.:

$$am^2 - bmk + ck^2 = (-Q)D + 1.$$

Έστω

$$A = \begin{bmatrix} a & \frac{b}{2} & \frac{k}{2} \\ \frac{b}{2} & c & \frac{m}{2} \\ \frac{k}{2} & \frac{m}{2} & Q \end{bmatrix}$$

Ο A έχει ορίζουσα $Q(ac - \frac{b^2}{4}) - \frac{m}{2}(\frac{am}{2} - \frac{kb}{4}) + \frac{k}{2}(\frac{bm}{4} - \frac{ck}{2}) = Q(-\frac{D}{4}) - \frac{2am^2-kbm}{8} + \frac{kbm-2k^2c}{8} = \frac{-2QD-2am^2+2kbm-2k^2c}{8} = \frac{2[-QD-am^2+kbm+k^2c]}{8} = \frac{2(-1)}{4} = -\frac{1}{4}$.

Από το θεώρημα 3.3.9 η $[a, b, c]$ είναι γνήσια ισοδύναμη με την μορφή $[N^2, b', c']$ με ΜΚΔ$(N, 2D) = 1$.

Επιλέγουμε $N > 0$. Αφού ΜΚΔ$(N, 2D) = 1$, από τη σχέση $D = b'^2 - 4N^2c'$, έχουμε ότι ΜΚΔ$(N, b', Nc') = 1$. Άρα η $[N, b', Nc']$ είναι μορφή Gauss (με διακρίνουσα $b'^2 - 4NNc' = b'^2 - 4N^2c' = D$). Είναι σε αρμονία με τον εαυτό της και

$$[N, b', Nc'] \circ [N, b', Nc'] = [N^2, b', c'].$$

Δηλαδή η $[N^2, b', c']$ είναι τετραγωνική μορφή, άρα και η $[a, b, c]$ είναι (αφού είναι γνήσια ισοδύναμη με την $[N^2, b', c']$).

□

3.5 Ασαφείς ή αυτο-αντίστροφες μορφές

Σε αυτό το κεφάλαιο θα ορίσουμε τις ασαφείς μορφές. Στη συνέχεια θα ορίσουμε μία πράξη με την οποία το σύνολο C των κλάσεων ισοδυναμίας των μορφών Gauss αποτελεί ομάδα. Μετά με τη βοήθεια της πράξης αυτής θα ορίσουμε τις αυτο-αντίστροφες μορφές και θα δείξουμε ότι μία μορφή είναι ασαφής αν και μόνο αν είναι αυτο-αντίστροφη. Τέλος θα χρησιμοποιήσουμε αυτό το αποτέλεσμα για να βγάλουμε μία πληροφορία σχετικά με το πλήθος των στοιχείων του C.

Μία μορφή Gauss $[a, b, c]$ θα λέγεται ασαφής αν και μόνο αν η $[a, b, c]$ είναι γνήσια ισοδύναμη με μία ειδική ασαφή μορφή $[a', a', c']$.

Θεώρημα 3.5.1:

Η μορφή $[a, b, c]$ είναι ασαφής αν και μόνο αν η $[a, b, c]$ είναι γνήσια ισοδύναμη με την $[c, b, a]$.

Απόδειξη:

($\Rightarrow$)

Έστω ότι η $[a, b, c]$ είναι ασαφής μορφή, δηλαδή είναι γνήσια ισοδύναμη με μία μορφή $[a', a', c']$. Ο πίνακας που αντιστοιχεί στην $[a, b, c]$ είναι ο $M = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$, ενώ αυτός που αντιστοιχεί στην $[a', a', c']$ είναι ο $M' = \begin{bmatrix} a' & \frac{a'}{2} \\ \frac{a'}{2} & c' \end{bmatrix}$.

Αφού οι μορφές είναι ισοδύναμες, θα υπάρχει πίνακας $G \in SL_2(\mathbb{Z})$, τέτοιος ώστε:

$$M = GM'G^T.$$

Θεωρούμε τώρα τους πίνακες $H = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ και $J = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$, τότε ο πίνακας HGJ ανήκει στο $SL_2(\mathbb{Z})$, αφού $detHGJ = detH \cdot detG \cdot detJ = (-1)1(-1) = 1$.

Επίσης

$$JM'J^T = M'.$$

($JM'J^T = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} a' & \frac{a'}{2} \\ \frac{a'}{2} & c' \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} a' & \frac{a'}{2} \\ \frac{a'}{2} & \frac{a'}{2} - c' \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} a' & \frac{a'}{2} \\ \frac{a'}{2} & \frac{a'}{2} - \frac{a'}{2} + c' \end{bmatrix} = M'$)

Ο M είναι γνήσια ισοδύναμος με τον M'. Ο M' είναι γνήσια ισοδύναμος με τον $(HGJ)M'(HGJ)^T = HGJM'J^TG^TH^T = HGM'G^TH^T = HMH^T$, άρα ο M είναι γνήσια ισοδύναμος με τον

$$HMH^T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} c & \frac{b}{2} \\ \frac{b}{2} & a \end{bmatrix},$$

που αντιστοιχεί στη μορφή $[c, b, a]$, δηλαδή η μορφή $[a, b, c]$ είναι γνήσια ισοδύναμη με την $[c, b, a]$.

($\Leftarrow$)

Έστω ότι η μορφή $[a, b, c]$ είναι γνήσια ισοδύναμη με την $[c, b, a]$, τότε θα υπάρχει πίνακας $G \in SL_2(\mathbb{Z})$ τ.ω. $G * [a, b, c] = [c, b, a]$.

Δηλαδή

$$GMG^T = \begin{bmatrix} c & \frac{b}{2} \\ \frac{b}{2} & a \end{bmatrix}.$$

Έστω $G' = \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} G$, τότε

$$G'MG'^T = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} GMG^T \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} c & \frac{b}{2} \\ \frac{b}{2} & a \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} -\frac{b}{2} & -a \\ -c & -\frac{b}{2} \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} = M.$$

Δηλαδή $G'M = M(G'^T)^{-1}$ και εξισώνοντας τους πάνω αριστερά όρους των πινάκων:

$$G'M = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} = \begin{bmatrix} ra + \frac{sb}{2} & \frac{rb}{2} + sc \\ ta + \frac{bu}{2} & uc + \frac{tb}{2} \end{bmatrix}$$

και

$$M(G'^T)^{-1} = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} -u & t \\ s & -r \end{bmatrix} = \begin{bmatrix} -au + \frac{bs}{2} & at - \frac{rb}{2} \\ -\frac{ub}{2} + cs & \frac{tb}{2} - cr \end{bmatrix}$$

έχουμε

$$ra + \frac{sb}{2} = -au + \frac{sb}{2}.$$

Δηλαδή $r = -u$ και επειδή $ru - st = 1$ ($ru - st = detG' = det \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \cdot |G| = -1 \cdot 1 = -1$), έπεται ότι

$$r^2 + st = 1.$$

Περίπτωση 1. $s \neq 0$

Έστω $g =$ΜΚΔ$(r+1, s)$, τότε η παραπάνω σχέση μας δίνει ότι

$$(r-1)(\frac{r+1}{g}) = -(\frac{s}{g})t,$$

άρα ο ακέραιος $\frac{r+1}{g}$ διαιρεί το t και ο ακέραιος $\frac{s}{g}$ διαιρεί το $r-1$, (αφού $g =$ΜΚΔ$(r+1, s)$, συνεπάγεται ότι $(\frac{r+1}{g}, \frac{s}{g}) = 1$).

Έστω

$$x = \frac{r+1}{g},\ y = \frac{s}{g},\ w = \frac{g+y}{2},\ z = \frac{xw-1}{y}$$

Θα αποδείξουμε ότι ο w είναι ακέραιος.

1) Αν ο s είναι περιττός, τότε και ο g σαν διαιρέτης του s θα είναι περιττός και το ίδιο θα ισχύει και για τον $y = \frac{s}{g}$, τότε όμως ο $g+y$ είναι άρτιος (περιττός +περιττός) και άρα ο $w = \frac{g+y}{2}$ είναι ακέραιος.

2) Αν ο s είναι άρτιος, τότε αφού $r^2 + st = 1$, ο r θα πρέπει να είναι περιττός (διαφορετικά το άθροισμα $r^2 + st$ θα ήταν άρτιο), τότε ο g θα είναι άρτιος ($g =$ΜΚΔ$(r+1, s)$, με $r+1$ και s άρτια).

Συγκρίνοντας τους όρους των $G'M$ και $M(G'^T)^{-1}$ έχουμε

$$\frac{rb}{2} + sc = at - \frac{rb}{2} \Rightarrow$$

$$rb + sc = at$$

Οι b (εξ' ορισμού των μορφών Gauss) και r είναι περιττοί, άρα ο rb είναι περιττός και ο sc άρτιος, τότε ο $rb + sc$ είναι περιττός, άρα και ο at είναι περιτός, άρα ο t περιττός.

Αφού $(r-1)(r+1) = -st$, με t περιττό, έχουμε ότι ο s διαιρείται από μεγαλύτερη δύναμη του 2 από αυτή που διαιρείται το $r+1$. Άρα ο $y = \frac{s}{g}$ είναι άρτιος και τότε ο $w = \frac{g+y}{2}$ είναι ακέραιος.

Θα δείξουμε ότι και ο z είναι ακέραιος.

Από τον ορισμό του z έχουμε,

$$z = \frac{x^{\frac{g+y}{2}} - 1}{y} = \frac{1}{2}(x + (\frac{xg-2}{y})) = \frac{1}{2}(x + \frac{r-1}{s/g}).$$

Για να δείξουμε ότι ο z είναι ακέραιος, αρκεί να δείξουμε ότι οι δύο προσθετέοι x και $\frac{r-1}{s/g}$ είναι ή και οι δύο άρτιοι ή και οι δύο περιττοί (να θυμηθούμε ότι ο $\frac{r-1}{s/g}$ είναι ακέραιος, αφού ο $y = \frac{s}{g}$ διαιρεί τον $r-1$).

1) Έστω ότι ο $y = \frac{s}{g}$ είναι άρτιος, τότε ο x είναι περιττός (αφού $(x, y) = (\frac{r+1}{g}, \frac{s}{g}) = 1$). Επίσης ο r είναι περιττός (ο $s = yg$ είναι άρτιος και $r^2 + st = 1$). Όπως προηγουμένως έπεται ότι ο t είναι περιττός. Αφού $(r-1)x = -yt$, με x, t περιττούς, έχουμε ότι ο $\frac{r-1}{y}$ είναι περιττός, άρα ο z είναι ακέραιος.

2) Αν ο $y = \frac{s}{g}$ είναι περιττός, τότε και ο s είναι περιττός (αν ο s ήταν άρτιος, όπως είδαμε στην περίπτωση 2) για τον w, θα είχαμε ότι ο y είναι άρτιος, αντίφαση).

i) Αν ο $x = \frac{r+1}{g}$ είναι άρτιος, τότε και ο $r+1$ είναι άρτιος και συνεπάγεται ότι και ο $r-1$ είναι άρτιος. Άρα ο $\frac{r-1}{s/g}$ είναι άρτιος (πηλίκο άρτιου με περιττό). Επομένως οι x και $\frac{r-1}{s/g}$ είναι και οι δύο άρτιοι.

ii) Αν ο $x = \frac{r+1}{g}$ είναι περιττός, έπεται ότι ο $r+1 = xg$ είναι περιττός (αφού ο g είναι περιττός, σαν διαιρέτης του περιττού ακεραίου s), τότε και ο $r-1$ είναι περιττός. Άρα ο $\frac{r-1}{s/g}$ είναι περιττός (πηλίκο περιττού με περιττό). Άρα οι x και $\frac{r-1}{s/g}$ είναι και οι δύο περιττοί.

Έχουμε δηλαδή ότι οι x, y, w και z είναι ακέραιοι. Ας θεωρήσουμε πίνακα

$$T = \begin{bmatrix} x & y \\ z & w \end{bmatrix},$$

τότε $T \in SL_2(\mathbb{Z})$, (αφού έχει ακέραιους όρους και $detT = xw - zy = xw - y\frac{xw-1}{y} = xw - xw + 1 = 1$) και ισχύει

$$TG' = \begin{bmatrix} rx + yt & sx + yu \\ zr + wt & sz + wu \end{bmatrix} = \begin{bmatrix} x & y \\ x - z & y - w \end{bmatrix} = JT$$

με τον πίνακα J όπως προηγουμένως. Έχουμε

$$JTMT^TJ^T = TG'T^{-1}TMT^T(TGT^{-1})^T = TG'MG'^TT^T = TMT^T,$$

δηλαδή $J(TMT^T)J^T = TMT^T$, τότε ο TMT^T αντιστοιχεί σε ειδική ασαφή μορφή.

(Αν για έναν πίνακα $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, ισχύει $JAJ^T = A$, τότε $\begin{bmatrix} a & a-b \\ a-c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, δηλαδή $b = c = \frac{a}{2}$, άρα $A = \begin{bmatrix} a & \frac{a}{2} \\ \frac{a}{2} & d \end{bmatrix}$ και ο A αντιστοιχεί στην ειδική ασαφή μορφή $[a, a, c]$).

Άρα η μορφή $[a, b, c]$ (που αντιστοιχεί στον πίνακα M) είναι ασαφής.

Περίπτωση 2.$s = 0$.

Τότε $r = \pm 1$. Αν $r = 1$ θέτουμε $x = 1$, $y = 0$, $w = 1$ και $z = \frac{1-t}{2}$, τότε όπως πριν θεωρούμε τον πίνακα

$$T = \begin{bmatrix} 1 & 0 \\ \frac{1-t}{2} & 1 \end{bmatrix}.$$

Ο πίνακας T έχει ακέραιους όρους ($rb + sc = at \Rightarrow at = b$ =περιττός, άρα ο t περιττός και ο $\frac{1-t}{2}$ είναι ακέραιος) και $detT = 1$, άρα $T \in SL_2(\mathbb{Z})$ και

$$TG' = \begin{bmatrix} 1 & 0 \\ \frac{1-t}{2} & 1 \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} r & s \\ \frac{(1-t)r}{2} + t & (1-t)s + u \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 \\ \frac{1+t}{2} & u \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 - \frac{1-t}{2} & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \frac{1-t}{2} & 1 \end{bmatrix} = JT.$$

Δηλαδή $TG' = JT$ και όπως πριν φτάνουμε στο αποτέλεσμα.

Για $r = -1$, θέτουμε $x = t$, $y = 2$, $w = 1$, $z = \frac{t-1}{2}$ και δουλεύουμε όμοια.

□

Θεώρημα 3.5.2:

Έστω F_1 και F_2 δύο μορφές Gauss (με την ίδια διακρίνουσα D) και N ένας μη μηδενικός ακέραιος, τότε υπάρχουν μορφές Gauss H_1 και H_2 τ.ω. η H_1 να είναι γνήσια ισοδύναμη με την F_1, η H_2 να είναι γνήσια ισοδύναμη με την F_2, οι H_1 και H_2 να βρίσκονται σε αρμονία και αν a_1, a_2 οι πρώτοι συντελεστές των μορφών H_1, H_2 αντίστοιχα, να είναι ΜΚΔ(a_1, a_2) =ΜΚΔ(a_1a_2, N)=1.

Απόδειξη:

Έστω $F_1 = [T_1, T_2, T_3]$, από το θεώρημα 3.3.8 υπάρχουν ακέραιοι U και V, πρώτοι μεταξύ τους, τέτοιοι ώστε

$$MK\Delta(T_1U^2 + T_2UV + T_3V^2, 2N) = 1.$$

Έστω ακέραιοι P, Q ώστε $UQ - VP = 1$ (τέτοιοι ακέραιοι υπάρχουν, αφού οι U και V είναι πρώτοι μεταξύ τους), τότε θεωρούμε τον πίνακα

$$G = \begin{bmatrix} U & V \\ P & Q \end{bmatrix},$$

με $G \in SL_2(\mathbb{Z})$. Έστω

$$F_1' = G * F_1 = [T_1', T_2', T_3'],$$

τότε ο $T_1' = T_1U^2 + T_2UV + T_3V^2$ είναι ένας μη μηδενικός ακέραιος, σχετικά πρώτος με το N.

Όμοια, υπάρχει μία μορφή Gauss $F_2' = [S_1', S_2', S_3']$, που είναι γνήσια ισοδύναμη με την μορφή F_2 και τ.ω. ο S_1' να είναι μη μηδενικός ακέραιος, σχετικά πρώτος με το $T_1'N$ (προκύπτει από το θεώρημα 3.3.8, αν στη θέση του X βάλουμε το $T_1'N$).

Έστω ακέραιοι n_1 και n_2 τ.ω. $T_1'n_1 - S_1'n_2 = \frac{S_2' - T_2'}{2}$ (τα S_1', T_1' είναι σχετικά πρώτοι, άρα υπάρχουν τέτοιοι ακέραιοι, επίσης αφού είναι περιττοί-σαν δεύτεροι συντελεστές των μορφών Gauss- ο $\frac{S_2' - T_2'}{2}$ είναι ακέραιος).

Θέτουμε

$$b = T_2' + 2T_1'n_1 = S_2' + 2S_1'n_2$$

Έστω

$$G_j = \begin{bmatrix} 1 & 0 \\ n_j & 1 \end{bmatrix},$$

τότε οι μορφές

$$H_1 = G_1 * F_1' = [T_1', b, T_1'n_1^2 + T_2'n_1 + T_3']$$

και

$$H_2 = G_2 * F_2' = [S_1', b, S_1'n_2^2 + S_2'n_2 + S_3']$$

πληρούν τις προϋποθέσεις, αφού η H_1 είναι γνήσια ισοδύναμη με την F_1, η H_2 να είναι γνήσια ισοδύναμη με την F_2, ΜΚΔ(a_1, a_2)=ΜΚΔ(T_1', S_1')=1 και ΜΚΔ(a_1a_2, N)=

ΜΚΔ$(T_1'S_1', N)$ =1. Μένει να δείξουμε ότι οι μορφές H_1 και H_2 βρίσκονται σε αρμονία, ισχύει ότι έχουν ίδιο δεύτερο συντελεστή, τον b και πρέπει να δείξουμε ότι το S_1' διαιρεί το $T_1'n_1^2 + T_2'n_1 + T_3'$. Οι δύο μορφές έχουν ίδια διακρίνουσα, άρα $b^2 - 4T_1'(T_1'n_1^2 + T_2'n_1 + T_3') = b^2 - 4S_1'(S_1'n_2^2 + S_2'n_2 + S_3')$, δηλαδή $T_1'(T_1'n_1^2 + T_2'n_1 + T_3') = S_1'(S_1'n_2^2 + S_2'n_2 + S_3')$, επειδή όμως $(S_1', T_1') = 1$, συνεπάγεται ότι πράγματι $S_1'|T_1'n_1^2 + T_2'n_1 + T_3'$.

□

Θεώρημα 3.5.3:

Έστω ότι οι μορφές Gauss f_1 και f_2 είναι γνήσια ισοδύναμες με τις g_1 και g_2 αντίστοιχα. Έστω ότι η f_1 είναι σε αρμονία με την f_2 και η g_1 με την g_2, τότε η $f_1 \circ f_2$ είναι γνήσια ισοδύναμη με την $g_1 \circ g_2$.

Απόδειξη:

Έστω

$$f_1 = [a_1, b, c_1]$$

$$f_2 = [a_2, c, b_2]$$

$$g_1 = [a_1', b', c_1']$$

$$g_2 = [a_2', b', c_2']$$

Περίπτωση 1. $f_1 = g_1$ και ΜΚΔ$(a_1, a_2') = 1$.

Έχουμε ότι η f_2 είναι γνήσια ισοδύναμη με τη g_2, θεωρούμε λοιπόν τον πίνακα $G = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ που ανήκει στο $SL_2(\mathbb{Z})$ (άρα $ru - st = 1$), τέτοιο ώστε $G * f_2 = g_2$. Έχουμε υποθέσει ότι $f_1 = g_1$, άρα $b = b'$ και τότε

$$G \begin{bmatrix} a_2 & \frac{b}{2} \\ \frac{b}{2} & c_2 \end{bmatrix} = \begin{bmatrix} a_2' & \frac{b}{2} \\ \frac{b}{2} & c_2' \end{bmatrix} (G^T)^{-1}$$

Ο πάνω δεξιά όρος του πίνακα $G \begin{bmatrix} a_2 & \frac{b}{2} \\ \frac{b}{2} & c_2 \end{bmatrix}$ είναι $\frac{rb}{2} + sc_2$, ενώ του $\begin{bmatrix} a_2' & \frac{b}{2} \\ \frac{b}{2} & c_2' \end{bmatrix} (G^T)^{-1}$ είναι $-ta_2' + \frac{br}{2}$. Για να ισχύει η ισότητα των δύο πινάκων, θα πρέπει οι δύο αυτοί όροι να είναι ίσοι, δηλαδή

$$\frac{rb}{2} + sc_2 = -ta_2' + \frac{br}{2}$$

και συνεπάγεται ότι $sc_2 = -ta_2'$.

Αφού οι f_1 και f_2 βρίσκονται σε αρμονία, έχουμε ότι $a_1|c_2$, τότε με τη βοήθεια της ισότητας $sc_2 = -ta_2'$, πρέπει $a_1|ta_2'$, επειδή όμως τα a_1 και a_2' είναι πρώτα μεταξύ τους (από την υπόθεση που κάναμε), θα πρέπει $a_1|t$, δηλαδή ο $\frac{t}{a_1}$ είναι ακέραιος. Τώρα θεωρούμε τον πίνακα

$$G' = \begin{bmatrix} r & sa_1 \\ \frac{t}{a_1} & u \end{bmatrix},$$

ο οποίος έχει ακέραιους όρους και $detG' = ru - sa_1\frac{t}{a_1} = ru - st = 1$, άρα ανήκει στο $SL_2(\mathbb{Z})$. Αν δείξουμε ότι ισχύει η σχέση $G' * (f_1 \circ f_2) = g_1 \circ g_2$, σημαίνει ότι η $f_1 \circ f_2$ είναι γνήσια ισοδύναμη με την $g_1 \circ g_2$ και έχουμε τελειώσει.

Είναι $f_1 \circ f_2 = [a_1a_2, b, \frac{c_1}{a_2}]$ και $g_1 \circ g_2 = [a_1'a_2', b', \frac{c_1'}{a_2'}]$, τότε η σχέση $G * (f_1 \circ f_2) = g_1 \circ g_2$ μας δίνει:

$$[a_1a_2r^2 + brsa_1 + \frac{c_1}{a_2}s^2a_1^2, 2a_2rt + b(ru+st) + 2\frac{c_1}{a_2}sa_1u, a_2\frac{t^2}{a_1} + b\frac{t}{a_1}u + \frac{c_1}{a_2u^2}] = [a_1'a_2', b', \frac{c_1'}{a_2'}]$$

Θα δείξουμε ότι οι πρώτοι όροι είναι ίσοι, δηλαδή ότι $a_1a_2r^2 + brsa_1 + \frac{c_1}{a_2}s^2a_1^2 = a_1'a_2'$.

Έχουμε ότι $f_1 = g_1$, άρα $a_1 = a_1'$, $b = b'$ και $c_1 = c_1'$. Επίσης από την σχέση $G * f_2 = g_2$ παίρνουμε ότι $a_2r^2 + brs + c_2s^2 = a_2'$, τότε $a_1a_2r^2 + brsa_1 + \frac{c_1}{a_2}s^2a_1^2 = a_1a_2r^2 + brsa_1 + \frac{c_2}{a_1}s^2a_1^2 = a_1a_2r^2 + brsa_1 + c_2s^2a_1 = a_1(a_2r^2 + brs + c_2s^2) = a_1'a_2'$.

Ομοίως για τους υπόλοιπους όρους.

Περίπτωση 2. $b = b'$ και ΜΚΔ$(a_1, a_2') = 1$.

Έχουμε $D = b^2 - 4a_1c_1$ και $D = b'^2 - 4a_2'c_2' = b^2 - 4a_2'c_2'$, τότε $a_1c_1 = a_2'c_2'$ και αφού ΜΚΔ$(a_1, a_2') = 1$, συνεπάγεται ότι $a_1|c_2'$. Αφού λοιπόν ισχύει ότι $b = b'$ και $a_1|c_2'$, έπεται ότι οι μορφές f_1 και g_2 βρίσκονται σε αρμονία. Έχουμε λοιπόν ότι $\frac{c_2'}{a_1} = \frac{c_1}{a_2'}$, αυτό σημαίνει πως οι μορφές $g_2 \circ f_1 = [a_1a_2', b, \frac{c_2'}{a_1}]$ και $f_1 \circ g_2 = [a_1a_2', b, \frac{c_1}{a_2'}]$ είναι ίσες.

Με εφαρμογή της περίπτωσης 1, παίρνουμε ότι η $g_2 \circ g_1$ είναι γνήσια ισοδύναμη με την $g_2 \circ f_1$ και ότι η $f_1 \circ f_2$ είναι γνήσια ισοδύναμη με την $f_1 \circ g_2$, που όπως δείξαμε είναι ίση με την $g_2 \circ f_1$, άρα η μορφή $g_1 \circ g_2$ είναι γνήσια ισοδύναμη με την $f_1 \circ f_2$.

Περίπτωση 3. ΜΚΔ$(a_1a_2, a_1'a_2')$=1.

Τότε θα υπάρχουν ακέραιοι n και n', τέτοιοι ώστε $a_1a_2n - a_1'a_2'n' = \frac{b-b'}{2}$ (ο $\frac{b-b'}{2}$ είναι ακέραιος, αφού οι b και b' από τον ορισμό των μορφών Gauss είναι περιττοί) και θέτουμε

$$B = b + 2a_1a_2n = b' + 2a_1'a_2'n'.$$

Ορίζουμε:

$$F_1 = \begin{bmatrix} 1 & 0 \\ a_2n & 1 \end{bmatrix} * f_1 = [a_1, B, *]$$

$$F_2 = \begin{bmatrix} 1 & 0 \\ a_1n & 1 \end{bmatrix} * f_2 = [a_2, B, *]$$

$$H_1 = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} * (f_1 \circ f_2) = [a_1a_2, B, *]$$

$$G_1 = \begin{bmatrix} 1 & 0 \\ a_2'n' & 1 \end{bmatrix} * g_1 = [a_1', B, *]$$

$$G_2 = \begin{bmatrix} 1 & 0 \\ a_1'n' & 1 \end{bmatrix} * g_2 = [a_2', B, *]$$

$$H_2 = \begin{bmatrix} 1 & 0 \\ n' & 1 \end{bmatrix} * (g_1 \circ g_2) = [a_1'a_2', B, *]$$

Από την ισότητα της διακρίνουσας ($D = b^2 - 4ac$) για την περίπτωση της μορφής H_1, έχουμε ότι $D = B^2 - 4a_1a_2*$, δηλαδή $a_1a_2|\frac{B^2-D}{4}$.

Αν $F_1 = [a_1, B, c_1]$, τότε η ισότητα της διακρίνουσας μας δίνει $D = B^2 - 4a_1c_1$, δηλαδή $c_1 = \frac{B^2-D}{4a_1}$, τότε όμως $a_2|c_1 = \frac{B^2-D}{4a_1}$, αφού όπως δείξαμε $a_1a_2|\frac{B^2-D}{4}$. Άρα οι μορφές Gauss F_1 και F_2 βρίσκονται σε αρμονία.

Όμοια σε αρμονία βρίσκονται και οι μορφές Gauss G_1 και G_2.

Από την περίπτωση 2 οι $F_1 \circ F_2$ και $G_1 \circ G_2$ είναι γνήσια ισοδύναμες (έχουμε υποθέσει ότι ΜΚΔ$(a_1a_2, a_1'a_2')$=1, άρα ΜΚΔ$(a_1, a_2') = 1$ και η υπόθεση της περίπτωσης 2 ισχύει για τις μορφές F_1, F_2, G_1 και G_2).

Ο τρίτος συντελεστής c μιας μορφής Gauss $[a, b, c]$ ορίζεται μονοσήμαντα από την διακρίνουσα, το a και το b. Αυτό σημαίνει ότι αν δύο μορφές έχουν την ίδια

διακρίνουσα και ίδιους τους δύο πρώτους συντελεστές θα πρέπει να έχουν και τον τρίτο συντελεστή ίδιο, άρα οι δύο μορφές πρέπει να ταυτίζονται. Σύμφωνα με την παρατήρηση αυτή έχουμε ότι $H_1 = F_1 \circ F_2$ και $H_2 = G_1 \circ G_2$.

Έχουμε δείξει όμως ότι οι μορφές $F_1 \circ F_2$ και $G_1 \circ G_2$ είναι γνήσια ισοδύναμες, άρα και η H_1 είναι γνήσια ισοδύναμη με την H_2. Από τον ορισμό των H_1 και H_2, η μορφή H_1 είναι γνήσια ισοδύναμη με την $f_1 \circ f_2$ και η H_2 με την $g_1 \circ g_2$, άρα η $f_1 \circ f_2$ είναι γνήσια ισοδύναμη με την $g_1 \circ g_2$.

Περίπτωση 4. Χωρίς ειδικούς περιορισμούς.

Από το θεώρημα 3.5.2, υπάρχουν μορφές Gauss:

$$F_1 = [A_1, B_1, *]$$

$$F_2 = [A_2, B_2, *]$$

τέτοιες ώστε η F_1 να είναι γνήσια ισοδύναμη με τις f_1 και g_1, η F_2 να είναι γνήσια ισοδύναμη με τις f_2 και g_2, οι F_1 και F_2 να βρίσκονται σε αρμονία και

$$MK\Delta(A_1, A_2) = MK\Delta(A_1A_2, a_1a_2a_1'a_2') = 1.$$

Άρα ΜΚΔ$(a_1a_2, A_1A_2) = 1$, τότε από την περίπτωση 3 η $f_1 \circ f_2$ είναι γνήσια ισοδύναμη με την $F_1 \circ F_2$. Όμοια η $g_1 \circ g_2$ είναι γνήσια ισοδύναμη με την $F_1 \circ F_2$, άρα η $f_1 \circ f_2$ είναι γνήσια ισοδύναμη με την $g_1 \circ g_2$.

□

Τώρα μπορούμε να ορίσουμε πράξη στο σύνολο C. Έστω $[F]$ η κλάση ισοδυναμίας που ορίζει η μορφή Gauss F. Έστω F_1 και F_2 δύο τυχαίες μορφές Gauss (με την ίδια διακρίνουσα D) και μορφές H_1 και H_2 που είναι γνήσια ισοδύναμες με τις F_1 και F_2 αντίστοιχα, και βρίσκονται σε αρμονία (τέτοιες μορφές υπάρχουν από το θεώρημα 3.5.2). Ορίζουμε την πράξη

$$[F_1][F_2] = [H_1 \circ H_2].$$

Από το θεώρημα 3.5.3 η πράξη είναι καλά ορισμένη (δηλαδή αν επιλέξουμε διαφορετικές μορφές από κάθε κλάση δεν αλλάζει η κλάση που θα πάρουμε). Η πράξη είναι αντιμεταθετική ($[F_1][F_2] = [H_1 \circ H_2] = [H_2 \circ H_1] = [F_2][F_1]$) και θα αποδείξουμε ότι είναι και προσεταιριστική.

Θεώρημα 3.5.4:

Η παραπάνω πράξη είναι προσεταιριστική, δηλαδή

$$([f_1][f_2])[f_3] = [f_1]([f_2][f_3])$$

Απόδειξη:

Έστω $f_3 = [a_3, b_3, c_3]$, από το θεώρημα 3.5.2 υπάρχουν μορφές Gauss H_1 και H_2 τέτοιες ώστε η H_1 να είναι γνήσια ισοδύναμη με την f_1, η H_2 να είναι γνήσια ισοδύναμη με την f_2 και αν a_1, a_2 είναι οι πρώτοι συντελεστές των μορφών H_1 και H_2 αντίστοιχα, να ισχύει ΜΚΔ(a_1, a_2) =ΜΚΔ$(a_1a_2, a_3) = 1$.

Έστω b_1 και b_2 οι δεύτεροι συντελεστές των μορφών H_1 και H_2 αντίστοιχα (εξ' ορισμού έχουμε ότι τα b είναι περιττά, άρα $\frac{b_1-b_2}{2} \in \mathbb{Z}$). Τότε αφου ΜΚΔ$(a_1, a_2)$ =1, θα υπάρχουν ακέραιοι n_1, n_2 τ.ω.

$$a_2n_2 - a_1n_1 = \frac{b_1 - b_2}{2}$$

Επίσης ΜΚΔ$(a_1a_2, a_3) = 1$, άρα υπάρχουν ακέραιοι n_3 και k τ.ω.

$$a_3n_3 - a_1a_2k = a_1n_1 + \frac{b_1 - b_3}{2}.$$

Θέτουμε

$$n_1' = n_1 + ka_2$$

$$n_2' = n_2 + ka_1$$

$$n_3' = n_3$$

τότε

$$b_1 + 2a_1n_1' = b_2 + 2a_2n_2' = b_3 + 2a_3n_3'.$$

Είναι εύκολο να δούμε ότι αυτό ισχύει με απλή αντικατάσταση των παραπάνω τύπων. Για παράδειγμα ας ελέγξουμε την πρώτη ισότητα, $b_1 + 2a_1n_1' = b_1 + 2a_1(n_1 + ka_2) = b_1 + 2a_1n_1 + 2a_1ka_2 = 2a_2n_2 - 2a_1n_1 + b_2 + 2a_1n_1 + 2a_1ka_2 = b_2 + 2a_2n_2 +$

$2ka_1a_2 = b_2 + 2a_2(n_2 + ka_1) = b_2 + 2a_2n_2'$. Ας ονομάσουμε αυτή την ποσότητα B. Για $i = 1, 2, 3$ θεωρούμε τον πίνακα

$$G_i = \begin{bmatrix} 1 & 0 \\ n_i' & 1 \end{bmatrix}$$

Έστω

$$F_1 = G_1 * H_1 = [a_1, 2a_1n_1' + b_1, *] = [a_1, B, *]$$

$$F_2 = G_2 * H_2 = [a_2, 2a_2n_2' + b_2, *] = [a_2, B, *]$$

$$F_3 = G_3 * f_3 = [a_1, 2a_3n_3' + b_3, *] = [a_3, B, *]$$

Οι μορφές F_1, F_2 και F_3 βρίσκονται σε αρμονία ανά δύο. Αυτό ισχύει γιατί όλες έχουν ίδιο το δεύτερο συντελεστή B και τότε από τον τύπο της διακρίνουσας $(D = B^2 - 4a_ic_i)$ παίρνουμε τη σχέση $a_1c_1 = a_2c_2 = a_3c_3$. Όμως, αφού τα a_1, a_2, a_3 είναι πρώτα μεταξύ τους θα πρέπει να ισχύει και η δεύτερη συνθήκη των αρμονικών μορφών, δηλαδή ότι το a της μίας μορφής διαιρεί το c της άλλης. Τώρα

$$([f_1][f_2])[f_3] = [F_1 \circ F_2][F_3] = [\left[a_1a_2, B, *\right]][F_3] = [a_1a_2a_3, B, *]$$

και

$$[f_1]([f_2][f_3]) = [F_1][F_2 \circ F_3] = [F_1][\left[a_2a_3, B, *\right]] = [a_1a_2a_3, B, *]$$

Άρα $([f_1][f_2])[f_3] = [f_1]([f_2][f_3])$ (δύο μορφές με ίδια D, a και b, αναγκαστικά έχουν και ίδιο c, δηλαδή είναι ίσες).

□

Θεώρημα 3.5.5:

Το πεπερασμένο σύνολο των κλάσεων ισοδυναμίας των μορφών Gauss, με την πράξη που ορίσαμε, αποτελεί αβελιανή ομάδα με ταυτοτικό στοιχείο την κλάση $[\left[1, 1, \frac{1-D}{4}\right]]$ και αντίστροφο του στοιχείου $[\left[a, b, c\right]]$ το $[\left[c, b, a\right]]$.

Απόδειξη:

Από το προηγούμενο θεώρημα έχουμε ότι η πράξη είναι προσεταιριστική. Με τη βοήθεια του πίνακα

$$\begin{bmatrix} 1 & 0 \\ \frac{b-1}{2} & 1 \end{bmatrix}$$

βλέπουμε ότι οι μορφές $[1, 1, \frac{1-D}{4}]$ και $[1, b, \frac{b^2-D}{4}]$ είναι γνήσια ισοδύναμες, τότε

$$[\left[a, b, c\right]][\left[1, 1, \frac{1-D}{4}\right]] = [\left[a, b, c\right]][\left[1, b, \frac{b^2-D}{4}\right]]$$

$$= [\left[a, b, c\right]]$$

(Οι μορφές $[a, b, c]$ και $[1, b, \frac{b^2-D}{4}]$ βρίσκονται σε αρμονία, αφού $b = b$ και $a_2 = 1|c = c_1$, άρα $[a, b, c] \circ [1, b, \frac{b^2-D}{4}] = [a \cdot 1, b, \frac{c}{1}] = [a, b, c]$).

Έχουμε λοιπόν ότι το ταυτοτικό στοιχείο είναι το $[\left[1, 1, \frac{1-D}{4}\right]]$ (η πράξη είναι αντιμεταθετική και δεν χρειάζεται να δείξουμε και ότι $[\left[1, 1, \frac{1-D}{4}\right]][\left[a, b, c\right]] = [\left[a, b, c\right]]$).

Θα δείξουμε ότι το αντίστροφο του στοιχείου $[\left[a, b, c\right]]$ είναι το $[\left[c, b, a\right]]$. Έχουμε

$$[\left[a, b, c\right]][\left[c, b, a\right]] = [\left[ac, b, 1\right]]$$

(προφανώς οι δύο μορφές είναι σε αρμονία αφού $b = b$ και $a|a$).

Χρησιμοποιώντας τον πίνακα

$$\begin{bmatrix} 0 & 1 \\ -1 & \frac{b+1}{2} \end{bmatrix}$$

βλέπουμε ότι οι μορφές $[ac, b, 1]$ και $[1, 1, \frac{1-D}{4}]$ είναι γνήσια ισοδύναμες. Άρα πράγματι το αντίστροφο στοιχείο $[\left[a, b, c\right]]$ είναι το $[\left[c, b, a\right]]$. Δηλαδή το πεπερασμένο σύνολο των κλάσεων ισοδυναμίας των μορφών Gauss, με την (αντιμεταθετική) πράξη που ορίσαμε αποτελεί αβελιανή ομάδα.

□

Μία μορφή Gauss f θα λέγεται **αυτο-αντίστροφη (self-inverse)** αν και μόνο αν $[f][f] = [\left[1, 1, \frac{1-D}{4}\right]]$. Επίσης, η κλάση $[f]$ θα λέγεται αυτο-αντίστροφη αν και μόνο αν είναι η f.

Θεώρημα 3.5.6:

Μία μορφή Gauss είναι αυτο-αντίστροφη αν και μόνο αν είναι ασαφής.

Απόδειξη:

($\Rightarrow$)

Ας υποθέσουμε ότι η μορφή Gauss $f = [a, b, c]$ είναι αυτο-αντίστροφη, δηλαδή η αντίστροφη κλάση της $[\left[a, b, c\right]]$ είναι η ίδια η $[\left[a, b, c\right]]$, όμως από το προηγούμενο θεώρημα έχουμε ότι η αντίστροφη κλάση της $[\left[a, b, c\right]]$ είναι η $[\left[c, b, a\right]]$, άρα $[\left[a, b, c\right]] = [\left[c, b, a\right]]$. Αυτό σημαίνει ότι οι μορφές $[a, b, c]$ και $[c, b, a]$ είναι γνήσια ισοδύναμες, τότε από το θεώρημα 3.5.1 συνεπάγεται ότι η μορφή $[f]$ είναι ασαφής.

($\Leftarrow$)

Ας υποθέσουμε ότι η μορφή $f = [a, b, c]$ είναι ασαφής, τότε από το θεώρημα 3.5.1 είναι γνήσια ισοδύναμη με την $[c, b, a]$, άρα $[\left[a, b, c\right]] = [\left[c, b, a\right]]$, όμως η $[\left[c, b, a\right]]$ όπως είδαμε στο προηγούμενο θεώρημα είναι η αντίστροφη κλάση της $[\left[a, b, c\right]]$, άρα η $[f]$ έχει αντίστροφο στοιχείο τον εαυτό της, άρα η f είναι αυτο-αντίστροφη.

□

Έστω C η ομάδα των κλάσεων ισοδυναμίας, όπως την ορίσαμε παραπάνω. Θεωρούμε τον ομομορφισμό $sq : C \to C$ τ.ω. $sq([f]) = [f][f]$. Ο πυρήνας του sq είναι το σύνολο των αυτο-αντίστροφων μορφών. Η εικόνα $im(sq)$ είναι το σύνολο των μορφών που μπορούν να γραφούν σαν $[f][f]$ -δηλαδή τα 'τετράγωνα'- και $ker(sq)$ ο πυρήνας του sq, τότε από το πρώτο θεώρημα των ισομορφισμό ομάδων έχουμε

$$|C| = |Ker(sq)| \cdot |im(sq)|.$$

Ο πυρήνας $Ker(sq)$ είναι το σύνολο των κλάσεων που απεικονίζονται μέσω του sq στη μοναδιαία κλάση $[\left[1, 1, \frac{1-D}{4}\right]]$. Αυτές όμως είναι είναι οι αυτο-αντίστροφες

κλάσεις, δηλαδή οι κλάσεις που περιέχουν αυτο-αντίστροφη μορφή. Όμως οι αυτο-αντίστροφες μορφές είναι ακριβώς οι ασαφείς μορφές, τότε οι αυτο-αντίστροφες κλάσεις είναι ακριβώς όσες είναι και οι ασαφείς κλάσεις. Οι ασαφείς κλάσεις είναι όσες και οι ειδικές ασαφείς κλάσεις (από τον ορισμό των ασαφών μορφών μία κλάση είναι ασαφής αν και μόνο αν είναι ειδική ασαφής), οι οποίες όπως είδαμε στο κεφάλαιο 3.1 είναι 2^{r-1} (όπου r το πλήθος των διακεκριμένων πρώτων διαιρετών του D), άρα $|Ker(sq)| = 2^{r-1}$ και η παραπάνω σχέση δίνει

$$|C| = 2^{r-1} \cdot |im(sq)|.$$

Με το παρακάτω θεώρημα θα συνδέσουμε αυτό το κεφάλαιο με τις τετραγωνικές μορφές του προηγούμενου κεφαλαίου.

Θεώρημα 3.5.7:

Μία μορφή Gauss g είναι τετραγωνική μορφή αν και μόνο αν $[g] \in im(sq)$.

Απόδειξη:

($\Rightarrow$)

Έστω ότι η g είναι τετραγωνική μορφή, αυτό σημαίνει ότι υπάρχουν δύο γνήσια ισοδύναμες μορφές F και F', οι οποίες βρίσκονται σε αρμονία τέτοιες ώστε η g να είναι γνήσια ισοδύναμη με την $F \circ F'$, τότε

$$[g] = [F \circ F'] = [F][F'] = [F][F],$$

άρα $[g] \in im(sq)$.

($\Leftarrow$)

Αν $[g] \in im(sq)$ τότε $[g] = [f][f] = [f' \circ f'']$, για κάποιες μορφές f' και f'', οι οποίες βρίσκονται σε αρμονία, με f' γνήσια ισοδύναμη με την f και f'' γνήσια ισοδύναμη με την f. Άρα η g είναι γνήσια ισοδύναμη με την $f' \circ f''$, με τις f' και f'' γνήσια ισοδύναμες και σε αρμονία, άρα η g είναι τετραγωνική μορφή.

□

Ας θυμηθούμε ότι μία κλάση omega kernel είναι μία κλάση του C η οποία περιέχει μία μορφή omega kernel (δηλαδή μία μορφή που να αναπαριστά ένα στοιχείο του H). Επίσης συμβολίσαμε με K το σύνολο των κλάσεων omega kernel. Στο προηγούμενο θεώρημα δείξαμε ότι $[f] \in im(sq)$ αν και μόνο αν είναι τετραγωνική μορφή,

δηλαδή (από θεώρημα 3.4.3) αν και μόνο αν είναι omega kernel, τότε $|im(sq)| = |K|$ και έχουμε $\frac{|C|}{|K|} = 2^{r-1}$. Προκύπτει λοιπόν το ακόλουθο θεώρημα:

Θεώρημα 3.5.8:

Ο αριθμός των κλάσεων ισοδυναμίας του C είναι 2^{r-1} φορές ο αριθμός των κλάσεων ισοδυναμίας που αναπαριστούν κάποιο στοιχείο του H, όπου r το πλήθος των διακεκριμένων πρώτων διαιρετών του D.

3.6 Αθροίσματα τρίγωνων αριθμών

Έστω U το σύνολο των κλάσεων $x \pmod D$ με $(x, D) = 1$. Για $x \in U$ ορίζουμε $J(m) = (\frac{m}{-D})$ (σύμβολο του Jacobi). Αφού $-D \equiv 3 \pmod 4$ (δηλαδή ο $\frac{-D-1}{2}$ είναι περιττός), έπεται ότι $J(-1) = (-1)^{\frac{-D-1}{2}} = -1$. Αν $x \in U$, το ίδιο θα ισχύει και για το $-x$ και $J(-x) = J(-1)J(x) = -J(x)$. Αυτό σημαίνει ότι τα μέλη του U χωρίζονται σε δύο ισοπληθικά σύνολα, σε αυτά που έχουν σύμβολο του Jacobi ίσο με 1 και αυτά που έχουν σύμβολο του Jacobi ίσο με -1. Κάθε σύνολο έχει πληθάριθμο $\frac{\phi(|D|)}{2}$ (ο D είναι αρνητικός).

Έστω $KerJ$ το σύνολο των στοιχείων του U με σύμβολο $Jacobi$ ίσο με 1. Το $KerJ$ είναι υποομάδα της πολλαπλασιαστικής ομάδας U. Είναι υποσύνολο του U και είναι ομάδα αφού ισχύει η προσεταιριστικότητα από ιδιότητες του συμβόλου Jacobi, ουδέτερο στοιχείο είναι το 1 που ανήκει στο $KerJ$, αφού $J(1) = -J(-1) = -(-1) = 1$ και αν x^{-1} το αντίστροφο του x (το αντίστροφο υπάρχει αφου U πολλαπλασιαστική ομάδα), τότε

$$x \cdot x^{-1} = 1 \Rightarrow J(x)J(x^{-1}) = J(1) \Rightarrow 1 \cdot J(x^{-1}) = 1 \Rightarrow J(x^{-1}) = 1,$$

άρα $x^{-1} \in KerJ$.

Επιπλέον το H είναι υποομάδα του $KerJ$. Από το θεώρημα 3.4.1 το H έχει $\frac{\phi(|D|)}{2^r}$ στοιχεία, όπου r το πλήθος των διακεκριμένων πρώτων διαιρετών του D. Αφού το $KerJ$ έχει $\frac{\phi(|D|)}{2}$ στοιχεία, η ομάδα πηλίκο $KerJ/H$ θα έχει 2^{r-1} στοιχεία.

Θεώρημα 3.6.1:

Αν ένας ακέραιος m είναι πρώτος με τον D και αναπαρίσταται από μία μορφή Gauss, τότε $J(m) = 1$.

Απόδειξη:

Έστω $f = [a, b, c]$ η μορφή Gauss που αναπαριστά τον ακέραιο m, δηλαδή υπάρχουν ακέραιοι r, s με $m = ar^2 + brs + cs^2$. Έστω $k = MK\Delta(r, s)$ (άρα το k^2 διαιρεί το m), τότε υπάρχουν ακέραιοι t και u τ.ω. $\frac{r}{k}u - \frac{s}{k}t = 1$. Θεωρούμε τον πίνακα

$$G = \begin{bmatrix} \frac{r}{k} & \frac{s}{k} \\ t & u \end{bmatrix}.$$

Ο πίνακας G ανήκει στο $SL_2(\mathbb{Z})$ και $G * F = [\frac{m}{k^2}, b, c]$. Από τον τύπο της διακρίνουσας έχουμε $D = b^2 - 4\frac{m}{k^2}c$, δηλαδή $D \equiv b^2 \pmod{\frac{m}{k^2}}$.

Έστω $m = 2^e m'$, όπου e μη αρνητικός ακέραιος και m' περιττός.

Αν ο e είναι περιττός, τότε ο $\frac{m}{k^2}$ θα είναι άρτιος (το k^2 σαν τετράγωνο διαιρείται από άρτια δύναμη του 2, άρα αν ο m διαιρείται από περιττή δύναμη του 2, κατά τη διαίρεση $\frac{m}{k^2}$, θα έχουμε τουλάχιστον ένα 2 στους παράγοντες του ακεραίου $\frac{m}{k^2}$). Αφού ο $\frac{m}{k^2}$ είναι άρτιος, η σχέση $D = b^2 - 4\frac{m}{k^2}c$ μας δίνει $b^2 \equiv D \pmod 8$, όμως ο b είναι περιττός, δηλαδή $b = 2k + 1$ και έχουμε $4k^2 + 4k + 1 \equiv D \pmod 8$, δηλαδή $4k(k + 1) + 1 \equiv D \pmod 8$, όμως ο $k(k + 1)$ είναι άρτιος, άρα $D \equiv 1 \pmod 8$ και έπεται ότι $J(2) = 1$ ($(\frac{2}{K}) = 1$, αν $K \equiv \pm 1 \pmod 8$). Τότε $J(2^e) = J(2)^e = 1^e = 1$.

Αν ο e είναι άρτιος τότε $J(2^e) = J(2)^e = 1$. Άρα σε κάθε περίπτωση έχουμε ότι $J(2^e) = 1$.

Τώρα θα υπολογίσουμε το $J(m')$. Αφού $D \equiv 1 \pmod 4$, ο $\frac{-D-1}{2}$ θα είναι περιττός. Από τον τετραγωνικό νόμο αντιστροφής έχουμε ότι

$$J(m') = (\frac{-D}{m'})(-1)^{\frac{m'-1}{2}\frac{-D-1}{2}} = (\frac{-D}{m'})(-1)^{\frac{m'-1}{2}}.$$

Όμως $(\frac{-D}{m'}) = (\frac{-Dk^2}{m'})$ και από την σχέση $D = b^2 - 4\frac{2^e m'}{k^2}c$, έχουμε ότι $Dk^2 \equiv b^2k^2 \pmod{m'}$, άρα

$$(\frac{-D}{m'}) = (\frac{-Dk^2}{m'}) = (\frac{-b^2k^2}{m'}) = (\frac{-1}{m'})(\frac{b^2}{m'})(\frac{k^2}{m'}) = (-1)^{\frac{m'-1}{2}}$$

και τότε $J(m') = (-1)^{\frac{m'-1}{2}}(-1)^{\frac{m'-1}{2}} = (-1)^{m'-1} = 1$ (αφού ο m' είναι περιττός).

Οπότε $J(m) = J(2^e)J(m') = 1 \cdot 1 = 1$.

□

Θεώρημα 3.6.2:

Έστω ότι μια μορφή Gauss f αναπαριστά τους ακεραίους m και n, με $MK\Delta(m, D) = MK\Delta(n, D) = 1$. Τότε, αν ο n^{-1} είναι ο αντίστροφος του $n \pmod D$, $mn^{-1} \in H$.

Απόδειξη:

Έστω $f = [a, b, c]$, τότε $m = ar^2 + brs + cs^2$ και $n = at^2 + btu + cu^2$. Θεωρούμε τον πίνακα

$$G = \begin{bmatrix} r & s \\ t & u \end{bmatrix}.$$

Είναι

$$G \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} G^T = \begin{bmatrix} m & \frac{k}{2} \\ \frac{k}{2} & n \end{bmatrix},$$

με $k = 2art + sbt + rbu + 2csu \in \mathbb{Z}$. Εξισώνοντας τις ορίζουσες, έχουμε

$$\frac{-D}{4}(detG)^2 = mn - \frac{k^2}{4}$$

και άρα $4mn = k^2 + QD$. Όμως κάθε τετράγωνο είναι στοιχείο του H, άρα και το $4mn \in H$. Το H είναι ομάδα, άρα αν B το αντίστροφο του $(2n)^2 \in H$, θα πρέπει και $B \in H$. Τότε και το γινόμενο $4mnB = 4mn(2n)^{-2} = mn^{-1}$ ανήκει στο H.

□

Αφού το H είναι υποομάδα του U, μπορούμε να ορίσουμε την ομάδα πηλίκο U/H. Από το προηγούμενο θεώρημα, αν η $f = [a, b, c]$ αναπαριστά τους m, n, οι οποίοι είναι πρώτοι με το D, τότε $mH = nH$ (αρκεί $m \in nH$, από το θεώρημα έχουμε ότι $mn^{-1} \in H$ άρα $n(mn^{-1}) \in nH$, δηλαδή $m \in nH$).

Επίσης, όλες οι μορφές της ίδιας κλάσεις αναπαριστούν τους ίδιους ακεραίους. Σύμφωνα με αυτές τις δύο παρατηρήσεις, μπορούμε να ορίσουμε την συνάρτηση

$$\omega : C \to U/H$$

$$[f] \mapsto mH$$

όπου m ακέραιος, πρώτος με το D, ο οποίος αναπαρίσταται από την μορφή f.

Θεώρημα 3.6.3:

Ο ω είναι ομομορφισμός ομάδων με πυρήνα K (το σύνολο των κλάσεων omega kernel).

Απόδειξη:

Για να δείξουμε ότι είναι ομομορφισμός αρκεί να δείξουμε ότι $(\omega[f])(\omega[g]) = \omega([f][g])$.

$(\omega[f])(\omega[g]) = pqH$, όπου p ακέραιος στο U που αναπαρίσταται από την f και q ακέραιος στο U που αναπαρίσταται από την g. Να σημειώσουμε ότι το pq είναι στοιχείο του U.

Έστω f' και g' μορφές σε αρμονία, με f' γνήσια ισοδύναμη με την f και g' γνήσια ισοδύναμη με την g (τέτοιες μορφές υπάρχουν από το θεώρημα 3.5.2), τότε η $f' \circ g'$ αναπαριστά τον pq (θεώρημα 3.4.2), άρα $\omega([f][g]) = \omega([f' \circ g']) = pqH$, δηλαδή πράγματι $(\omega[f])(\omega[g]) = \omega([f][g])$.

Επιπλέον $\omega[f] = H$ μόνο στην περίπτωση που η f αναπαριστά έναν αριθμό της μορφής $x + QD$, με $x \in H$- δηλαδή αν η f είναι μορφή omega kernel.

□

Τότε από το πρώτο θεώρημα των ισομορφισμό ομάδων έχουμε $|C| = |Ker\omega| \cdot |im(\omega)|$, δηλαδή

$$|im(\omega)| = \frac{|C|}{|K|}$$

το οποίο όπως δείξαμε στο θεώρημα 3.5.8 ισούται με 2^{r-1}, όπου r ο αριθμός των διακεκριμένων πρώτων διαιρετών του D.

Η εικόνα $im(\omega)$ είναι υποσύνολο του $Ker(J)/H$ (έστω $mH \in im(\omega)$, τότε $m \in \mathbb{Z}$, $(m, D) = 1$ και το m αναπαρίσταται από μία μορφή Gauss f, από το θεώρημα 3.6.1 $J(m) = 1$, άρα $m \in KerJ$, δηλαδή $mH \in Ker(J)/H$), που όπως είδαμε στην αρχή του κεφαλαίου έχει 2^{r-1} στοιχεία.

Έχουμε λοιπόν το ακόλουθο θεώρημα:

Θεώρημα 3.6.4:

$$im(\omega) = Ker(J)/H$$

Τέλος έχουμε

Θεώρημα 3.6.5:

Κάθε θετικός ακέραιος Z είναι άθροισμα τριών τρίγωνων αριθμών.

Απόδειξη:

Έστω $u = 8Z + 3$ και $D = -u$. Τότε $J(-2) = (\frac{-2}{-D}) = (\frac{-2}{u}) = (-1)^{\frac{u-1}{2}}(\frac{2}{u}) = 1 \cdot 1 = 1$ (ο $\frac{u-1}{2}$ είναι άρτιος και $u \equiv 3 \pmod 8$), δηλαδή $-2 \in KerJ$ και από το θεώρημα 3.6.4 υπάρχει μία μορφή Gauss f τέτοια ώστε $\omega[f] = -2H$. Από το θεώρημα 3.5.2 για $F_1 = f$, $F_2 = f$ και $N = D$, υπάρχει μορφή $[a', b, c']$ στην κλάση

$[f]$, με $(a'a', D) = 1$, δηλαδή με $(a', D) = 1$. Τώρα από το θεώρημα 3.6.2 για $m = a'$ και $n = -2$ ισχύει ότι $a'(-2)^{-1} \equiv h \pmod{D}$ για κάποιο $h \in H$, δηλαδή $a' \equiv -2h \pmod{D}$.

Θέτουμε $a = 2a'$ και $c = 2c'$, τότε $ac - b^2 = 4a'c' - b^2 = -D = u$.

Έστω z λύση της $z^2 \equiv h \pmod{D}$ (η ισοτιμία έχει λύση αφού $h \in H$), τότε $z \in U$ και έστω z^{-1} το αντίστροφό του $\pmod{D}$. Έπεται ότι:

$$-a = -2a' \equiv 4h \equiv (2z)^2 \pmod{u}.$$

Έστω $N = 2z$, τότε $N \in U$ (είναι $(z, D) = 1$ και $(2, D) = 1$, άρα και $(2z, D) = 1$). Άρα θα υπάρχει ο N^{-1} και θα υπάρχει επίσης ένας ακέραιος Μ που να είναι ισότιμος με τον $N^{-1}b \pmod{u}$, τότε $MN = b \pmod{u}$.

Είναι
$$\begin{aligned} -c \equiv -(N^{-1})^2 N^2 c &\equiv (N^{-1})^2 ac \quad (\text{αφού έχουμε ότι } -N^2 \equiv a \pmod{u}) \\ &\equiv (N^{-1})^2 b^2 \quad (\text{αφού } ac - b^2 = u) \\ &\equiv M^2 \pmod{u} \end{aligned}$$

Ορίζουμε τους παρακάτω έξι ακεραίους:

$$C = \frac{a + N^2}{u} \qquad (-a \equiv N^2 \pmod{u}, \text{ άρα } C \in \mathbb{Z})$$

$$B = \frac{MN - b}{u} \qquad (b \equiv MN \pmod{u}, \text{ άρα } B \in \mathbb{Z})$$

$$A = \frac{c + M^2}{u} \qquad (-c \equiv M^2 \pmod{u}, \text{ άρα } A \in \mathbb{Z})$$

$$m = BN - CM = \frac{-aM - bN}{u}$$

$$n = BM - AN = \frac{-bM - cN}{u}$$

$$s = AC - B^2 = \frac{1 - mM - nN}{u}$$

Ισχύουν οι ισότητες $bn - cm = M$, $an - bm = -N$ και $1 - mM - nN = su$.

(Η πρώτη ισότητα ισχύει αφού

$$bn - cm = b\frac{-bM - cN}{u} - c\frac{-aM - bN}{u} = \frac{-b^2M - bcN + acM + bcN}{u} =$$

$$= \frac{-b^2 + ac}{u}M = \frac{-D}{u}M = M,$$

όμοια για τις υπόλοιπες).

Ορίζουμε τον πίνακα $R = \begin{bmatrix} a & b & m \\ b & c & n \\ m & n & s \end{bmatrix}$, ο οποίος έχει ορίζουσα

$$detR = m(bn - mc) - n(an - bm) + s(ac - b^2) = mM + nN + su = 1.$$

Επίσης έχουμε

$$su = 1 - mM - nN = 1 - bmn + cm^2 + an^2 - bmn =$$

$$1 - 2bmn + an^2 + (\frac{u + b^2}{a})m^2 = \frac{m^2u}{a} + \frac{(an - bm)^2}{a} + 1.$$

Αυτό σημαίνει πως ο συντελεστής του z^2 στην παράσταση

$$F(x, y, z) = \frac{(ax + by + mz)^2}{a} + \frac{(uy + (an - bm)z)^2}{au} + \frac{z^2}{u}$$

είναι ίσος με s.

Όμως

$$[x\ y\ z]R[x\ y\ z]^T = F(x, y, z).$$

Ο $[x\ y\ z]$ είναι ένας 1×3 πίνακας.

Εφόσον $a = 2a' > 0$ (το a' είναι θετικό σαν δεύτερος συντελεστής της μορφής Gauss $[a', b, c']$) και $u > 0$ ($u = -D > 0$), έπεται ότι το $F(x, y, z)$ δεν μπορεί να γίνει αρνητικό για οποιαδήποτε τιμή των ακεραίων x, y και z.

Από το θεώρημα 3.3.7 ο πίνακας R είναι ισοδύναμος με έναν από τους πίνακες

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ ή } \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Ας ονομάσουμε το δεύτερο πίνακα Q. Αν ο R ήταν ισοδύναμος με τον Q, τότε θα υπήρχε πίνακας $G \in GL_3(\mathbb{Z})$ με $GQG^T = R$. Έστω

$$[x\ y\ z] = [0\ 1\ 0]G^{-1},$$

τότε

$$[x\ y\ z]R[x\ y\ z]^T = [0\ 1\ 0]G^{-1}GQG^T(G^{-1})^T[0\ 1\ 0]^T =$$

$$[0\ 1\ 0]Q[0\ 1\ 0]^T = [0\ 1\ 0]\begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}[0\ 1\ 0]^T = -1.$$

Αφού όμως η παράσταση $F(x, y, z)$ παίρνει μόνο μη αρνητικές τιμές, αυτό είναι αδύνατο. Άρα ο πίνακας R είναι ισοδύναμος με τον ταυτοτικό.

Πρέπει λοιπόν να υπάρχει ένας πίνακας $H \in GL_3(\mathbb{Z})$ τ.ω. ο HRH^T να είναι ο ταυτοτικός, άρα $R = H^{-1}(H^T)^{-1}$. Η σχέση $R\overline{R}^T = (detR)I$ μας δίνει $R\overline{R}^T = I$. Αντικαθιστώντας τώρα από την ισότητα $R = H^{-1}(H^T)^{-1}$, παίρνουμε $H^{-1}(H^T)^{-1}\overline{R}^T = I$, δηλαδή $\overline{R}^T = H^TH$.

Ο κάτω δεξιά όρος του πίνακα $\overline{R}^T$ είναι $ac - b^2 = u = 8Z + 3$, ενώ του H^TH είναι ένα άθροισμα τριών τετραγώνων $x_1^2 + x_2^2 + x_3^2$, με x_1, x_2 και x_3 ακεραίους (αρκεί να δούμε τον H στην μορφή $\begin{bmatrix} * & * & x_1 \\ * & * & x_2 \\ * & * & x_3 \end{bmatrix}$). Εξισώνοντας έχουμε

$$8Z + 3 = x_1^2 + x_2^2 + x_3^2.$$

Αν δούμε τη σχέση $\pmod 8$, είναι $x_1^2 + x_2^2 + x_3^2 \equiv 3 \pmod 8$. Για να ισχύει η ισοτιμία θα πρέπει και οι τρείς αριθμοί να είναι περιττοί και η παραπάνω ισότητα μας δίνει

$$8Z + 3 = (2y_1 + 1)^2 + (2y_2 + 1)^2 + (2y_3 + 1)^2,$$

άρα

$$Z = \frac{y_1(y_1 + 1)}{2} + \frac{y_2(y_2 + 1)}{2} + \frac{y_3(y_3 + 1)}{2}.$$

Γράψαμε δηλαδή τον τυχαίο ακέραιο Z σαν άθροισμα τριών τρίγωνων αριθμών.

□

Παράδειγμα

Θα γράψουμε το 13 σαν άθροισμα τριών τρίγωνων αριθμών, ακολουθώντας την προηγούμενη διαδικασία. Θεωρούμε $u = 8 \cdot 13 + 3 = 107$ και $D = -107$.

Για τις τιμές $a = 2$, $b = 1$, $c = 54$, μπορούμε να επιλέξουμε $N = 31$. Τότε $M = 38$, $C = 9$, $B = 11$, $A = 14$, $m = -1$, $n = -16$ και $s = 5$. Τότε ο πίνακας R είναι ο

$$\begin{bmatrix} 2 & 1 & -1 \\ 1 & 54 & -16 \\ -1 & -16 & 5 \end{bmatrix}$$

και για τον πίνακα $H = \begin{bmatrix} -2 & -2 & -7 \\ -3 & -2 & -7 \\ 1 & 1 & 3 \end{bmatrix} \in GL_3(\mathbb{Z})$ ισχύει $HRH^T = I$.

Ο κάτω δεξιά όρος του πίνακα $H^T H$ είναι

$$(-7)^2 + (-7)^2 + 3^2 = 107,$$

άρα

$$8 \cdot 13 + 3 = (2 \cdot 3 + 1)^2 + (2 \cdot 3 + 1)^2 + (2 \cdot 1 + 1)^2$$

δηλαδή

$$13 = \frac{3 \cdot 4}{2} + \frac{3 \cdot 4}{2} + \frac{1 \cdot 2}{2}.$$

□

3.7 Το θεώρημα των πολύγωνων αριθμών

Ας θυμηθούμε από την εισαγωγή, ότι πολύγωνος είναι ένας μη αρνητικός ακέραιος αριθμός, της μορφής $m\frac{(t^2-t)}{2}+t$. Για $m=1$ έχουμε τους τρίγωνους αριθμούς, για $m=2$ έχουμε τους τετράγωνους κ.ο.κ. Δηλαδή ο $m\frac{(t^2-t)}{2}+t$ είναι $m+2$-γωνος αριθμός. Η εικασία του Fermat λέει πως, για κάθε ακέραιο m, κάθε ακέραιος γράφεται σαν άθροισμα $m+2$ τέτοιων όρων. Θα ξεκινήσουμε την απόδειξη με ένα θεώρημα από την απόδειξη του Gauss για την περίπτωση των τρίγωνων αριθμών.

Θεώρημα 3.7.1:

Έστω k και s περιττοί θετικοί ακέραιοι τέτοιοι ώστε

$$\sqrt{3k-2}-1 \leq s \leq \sqrt{4k},$$

τότε υπάρχουν μη αρνητικοί ακέραιοι t, u, v και w, τέτοιοι ώστε:

$$k = t^2+u^2+v^2+w^2$$

$$s = t+u+v+w$$

Απόδειξη:

Έχουμε από το προηγούμενο κεφάλαιο πως κάθε θετικός ακέραιος είναι ίσος με ένα άθροισμα τριών τριγώνων αριθμών, τότε θα δείξουμε ότι κάθε ακέραιος της μορφής $8n+3$ είναι άθροισμα τριών τετραγώνων περιττών θετικών ακεραίων.

Έστω n θετικός ακέραιος, τότε θα υπάρχουν τρείς τρίγωνοι αριθμοί τ.ω.

$$n = \frac{t_1^2-t_1}{2}+t_1+\frac{t_2^2-t_2}{2}+t_2+\frac{t_2^2-t_2}{2}+t_2$$

$$8n+3 = 8\frac{t_1^2-t_1}{2}+8t_1+1+8\frac{t_2^2-t_2}{2}+8t_2+1+8\frac{t_2^2-t_2}{2}+8t_2+1$$

$$8n+3 = 4t_1^2-4t_1+8t_1+1+4t_2^2-4t_2+8t_2+1+4t_3^2-4t_3+8t_3+1$$

$$8n+3=(2t_1+1)^2+(2t_2+1)^2+(2t_3+1)^2$$

Οι $2t_i+1$ μπορούν να επιλεγούν ώστε να είναι θετικοί, ενώ αν δούμε την τελευταία ισότητα $\pmod 8$ έπεται ότι θα πρέπει να είναι και περιττοί.

Ο $4k-s^2$ είναι θετικός ακέραιος ($s\leq\sqrt{4k}$) και θα δείξουμε ότι είναι της μορφής $8n+3$. Αφού οι k,s είναι περιττοί θα γράφονται σαν $k=2k_1+1$ και $s=2s_1+1$, για κάποια $k_1,s_1\in\mathbb{Z}$ και τότε έχουμε

$$4k-s^2=8k_1+4-4s_1^2-4s_1-1=8k_1-4s_1(s_1+1)+1=8k_1-8l+3=8(k_1-l)+3$$

(ο $s_1(s_1+1)$ είναι άρτιος σαν γινόμενο δύο συνεχόμενων ακεραίων, θα υπάρχει λοιπόν $l\in\mathbb{Z}$ τέτοιο ώστε $s_1(s_1+1)=2l$).

Άρα θα υπάρχουν θετικοί περιττοί ακέραιοι x,y και z για τα οποία να ισχύει ότι

$$4k-s^2=x^2+y^2+z^2.$$

Είναι

$$(x+y+z)^2\leq(x+y+z)^2+(x-y)^2+(x-z)^2+(y-z)^2=3(4k-s^2)\ \ (I)$$

Θα δείξουμε τώρα ότι ισχύει και ότι $3(4k-s^2)<(s+4)^2\ \ (II)$

Έχουμε ότι $\sqrt{3k-2}-1\leq s\Rightarrow\sqrt{3k-2}\leq s+1\Rightarrow 3k-2\leq s^2+2s+1\Rightarrow 12k-8\leq 4s^2+8s+4\Rightarrow 12k-3s^2\leq s^2+8s+12\Rightarrow 12k-3s^2<s^2+8s+16\Rightarrow 12k-3s^2<(s+4)^2\Rightarrow 3(4k-s^2)<(s+4)^2$.

Από (I) και (II), έπεται ότι $(x+y+z)^2\leq 3(4k-s^2)<(s+4)^2$, δηλαδή

$$x+y+z<s+4$$

και τότε $\frac{s-x-y-z}{4}>-1$, αφού όμως τα x,y και z είναι θετικοί ακέραιοι αν αλλάξουμε μερικά '-' με '+' το κλάσμα μεγαλώνει και άρα

$$\frac{s\pm x\pm y\pm z}{4}>-1,$$

για οποιοδήποτε συνδιασμό των '-' και '+'.

Θέτουμε $c=s-x-y-z$ και $d=s+x+y+z$. Αφού οι s,x,y και z είναι όλοι περιττοί, οι c και d είναι άρτιοι. Επιπλέον $c+d=2s$, με s περιττό, άρα ένας από τους c και d διαιρείται από το 4.

($c+d=2s$, αν $c=2c_1$ και $d=2d_1$, τότε $c_1+d_1=s\equiv 1 \pmod 2$, θα πρέπει δηλαδή ένας εκ των c και d να είναι $\equiv 1 \pmod 2$ και ο άλλος $\equiv 0 \pmod 2$).

Περίπτωση 1. $4|c$**.**

Έστω

$$t=\frac{c}{4}$$

$$u=t+\frac{y+z}{2}$$

$$v=t+\frac{x+z}{2}$$

$$w=t+\frac{x+y}{2}$$

τα t,u,v και w είναι μη αρνητικοί ακέραιοι ($\frac{s\pm x\pm y\pm z}{4}>-1$), με άθροισμα s, ενώ το άθροισμα των τετραγώνων τους είναι ίσο με $\frac{s^2+x^2+y^2+z^2}{4}=k$.

Περίπτωση 2. $4|d$**.**

Έστω

$$t=\frac{d}{4}$$

$$u=t-\frac{y+z}{2}$$

$$v=t-\frac{x+z}{2}$$

$$w=t-\frac{x+y}{2}$$

τα t,u,v και w είναι μη αρνητικοί ακέραιοι ($\frac{s\pm x\pm y\pm z}{4}>-1$), με άθροισμα s, ενώ το άθροισμα των τετραγώνων τους είναι ίσο με k.

□

Πριν δούμε το θεώρημα των πολυγώνων αριθμών, θα χρειαστούμε το παρακάτω θεώρημα κλειδί.

Θεώρημα 3.7.2:

Έστω k και s περιττοί θετικοί ακέραιοι τέτοιοι ώστε

$$\sqrt{3k-2}-1 \leq s \leq \sqrt{4k}$$

Έστω m ακέραιος, μεγαλύτερος του 2 και r μη αρνητικός ακέραιος με $r \leq m-2$, τότε ο $\frac{m(k-s)}{2}+s+r$ είναι άθροισμα $m+2$ $(m+2)$-γώνων αριθμών (επιτρέπονται τα μηδενικά).

Απόδειξη:

Από το θεώρημα 3.7.1 υπάρχουν μη αρνητικοί ακέραιοι t,u,v,w τέτοιοι ώστε

$$k = t^2+u^2+v^2+w^2$$

$$s = t+u+v+w$$

τότε $\frac{m(k-s)}{2}+s+r = \frac{m(t^2-t)}{2}+t+\frac{m(u^2-u)}{2}+u+\frac{m(v^2-v)}{2}+v+\frac{m(w^2-w)}{2}+w+1+...+1,$

με r το πλήθος άσσους. Αφού το $r \leq m-2$ το άθροισμα του δεξιού μέλους της ισότητας αποτελείται από λιγότερους από $m+2$ $m+2$-γωνους αριθμούς. Αν επιτρέψουμε και τα μηδενικά ο $\frac{m(k-s)}{2}+s+r$ είναι άθροισμα $m+2$ $(m+2)$-γώνων αριθμών.

□

Από εδώ και πέρα θα θεωρούμε ότι ο k είναι περιττός θετικός ακέραιος. Για δοθέν k υπάρχει πάντα περιττός ακέραιος s με $\sqrt{3k-2}-1 \leq s \leq \sqrt{4k}$ (παράρτημα). Έστω $s_1(k)$ ο μικρότερος περιττός θετικός ακέραιος σε αυτό το διάστημα και $s_2(k)$ ο μεγαλύτερος (μπορεί φυσικά τα $s_1(k)$ και $s_2(k)$ να είναι ίσα για κάποιο k).

Για $m>2$ ορίζουμε

$$g(k) = \frac{m(k-s_2(k))}{2}+s_2(k) = \frac{mk}{2}-(\frac{m}{2}-1)s_2(k)$$

$$h(k) = \frac{m(k-s_1(k))}{2}+s_1(k)+m-2 = \frac{mk}{2}-(\frac{m}{2}-1)s_1(k)+m-2$$

Θεώρημα 3.7.3:

Έστω ακέραιος m μεγαλύτερος του 2 και N ακέραιος μεγαλύτερος ή ίσος του $44m + 19$, τότε ο N είναι άθροισμα $m + 2$ $(m + 2)$-γωνων αριθμών.

Απόδειξη:

Καθώς ο s διατρέχει τους περιττούς αριθμούς

$$s_2(k), s_2(k) - 2, ..., s_1(k)$$

(είναι όλοι οι περιττοί αριθμοί μεταξύ των $\sqrt{3k-2} - 1$ και $\sqrt{4k}$)

και για κάθε s, ο r παίρνει τιμές από το 0 στο $m - 2$, η μορφή

$$\frac{m(k-s)}{2} + s + r$$

παίρνει όλες τις ακέραιες τιμές μεταξύ των $g(k)$ και $h(k)$, συμπεριλαμβανομένων των άκρων $g(k)$ και $h(k)$. Παίρνει δηλαδή τις τιμές

$$\frac{mk}{2} - (\frac{m}{2} - 1)s_2(k) \ \ ... \ \ \frac{mk}{2} - (\frac{m}{2} - 1)s_2(k) + m - 2$$

$(s = s_2(k)$ και $r = 0, ..., m - 2)$

$$\frac{mk}{2} - (\frac{m}{2} - 1)(s_2(k) - 2) \ \ ... \ \ \frac{mk}{2} - (\frac{m}{2} - 1)(s_2(k) - 2) + m - 2$$

$(s = s_2(k) - 2$ και $r = 0, ..., m - 2)$

.

.

.

$$\frac{mk}{2} - (\frac{m}{2} - 1)s_1(k) \ \ ... \ \ \frac{mk}{2} - (\frac{m}{2} - 1)s_1(k) + m - 2$$

$(s = s_1(k)$ και $r = 0, ..., m - 2)$

με τον τελευταίο αριθμό σε κάθε σειρά ίσο με τον πρώτο αριθμό της επόμενης.

Έστω $k \geq 0$, τότε

$$\sqrt{4(k+2)} - 2 > \sqrt{3k-2} - 1 + 2 \ \ (I).$$

Από τον ορισμό του $s_2(k)$ έχουμε $\sqrt{3(k+2)} - 1 \leq s_2(k+2) \leq \sqrt{4(k+2)}$, επειδή όμως ο s_2 είναι ο μεγαλύτερος περιττός σε αυτό το διάστημα, θα ισχύει

$$\sqrt{4(k+2)} - 2 \leq s_2(k+2) \leq \sqrt{4(k+2)} \ \ (II).$$

Επίσης από τον ορισμό του $s_1(k)$ έχουμε $\sqrt{3k-2} - 1 \leq s_1(k) \leq \sqrt{4k}$, επειδή όμως ο s_1 είναι ο μικρότερος περιττός σε αυτό το διάστημα, θα ισχύει

$$\sqrt{3k-2} - 1 \leq s_1(k) \leq \sqrt{3k-2)} - 1 + 2 \ \ (III).$$

Από $(I), (II)$ και (III) έχουμε ότι $s_2(k+2) > s_1(k)$, τότε έπεται ότι $h(k) > g(k+2) - 2$ ή $h(k) \geq g(k+2) - 1$ (η ισχύ της ανισότητας φαίνεται εύκολα με απλή αντικατάσταση των τύπων του $h(k)$ και $g(k+2)$).

Θεωρούμε τα διαστήματα

$$[g(107), h(107)], [g(109), h(109)], [g(111), h(111)], ...$$

Η ακολουθία

$$g(107), g(109), g(111), ...$$

τείνει στο άπειρο. Αφού $h(k) > g(k+2)-1$, η ένωση των παραπάνω διαστημάτων περιέχει όλους τους ακέραιους $\geq g(107) = \frac{m107}{2} - (\frac{m}{2} - 1)s_2(107) = \frac{107m}{2} - (\frac{m}{2} - 1)19 = 44m + 19$.

Άρα κάθε $N \geq 44m + 19$ θα είναι κάποιος αριθμός σε διάστημα $[g(k), h(k)]$, δηλαδή κάποιος αριθμός της μορφής $\frac{m(k-s)}{2} + s + r$, από το θεώρημα 3.7.2 έχουμε το αποτέλεσμα.

□

Επίσης $g(105) = 43m + 19$ και $h(105) = 45m + 15$, άρα $h(105) \geq g(107) - 1$ και μπορούμε να αυξήσουμε την ισχύ του θεωρήματος από τον $44m + 19$ στον $43m + 19$. Συνεχίζοντας με όμοιο τρόπο μπορούμε να αυξήσουμε την ισχύ του θεωρήματος μέχρι το $g(89) = 36m+17$. Όμως $h(87) = 36m+15$ και η ανισότητα $h(87) \geq g(89)-1$ δεν ισχύει, με αποτέλεσμα ο ακέραιος $36m + 16$ να μην ανήκει στην ένωση των

διαστημάτων $[g, h]$. Αυτό όμως δεν αποτελεί πρόβλημα αφού ο $36m + 16$ γράφεται εύκολα σαν άθροισμα τεσσάρων $(m + 2)$-γωνων αριθμών:

$36m+16 = (28m+8)+(6m+4)+(m+2)+(m+2) = (\frac{m(8^2-8)}{2}+8)+(\frac{m(4^2-4)}{2}+4)+(\frac{m(2^2-2)}{2}+2)+(\frac{m(2^2-2)}{2}+2)$

Για τα διαστήματα

$$[g(71), h(71)], ..., [g(87), h(87)]$$

ισχύει η ανισότητα $h(k) > g(k + 2) - 1$, άρα περιέχουν όλους τους ακέραιους από τον $28m + 15$ ως και τον $36m + 15$ και το θεώρημα επεκτείνεται ως τον $28m + 15$.

Ο επόμενος ακέραιος που δεν ανήκει στην ένωση είναι ο $28m + 14$, ο οποίος όμως γράφεται $28m + 14 = (21m + 17) + (6m + 4) + (m + 2) + 1$ και το θεώρημα ισχύει και για τον $28m + 14$.

Συνεχίζοντας με αυτόν τον τρόπο βλέπουμε ότι το θεώρημα ισχύει για όλους τους θετικούς ακεραίους. Οι μόνοι ακέραιοι που δεν ανήκουν στην ένωση των διαστημάτων $[g, h]$ είναι οι ακόλουθοι (οι οποίοι όμως γράφονται εύκολα σαν άθροισμα $m + 2$ $(m + 2)$-γωνων αριθμών).

$m + 2$	$8m + 8$	$19m + 12$
$2m + 4$	$9m + 8$	$20m + 12$
$3m + 4$	$10m + 8$	$21m + 12$
$4m + 6$	$13m + 10$	$27m + 14$
$5m + 6$	$14m + 10$	$28m + 14$
$6m + 6$	$15m + 10$	$36m + 16$

Οι $m + 2$-γωνοι αριθμοί που θα χρειαστούμε είναι οι $1, m + 2, 3m + 3, 6m + 4, 10m + 5, 15m + 6, 21m + 7, 28m + 8$ (είναι οι αριθμοί της μορφής $\frac{m(t^2-t)}{2} + t$, για $t = 1, 2, 3, 4, 5, 6, 7, , 8$). Τότε $m+2$, $2m+4 = (m+2)+(m+2)$, $3m+4 = (3m+3)+1$, $4m+6 = (3m+3)+(m+2)+1$, $5m+6 = (m+2)+(m+2)+(m+2)+(m+2)+1+...+1$, με $m - 2$ το πλήθος άσσους κ.ο.κ.

Κεφάλαιο 4

Παράρτημα

4.1 p-ομάδες

Ορισμός:

Έστω G ομάδα, τα στοιχεία $a, b \in G$ θα λέγονται συζυγή αν υπάρχει $g \in G$ τέτοιο ώστε $a = g^{-1}bg$.

Η συζυγία είναι σχέση ισοδυναμίας.

Οι κλάσεις ισοδυναμίας είναι οι συζυγείς κλάσεις της G.

Εαν οι συζυγείς κλάσεις της G είναι οι $C_1, ..., C_r$, τότε μία από αυτές, έστω η C_1 περιέχει μόνο το μοναδιαίο στοιχείο της G, (αν a συζυγές με το 1 (το μοναδιαίο στοιχείο της G), τότε για κάποιο $g \in G$ είναι $a = g^{-1} \cdot 1 \cdot g = g^{-1} \cdot g = 1$). Έτσι $|C_1| = 1$.

Αφού οι συζυγείς κλάσεις αποτελούν διαμέριση της G θα έχουμε ότι:

$|G| = 1 + |C_2| + ... + |C_r|$, (ισότητα κλάσεων της G).

Ορισμός:

Έστω G ομάδα και $x \in G$, τότε ορίζουμε το σύνολο: $C_G(x) = \{g \in G | xg = gx\}$

Η $C_G(x)$ είναι υποομάδα της G και ονομάζεται κανονικοποιούσα ομάδα του x στη G.

Υπάρχει μία χρήσιμη σχέση ανάμεσα στη $C_G(x)$ και στις συζυγής κλάσεις.

Λήμμα 4.1.1:

Έστω G ομάδα και $x \in G$, τότε ο αριθμός των στοιχείων στην κλάση συζυγίας του x ισούται με το δείκτη της $C_G(x)$ στη G.

Απόδειξη:

Έστω a, b δυο στοιχεία στην κλάση συζυγίας του x, τότε $a = g^{-1}xg$ και $b = j^{-1}xj$, για κάποια $g, j \in G$. Όμως τα a, b είναι συζυγής, άρα $a = c^{-1}bc$, για κάποιο $c \in G$, τότε

$$g^{-1}xg = c^{-1}j^{-1}xjc \Leftrightarrow g^{-1}xg = (jc)^{-1}x(jc) \Leftrightarrow g^{-1}xg = h^{-1}xh, \text{ με } (h = jc).$$

Η εξίσωση αυτή ισχύει αν και μόνο αν $hg^{-1}x = xhg^{-1}$, δηλαδή να και μόνο αν $hg^{-1} \in C_G(x)$. Δηλαδή τα h, g ανήκουν στο ίδιο σύμπλοκο της $C_G(x)$ στη G. Ο αριθμός αυτών των συμπλόκων είναι ο δείκτης της $C_G(x)$ στη G και το λήμμα αποδείχθηκε.

□

Λήμμα 4.1.2:

Ο αριθμός των στοιχείων σε οποιαδήποτε συζυγή κλάση μιας πεπερασμένης ομάδας G διαιρεί την τάξη της G.

Απόδειξη:

Έστω G πεπερασμένη ομάδα και $x \in G$. Έστω C η κλάση συζυγίας του x στη G. Από το λήμμα 4.1.1 έχουμε ότι $|C| = (G : C_G(x))$ και αφού η G είναι πεπερασμένη $(G : C_G(x)) = \frac{|G|}{|C_G(x)|}$, άρα $|C_G(x)| = \frac{|G|}{|C|}$.

□

Ορισμός:

Έστω πρώτος p, τότε μια πεπερασμένη ομάδα G θα λέγεται p-ομάδα αν η τάξη της είναι δύναμη του p.

Ορισμός:

Το κέντρο $Z(G)$ μιας ομάδας θα είναι το σύνολο:

$$Z(G) = \{x \in G | xg = gx \ \ \forall g \in G\}.$$

Η $Z(G)$ είναι κανονική υποομάδα της G. Αρχικά θα δείξουμε ότι είναι υποομάδα. Έστω $a, b \in Z(G)$ αρκεί να δείξουμε ότι $ab^{-1} \in Z(G)$. Είναι $gab^{-1} = agb^{-1}$, (αφού $a \in Z(G)$) (1) και $b \in Z(G)$ άρα για κάθε $g \in G$ ισχύει $bg = gb \Leftrightarrow gb^{-1} = b^{-1}g \Leftrightarrow b^{-1}g = gb^{-1} \Leftrightarrow b^{-1} \in Z(G)$ (2).

Από (1) και (2) : $gab^{-1} = agb^{-1} = ab^{-1}g$, τότε $ab^{-1} \in Z(G)$.

Τώρα θα δείξουμε ότι $Z(G) \trianglelefteq G$. Έστω $a \in Z(G)$ και $g \in G$, αρκεί $gag^{-1} \in Z(G)$. Όμως $gag^{-1} = agg^{-1} = a \in Z(G)$.

□

Θεώρημα 4.1.3:

Εαν $G \neq 1$ είναι πεπερασμένη p-ομάδα, τότε έχει μη τετριμμένο κέντρο.

Απόδειξη :

Από την ισότητα κλάσεων έχουμε $|G| = 1 + |C_2| + ... + |C_n|$, και αφού η G είναι p-ομάδα είναι $|G| = p^n$, άρα $1 + |C_2| + ... + |C_n| = p^n$. Από λήμμα 4.1.2 έχουμε ότι $|C_i = p^{n_i}|$, για κάποιο $n_i \geq 0$. Το $p|p^n$, άρα $p|1 + |C_2| + ... + |C_n|$. Τότε το λιγότερο $p - 1$ το πλήθος $|C_i|$ πρέπει να είναι ίσα με 1.

Αλλά αν x ανήκει σε μία από αυτές τις κλάσεις συζυγίας με ένα μόνο στοιχείο (είδαμε ότι υπάρχουν $p - 1$ τέτοιες κλάσεις, άρα το x είναι διαφορετικό του μοναδιαίου), θα πρέπει $x = g^{-1}xg$, για κάθε $g \in G$, διαφορετικά αν για κάποιο $g \in G$ είχαμε $g^{-1}xg = y \neq x$ η κλάση θα είχε τουλάχιστον δύο στοιχεία,τα x, y αντίφαση.

Δηλαδή $gx = xg$, για κάθε $g \in G$, άρα $x \in Z(G)$, άρα $Z(G) \neq 1$.

□

Λήμμα 4.1.4:

Αν A πεπερασμένη αβελιανή ομάδα, της οποίας η τάξη διαιρείται από έναν πρώτο p, τότε η A έχει ένα στοιχείο τάξης p.

Απόδειξη :

Θα κάνουμε επαγωγή ως προς το $|A|$.

Εαν $|A|$ πρώτος, τότε η ομάδα είναι κυκλική και ο γεννήτορας έχει τάξη p.

Αν $|A|$ οχι πρώτος, έστω μια γνήσια υποομάδα M της A, της οποίας η τάξη να είναι μέγιστη, έστω m. Εαν το p διαιρεί το m, τότε από επαγωγική υπόθεση έχουμε το αποτέλεσμα.

Υποθέτουμε ότι $p \not| m$. Έστω $t \in A$ αλλά $t \notin M$ και T η κυκλική ομάδα που παράγεται από το t. Τότε η MT είναι υποομάδα της A μεγαλύτερη από τη M και από το μέγιστο της M έχουμε: $MT = A$.

(Ισχυρισμός: MT υποομάδα της A

Απόδειξη: MT υποσύνολο της A, αφού A αβελιανή είναι M υποομάδα της A και T υποομάδα της A. Έστω $x, y \in MT$, τότε $x = ac$ και $y = bd$, με $a, b \in M,\ c, d \in T$. Τότε $xy^{-1} = ac(bd)^{-1} = acd^{-1}b^{-1} = ab^{-1}cd^{-1} \in MT$, αφού $ab^{-1} \in M$ και $cd^{-1} \in T$.)

Από το πρώτο θεώρημα ισομορφισμών

(Έστω G, H, A ομάδες, εαν $H \trianglelefteq G$ και A υποομάδα της G, τότε: $H \cap A \trianglelefteq A$ και $A/H \cap A \simeq HA/H$)

και αφού η A αβελιανή, άρα κάθε υποομάδα της είναι κανονική, θα έχουμε

$$|MT| = |M||T|/|M \cap T|.$$

Έχουμε ότι $p \mid\ |MT| \Rightarrow p|\ |MT| \cdot |M \cap T| \Rightarrow p|\ |M| \cdot |T|$. Όμως $|M| = m$ και $p \not| m$, άρα $p||T| = r$.

Αφού η T είναι κυκλική, το στοιχείο $t^{\frac{r}{p}}$ έχει τάξη p.

□

Λήμμα 4.1.5:

Έστω G πεπερασμένη p-ομάδα, τάξης p^n, τότε η G έχει μια σειρά από κανονικές υποομάδες:

$$1 = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G,$$

όπου $|G_i| = p^i$, για κάθε $i = 0, ..., n$.

Απόδειξη:

Θα κάνουμε επαγωγή ως προς n.

Αν $n = 0$ τότε είμαστε εντάξει.

Αν $n > 0$, τότε $Z(G) \neq 1$, από το θεώρημα 4.1.3.

Αφού η $Z(G)$ είναι αβελιανή (εξ' ορισμού) με τάξη p^m (η τάξη της $Z(G)$, σαν υποομάδα της G, διαιρεί την $|G| = p^n$), έχει στοιχείο τάξης p (από το λήμμα 4.1.4).

Η κυκλική υποομάδα K που παράγεται από αυτό το στοιχείο, έχει τάξη p και είναι κανονική, αφού K υποομάδα της $Z(G)$.

(Έστω $u \in K$ για κάθε $g \in G$: $gug^{-1} = {}^{1}ugg^{-1} = u \in K$, άρα $K \trianglelefteq G$)

Τότε η G/K είναι μια p ομάδα με τάξη p^{n-1}.

(Αφού $K \trianglelefteq G \Rightarrow G/K$ ομάδα και $|G/K| = |G|/|K| = \frac{p^n}{p} = p^{n-1}$).

Άρα από την επαγωγική υπόθεση αυτή θα έχει σειρά κανονικών υποομάδων:

$$K/K = G_1/K \subseteq ... \subseteq G_n/K,$$

όπου $|G_i/K| = p^{i-1}$.

Αλλά τότε $|G_i| = p^i$ και $G_i \triangleleft G$, θέτουμε $G_0 = 1$ και έχουμε το αποτέλεσμα.

□

[1] $u \in K \subseteq Z(G) \Rightarrow gu = ug$

4.2 Θεωρία Galois

Σε αυτή την παράγραφο θα προσπαθήσουμε να δώσουμε μία εικόνα για τις επεκτάσεις σωμάτων και τη θεωρία Galois, για τη θεμελίωση των παρακάτω δείτε τη σχετική βιβλιογραφία ([3], [15], [19]).

Έστω K, L σώματα, αν το K είναι υπόσωμα του L, θα λέμε ότι το L είναι μία επέκταση του K και θα το συμβολίζουμε με L/K.

Το L είναι K-διανυσματικός χώρος.

Ορισμός:

Η διάσταση του L σαν K-δ.χ. θα λέγεται βαθμός της επέκτασης L/K και θα συμβολίζεται $[L : K]$. Αν $[L : K] < \infty$, η επέκταση θα λέγεται πεπερασμένη.

Πρόταση:

Αν L/K και K/M επεκτάσεις σωμάτων, τότε:

$$[L : K][K : M] = [L : M]$$

Ορισμός:

Το $K(a_1, ..., a_n)$ είναι το σώμα που προκύπτει από το K με επισύναψη των στοιχείων $a_1, ..., a_n$.

Θεώρημα:

Έστω L/K επέκταση σωμάτων. Αν $a \in L$, αλγεβρικό ως προς το K (δηλαδή υπάρχει πολυώνυμο του $K[x]$ που να έχει το a σαν ρίζα), τότε υπάρχει μονικό ανάγωγο πολυώνυμο $p(x) \in K[x]$ τ.ω. $p(a) = 0$ και συμβολίζεται με $Irr(a, K)$. Το $p(x)$ λέγεται το ελάχιστο πολυώνυμο του a πάνω από το K.

Πόρισμα:

Αν L/K επέκταση σωμάτων και $a \in L$ αλγεβρικό ως προς το K, τότε $[K(a) : K] = degIrr(a, K)$.

Σε αυτό το κεφάλαιο θα μελετήσουμε κυρίως επεκτάσεις με ιδιαίτερα χαρακτηριστικά, αυτές είναι οι επεκτάσεις Galois. Μία επέκταση πάνω από το $\mathbb{Q}$ είναι Galois αν και μόνο αν είναι κανονική (γενικά πρέπει επίσης να είναι και διαχωρίσιμη, αλλά κάθε επέκταση πάνω από το $\mathbb{Q}$ είναι, οπότε δε θα ασχοληθούμε περαιτέρω με την έννοια).

Μία επέκταση L/K λέγεται κανονική αν για κάθε $a \in L$ το $Irr(a, K)$ έχει όλες

του τις ρίζες στο L.

π.χ. η $\mathbb{C}/\mathbb{R}$ είναι κανονική, ενώ η $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ όχι, αφού το $Irr(\sqrt[3]{2},\mathbb{Q})$ έχει ρίζες τις $\sqrt[3]{2}, \omega\sqrt[3]{2}$ και $\omega^2\sqrt[3]{2}$, όπου ω πρωταρχική 3-ρίζα του 1, αλλά $\omega\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$. Όμως η $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ είναι κανονική.

Σώμα ανάλυσης ενός πολυωνύμου $f(x) \in K[x]$ είναι το μικρότερο σώμα L που περιέχει το K και τις ρίζες του $f(x)$.

Ομάδα Galois μιας επέκτασης L/K είναι οι K-ισομορφισμοί του L (ισομορφισμοί του L που δρουν ταυτοτικά στα στοιχεία του K).

Αν $L = K(a_1, ..., a_n)$, με $\{a_1, ..., a_n\} \subseteq L$, οι K-αυτομορφισμοί του L καθορίζονται πλήρως από τη δράση τους στα στοιχεία $a_1, ..., a_n$.

Στην ειδική περίπτωση που τα $a_1, ..., a_n$ είναι οι ρίζες ενός πολυωνύμου $f(x) \in K[x]$, η ομάδα των K-αυτομορφισμών, δηλαδή η ομάδα Galois μπορεί να θεωρηθεί σαν την ομάδα μεταθέσεων των ριζών του $f(x) \in K[x]$.

Πόρισμα:

L/K επέκταση Galois $\Leftrightarrow \sharp Gal(L/K) = [L : K]$.

Η ιδέα της θεωρίας Galois είναι να αντιστοιχίσουμε τα ενδιάμεσα σώματα μιας επέκτασης Galois L/K με τις υποομάδες της $Gal(L/K)$.

Θεμελιώδες θεώρημα της θεωρίας Galois:

Έστω L/K πεπερασμένη επέκταση Galois και $G = Gal(L/K)$. Υπάρχει 1-1 και επί αντιστοιχία ανάμεσα στα $A = \{F|F$ σώμα $, K \subseteq F \subseteq L\}$ και $B = \{H|H$ ομάδα, $H \leq G\}$

$\phi : A \to B$ και $\psi : B \to A$

$F \mapsto Gal(L/F)$ $H \mapsto \mathfrak{F}(H)$

Επιπλέον, αν $F \to H = Gal(L/F)$, τότε $[L : F] = \sharp H$ και $[F : K] = [G : H]$.

Τέλος:

$H \trianglelefteq Gal(L/K) \Leftrightarrow F/K$ είναι επέκταση Galois. Τότε $Gal(F/K) \simeq G/H$

Σημείωση:

Έστω L/K επέκταση σωμάτων και S υποομάδα των ισομορφισμών από το L στο L (αυτομορφισμοί του L), τότε:

$$\mathfrak{F}(S) = \{a \in L : \ T(a) = a, \ \forall T \in S\}$$

Τότε $\mathfrak{F} \leq L$. Το $\mathfrak{F}$ λέγεται το σώμα σταθερών στοιχείων του S.

Παράδειγμα: Ας θεωρήσουμε την επέκταση σωμάτων $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$, είναι επέκταση Galois, αφού είναι επέκταση του $\mathbb{Q}$(άρα διαχωρίσιμη) και κανονική (το $\mathbb{Q}(\sqrt{2},\sqrt{3})$ είναι σώμα ανάλυσης των x^2-3, x^2-2). Άρα αφού $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$ θα είναι $\sharp Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})=4$ (η επέκταση είναι Galois).

Έχουμε πει ότι τα στοιχεία της ομάδας Galois είναι μεταθέσεις των ριζών των αναγώγων πάνω από το $\mathbb{Q}$ πολυωνύμων x^2-3 και x^2-2. Έστω λοιπόν $\sigma \in Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$, θα δούμε ποιές είναι οι δυνατές εικόνες των $\sqrt{2},\sqrt{3}$ (ρίζες των αναγώγων) μέσω της σ,

$$\sqrt{2}\to\pm\sqrt{2} \qquad \sqrt{3}\to\pm\sqrt{3}$$

Άρα οι δυνατές μεταθέσεις είναι:

$id:\sqrt{2}\to\sqrt{2}$ και $\sqrt{3}\to\sqrt{3}$

$s:\sqrt{2}\to-\sqrt{2}$ και $\sqrt{3}\to\sqrt{3}$

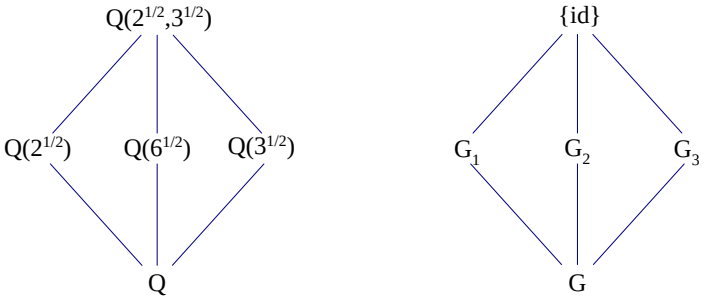
$t:\sqrt{2}\to\sqrt{2}$ και $\sqrt{3}\to-\sqrt{3}$

$x:\sqrt{2}\to-\sqrt{2}$ και $\sqrt{3}\to-\sqrt{3}$

Άρα $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})=\{id,s,t,x\}=\{id,s,t,s\circ t\}=G$

Έυκολα υπολογίζεται ότι $s^2=id,\ t^2=id,\ (s\circ t)^2=id$ και η G είναι πράγματι ομάδα τάξης 4 (είναι ισοδύναμη με την τετραδική ομάδα του Klein).

Έστω $G_1=<s>$, $G_2=<s\circ t>$ και $G_3=<t>$, οι υποομάδες της ομάδας Galois που παράγονται από τα s, $s\circ t$ και t αντίστοιχα, τότε το παρακάτω σχήμα δείχνει την αντιστοιχία των ενδιάμεσων σωμάτων της επέκτασης με τις υποομάδες της ομάδας Galois.



Η παραπάνω αντιστοιχία αποδεικνύεται εύκολα, υπολογίζοντας τα $\mathfrak{F}(< s >)$, $\mathfrak{F}(< t >)$ και $\mathfrak{F}(< st >)$.

Αν αριθμήσουμε τις ρίζες:

$\sqrt{2} \to 1,\ -\sqrt{2} \to 2,\ \sqrt{3} \to 3,\ -\sqrt{3} \to 4$

μπορούμε να δούμε τις μεταθέσεις σαν στοιχεία της S_n και θα έχουμε $s = (12),\ t = (34)$ και $s \circ t = (12)(34)$.

4.3 Συμπληρωματικά της παραγράφου 2.6

Πρέπει να αποδείξουμε την πρόταση που χρησιμοποιήσαμε στην παράγραφο 2.6, ότι κάθε γινόμενο m διαδοχικών ακεραίων διαιρείται από το $m!$.

Για δοθέντα ακέραιο m και πρώτο p, θα υπολογίσουμε τη μέγιστη δύναμη του p που διαιρεί το $m!$. Ορίζουμε με m' το ακέραιο μέρος του $\frac{m}{p}$, τότε από τους m παράγοντες του γινομένου $m! = 1 \cdot 2 \cdot 3 \cdot ... \cdot m$, μόνο οι ακόλουθοι m' είναι διαιρετοί από το p:

$$p,\ 2p,\ 3p,\ ...,\ m'p.$$

Αφού λοιπόν οι υπόλοιποι παράγοντες δεν διαιρούνται από το p, το ερώτημα μας είναι ισοδύναμο με το ποια είναι η μεγαλύτερη δύναμη του p που διαιρεί το γινόμενο:

$$1 \cdot 2 \cdot 3 \cdot ... \cdot m' \cdot p^{m'},$$

Η μεγαλύτερη δύναμη του p που διαιρεί το $1 \cdot 2 \cdot 3 \cdot ... \cdot m' \cdot p^{m'}$, είναι το άθροισμα του m' με τη μεγαλύτερη δύναμη του p που διαιρεί το γινόμενο $1 \cdot 2 \cdot 3 \cdot ... \cdot m'$.

Τώρα όμως έχουμε φτάσει σε ισοδύναμο με το αρχικό πρόβλημα, ακολουθώντας την ίδια διαδικασία καταλήγουμε στο ότι η μέγιστη δύναμη του p είναι ίση με το άθροισμα $m' + m'' + m''' + ...$, όπου τα $m'', m''', ...$ είναι τα ακέραια μέρη των $\frac{m'}{p}, \frac{m''}{p}, ...$. Η διαδικασία τελείωνει όταν κάποια στιγμή ο p γίνει μεγαλύτερος από κάποιο m.

Θα φανεί χρήσιμο για τη συνέχεια να κάνουμε την παρατήρηση ότι οι αριθμοί $m', m'', m''', ...$ είναι επίσης και ακέραια μέρη των $\frac{m}{p}, \frac{m}{p^2}, \frac{m}{p^3}, ...$ αντίστοιχα. Αφού αν r το ακέραιο μέρος του $\frac{m}{a}$ και s το ακέραιο μέρος του $\frac{r}{b}$, τότε το s είναι επίσης το ακέραιο μέρος του $\frac{m}{ab}$ ($r = \lfloor \frac{m}{a} \rfloor \Rightarrow \frac{m}{a} = r + u,\ 0 \leq u < 1$ και $s = \lfloor \frac{r}{b} \rfloor \Rightarrow \frac{r}{b} = s + v,\ 0 \leq v < 1$, τότε $\frac{m}{ab} = s + \frac{u}{b} + v$ με $0 \leq \frac{u}{b} + v < 1$, άρα $s = \lfloor \frac{m}{ab} \rfloor$).

Παράδειγμα:

Έστω $m = 60$ και $p = 7$, τότε:

$m' = \lfloor \frac{60}{7} \rfloor = \lfloor 8,5714... \rfloor = 8$

$m'' = \lfloor \frac{8}{7} \rfloor = \lfloor 1,1428... \rfloor = 1$ (που είναι επίσης το $\lfloor \frac{60}{7^2} \rfloor$)

$m' = \lfloor \frac{1}{7} \rfloor = \lfloor 0,1428... \rfloor = 0$ (που είναι επίσης το $\lfloor \frac{60}{7^3} \rfloor$)

Άρα η μέγιστη δύναμη του 7 που διαιρεί το 60!, είναι 8+1+0=9.

□

Στη συνέχεια θα αποδείξουμε ότι αν $m = f + g + h + ...$, τότε ο $\frac{m!}{f!g!h!...}$ είναι ακέραιος.

Έστω p ένας πρώτος διαιρέτης του παρανομαστή, τότε όπως είδαμε πριν $f' + f'' + f''' + ...$, $g' + g'' + g''' + ...$, $h' + h'' + h''' + ...$, ... είναι οι μέγιστες δυνάμεις του p που διαιρούν τα $f!$,$g!$,$h!$..., άρα η μέγιστη δύναμη του p που διαιρεί τον παρανομαστή, θα είναι:

$$(f' + f'' + f''' + ...) + (g' + g'' + g''' + ...) + (h' + h'' + h''' + ...) + ... \ (1).$$

Από την άλλη μεριά $m' + m'' + m''' + ...$ (2) είναι ο μέγιστος εκθέτης του p που διαιρεί τον αριθμητή. Αρκεί λοιπόν να δείξουμε ότι η μέγιστη δύναμη του p που διαιρεί τον παρανομαστή είναι μικρότερη ή ίση από αυτή που διαιρεί τον αριθμητή. Δηλαδή ότι το άθροισμα (1) είναι μικρότερο ή ίσο από το (2).

Από τη σχέση $m = f + g + h + ...$, έχουμε τις σχέσεις:

$\frac{m}{p} = \frac{f}{p} + \frac{g}{p} + \frac{h}{p} + ...$

$\frac{m}{p^2} = \frac{f}{p^2} + \frac{g}{p^2} + \frac{h}{p^2} + ...$

$\frac{m}{p^3} = \frac{f}{p^3} + \frac{g}{p^3} + \frac{h}{p^3} + ...$

κ.τ.λ.

Παίρνοντας τα ακέραια μέρη έχουμε ότι:

$m' \geq f' + g' + h' + ...$

$m'' \geq f'' + g'' + h'' + ...$

$m''' \geq f''' + g''' + h''' + ...$

κ.τ.λ.

Προσθέτοντας τις ανισότητες έχουμε το αποτέλεσμα.

Τώρα η πρόταση ότι κάθε γινόμενο m διαδοχικών ακεραίων διαιρείται από το $m!$ προκύπτει άμεσα.

Οι m διαδοχικοί ακέραιοι θα έχουν την μορφή $(a+1)\cdot(a+2)\cdot...(a+m-1)\cdot(a+m)$, τότε $\frac{(a+1)\cdot(a+2)\cdot...(a+m-1)\cdot(a+m)}{m!} = \frac{(m+a)!}{m!a!}$ που δείξαμε ότι είναι ακέραιος.

4.4 Συμπληρωματικά παραγράφων 3.3, 3.4 και 3.7

Στην απόδειξη του θεωρήματος 3.3.9 χρησιμοποιήσαμε τα εξής:

i) $detS = 1$.

Απόδειξη

$$detS = U^2(UJ^3+J^2VH-2HVJ^2)-UH(2UVJ^2-2HJV^2)+H^2(2UV^2J-UV^2J-V^3H) =$$

$$= U^2(UJ^3 - HVJ^2) - UH(2UVJ^2 - 2HJV^2) + H^2(UV^2J - V^3H) =$$

$$= U^3J^3 - U^2J^2HV - 2U^2J^2HV + 2V^2H^2UJ + H^2V^2UJ - V^3H^3 =$$

$$= U^3J^3 - 3U^2J^2HV + 3H^2V^2UJ - V^3H^3 = (UJ - VH)^3 = 1^3 = 1$$

□

ii) $SMS^T = M$.

Απόδειξη

$$SMS^T = \begin{bmatrix} U^2 & UH & H^2 \\ 2UV & UJ+VH & 2HJ \\ V^2 & VJ & J^2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} U^2 & 2UV & V^2 \\ UH & UJ+VH & VJ \\ H^2 & 2HJ & J^2 \end{bmatrix} =$$

$$= \begin{bmatrix} -\frac{H^2}{2} & UH & -\frac{U^2}{2} \\ -HJ & UJ+VH & -UV \\ -\frac{J^2}{2} & VJ & -\frac{V^2}{2} \end{bmatrix} \cdot \begin{bmatrix} U^2 & 2UV & V^2 \\ UH & UJ+VH & VJ \\ H^2 & 2HJ & J^2 \end{bmatrix}$$

Τότε το στοιχείο 11 είναι ίσο με $-\frac{U^2H^2}{2} + U^2H^2 - \frac{U^2H^2}{2} = 0$.

Το στοιχείο 12 είναι ίσο με $UVH^2 + U^2HJ + UVH^2 - U^2HJ = 0$.

Το στοιχείο 13 είναι ίσο με

$$-\frac{H^2V^2}{2}+UHVJ-\frac{U^2J^2}{2}=-\frac{H^2V^2-2UVHJ+U^2J^2}{2}=-\frac{(HV-UJ)^2}{2}=-\frac{1}{2}.$$

Το στοιχείο 21 είναι ίσο με $-HJU^2+U^2HJ+VUH^2-UVH^2=0$.

Το στοιχείο 22 είναι ίσο με $-2UVHJ+(UJ+VH)^2-2UVHJ=$
$-2UVHJ+U^2J^2+2UJVH+V^2H^2-2UVHJ=(UJ-VH)^2$
$=1^2=1$.

Το στοιχείο 23 είναι ίσο με $-HJV^2+UJ^2V+V^2HJ-UVJ^2=0$.

Το στοιχείο 31 είναι ίσο με

$$-\frac{U^2J^2}{2}+VJUH-\frac{H^2V^2}{2}=-\frac{(UJ-HV)^2}{2}=-\frac{1}{2}.$$

Το στοιχείο 32 είναι ίσο με $-\frac{2UVJ^2}{2}+VJ(UJ+VH)-\frac{2HJV^2}{2}=0$.

Το στοιχείο 33 είναι ίσο με $-\frac{J^2V^2}{2}+V^2J^2-\frac{J^2V^2}{2}=0$.

Άρα $SMS^T=\begin{bmatrix}0&0&-\frac{1}{2}\\0&1&0\\-\frac{1}{2}&0&0\end{bmatrix}=M$

□

iii) Η δεξιά στήλη του $\overline{S}$ είναι $\begin{bmatrix}V^2\\-UV\\U^2\end{bmatrix}$.

Απόδειξη

Το στοιχείο 13 του $\overline{S}$ είναι ίσο με
$2UV^2J-UV^2J-V^3H=UV^2J-V^3H=V^2(UJ-VH)=V^2\cdot 1=V^2$.

Το στοιχείο 23 του $\overline{S}$ είναι ίσο με
$-U^2VJ+V^2UH=-UV(UJ-VH)=-UV\cdot 1=-UV$.

Το στοιχείο 33 του $\overline{S}$ είναι ίσο με
$U^3J+U^2VH-2U^2VH=U^3J-U^2VH=U^2(UJ-VH)=U^2\cdot 1=U^2$.

Άρα πράγματι η δεξιά στήλη του $\overline{S}$ είναι η $\begin{bmatrix}V^2\\-UV\\U^2\end{bmatrix}$.

□

iv) $as_1^2 - bs_1r_1 + cr_1^2 = (r_1s_2 - r_2s_1)^2$.

Απόδειξη

$as_1^2-bs_1r_1+cr_1^2 = r_2^2s_1^2-r_1r_3s_1^2-(2r_2s_2-r_1s_3-r_3s_1)s_1r_1+r_1^2s_2^2-s_1s_3r_1^2 = r_2^2s_1^2-r_1r_3s_1^2-2r_1r_2s_1s_2+r_1^2s_3s_1+r_1r_3s_1^2-s_1s_3r_1^2 = r_2^2s_1^2-2r_1r_2s_1s_2+r_1^2s_2^2 = (r_1s_2-r_2s_1)^2$

□

Στην απόδειξη του θεωρήματος 3.4.2 χρησιμοποιήσαμε τη σχέση

$$(a_1x_1^2 + bx_1y_1 + c_1y_1^2)(a_2x_2^2 + bx_2y_2 + c_2y_2^2) = a_1a_2X^2 + bXY + cY^2$$

την οποία πρέπει και να αποδείξουμε.

Το αριστερά μέλος της ισότητας δίνει

$(a_1x_1^2 + bx_1y_1 + c_1y_1^2)(a_2x_2^2 + bx_2y_2 + c_2y_2^2) = a_1a_2x_1^2x_2^2 + a_1b_2x_1^2x_2y_2 + a_1x_1^2c_2y_2^2 + b_1a_2x_1y_1x_2^2 + b_1b_2x_1x_2y_1y_2 + b_1x_1y_1c_2y_2^2 + c_1a_2y_1^2x_2^2 + c_1y_1^2x_2^2 + c_1y_1^2b_2x_2y_2 + c_1c_2y_1^2y_2^2$

Το δεξί μέλος της ισότητας δίνει

$a_1a_2x_1^2x_2^2 + a_1a_2c^2y_1^2y_2^2 - 2a_1a_2x_1x_2cy_1y_2 + bx_1^2x_2a_1y_2 + bx_1x_2^2a_2y_1 + b^2x_1x_2y_1y_2 - a_1bcx_1y_2^2y_1 - a_2bcy_1^2y_2x_2 - b^2cy_1^2y_2^2 + ca_1^2x_1^2y_2^2 + 2a_1a_2cy_1y_2x_2x_1 + 2a_1bcx_1y_1y_2^2 + ca_2^2y_1^2x_2^2 + 2a_2cby_1^2y_2x_2 + cb^2y_1^2y_2^2$.

Για να δείξουμε ότι τα δύο μέλη είναι ίσα αρκεί να δείξουμε ότι οι αντίστοιχοι συντελεστές των $x_1^ix_2^jy_1^{i'}y_2^{j'}$ είναι ίσοι.

Ο συντελεστής του $x_1^2x_2^2$ και στα δύο μέλη είναι ο a_1a_2.

Για το $y_1^2y_2^2$, στο πρώτο μέλος έχει συντελεστή c_1c_2 και στο δεύτερο $-b^2c + b^2c + a_1a_2c^2 = a_1a_2cc = a_1a_2\frac{c_2}{a_1}\frac{c_1}{a_2} = c_1c_2$ ($c = \frac{c_2}{a_1} = \frac{c_1}{a_2}$).

Ο συντελεστής του $x_1y_1x_2^2$ και στα δύο μέλη είναι ο a_2b ($b = b_1 = b_2$).

Ο συντελεστής του $y_1^2x_2^2$ και στο πρώτο μέλος είναι ο c_1a_2 και στο δεύτερο $ca_2^2 = \frac{c_1}{a_2}a_2^2 = c_1a_2$.

Το $y_1^2y_2x_2$, στο πρώτο μέλος έχει συντελεστή $c_1b_2 = c_1b$ και στο δεύτερο $2a_2bc - a_2bc = a_2bc = a_2b\frac{c_1}{a_2} = bc_1$.

Ο συντελεστής του $x_1^2x_2y_2$ και στα δύο μέλη είναι ο ba_1.

Ο συντελεστής του $x_1x_2y_1y_2$ πρώτο μέλος είναι b^2 και στο δεύτερο $-2a_1a_2c + b^2 + 2a_1a_2c = b^2$.

Ο συντελεστής του $x_1^2 y_1^2$ πρώτο μέλος είναι $a_1 c_2$ και στο δεύτερο $ca_1^2 = \frac{c_2}{a_1} a_1^2 = c_2 a_1$.

Τέλος ο συντελεστής του $x_1 y_1 y_2^2$ πρώτο μέλος είναι $b_1 c_2 = bc_2$ και στο δεύτερο $2bca_1 - bca_1 = bca_1 = b\frac{c_2}{a_1} a_1 = bc_2$.

□

Στην παράγραφο 3.7 δεχτήκαμε ότι υπάρχει πάντα τουλάχιστον ένας περιττός ακέραιος s μεταξύ των $\sqrt{3k-2} - 1$ και $\sqrt{4k}$.

Απόδειξη:

Αρχικά θα το αποδείξουμε για $k = 1, 2, 3, 4, 5, 6, 7, 8, 9$.

$$k = 1 : \ 0 \leq s \leq 2 \Rightarrow s = 1$$

$$k = 2 : \ 1 \leq s \leq 2,8 \Rightarrow s = 1$$

$$k = 3 : \ 1,64 \leq s \leq 3,4 \Rightarrow s = 3$$

$$k = 4 : \ 2,16 \leq s \leq 4 \Rightarrow s = 3$$

$$k = 5 : \ 2,6 \leq s \leq 4,47 \Rightarrow s = 3$$

$$k = 6 : \ 3 \leq s \leq 4,8 \Rightarrow s = 3$$

$$k = 7 : \ 3,35 \leq s \leq 5,2 \Rightarrow s = 5$$

$$k = 8 : \ 3,69 \leq s \leq 5,65 \Rightarrow s = 5$$

$$k = 9 : \ 4 \leq s \leq 6 \Rightarrow s = 5$$

Για $k > 9$ θα δείξουμε ότι $\sqrt{4k} - (\sqrt{3k-2} - 1) > 2$.

$$\sqrt{4k} - (\sqrt{3k-2} - 1) > 2 \Leftrightarrow$$

$$\sqrt{4k} - \sqrt{3k-2} > 1 \Leftrightarrow$$

$$4k + 3k - 2 - 2\sqrt{4k}\sqrt{3k-2} > 1 \Leftrightarrow$$

$$2\sqrt{4k(3k-2)} < 7k - 3 \Leftrightarrow$$

$$4 \cdot 4k(3k-2) < 49k^2 - 42k + 9 \Leftrightarrow$$

$$k^2 - 10k + 9 > 0$$

Το πολυώνυμο έχει ρίζες τα -1 και 9 και άρα για $k > 9$ το πολυώνυμο είναι θετικό και η ανισότητα ισχύει.

□

4.5 Ο αριθμός λύσεων της ισοτιμίας $x^2 \equiv R \pmod{D}$

Θεώρημα 4.5.1:

Έστω R ακέραιος και p περιττός πρώτος με $(p, R) = 1$. Αν η $x^2 \equiv R \pmod{p^n}$ έχει λύση s τότε έχει ακριβώς δύο λύσεις, τις s και $-s$.

Απόδειξη:

Αν το s είναι λύση της ισοτιμίας προφανώς θα είναι και το $-s$.

Αφού $(p, R) = 1$ έπεται ότι $s \not\equiv -s \pmod{p^n}$. Αν ίσχυε $s \equiv -s \pmod{p^n}$, θα είχαμε ότι $p^n | 2s$ και αφού p περιττός πρώτος, το p θα διαιρούσε το s. Όμως $s^2 \equiv R \pmod{p^n}$, άρα $p^n | s^2 - R$ και αφού $p|s$ θα πρέπει $p|R$, άτοπο.

Έστω τώρα ότι η ισοτιμία είχε και μια άλλη λύση t, τότε $t^2 \equiv s^2 \pmod{p^n}$ και έπεται

$$(t - s)(t + s) \equiv 0 \pmod{p^n}$$

Αν το p διαιρούσε και τους δύο παράγοντες θα διαιρούσε και τη διαφορά τους, δηλαδή το $2s$, τότε όπως πριν $p|R$, άτοπο. Άρα το p^n διαιρεί ή το $t - s$ ή το $t + s$, δηλαδή $t \equiv \pm s \pmod{p^n}$.

□

Θεώρημα 4.5.2 (Κινέζικο Θεώρημα Υπολοίπων):

Έστω m και n θετικοί ακέραιοι πρώτοι μεταξύ τους. Έστω s και t ακέραιοι τ.ω. $ms - nt = 1$. Τότε $x \equiv a \pmod{m}$ και $x \equiv b \pmod{n}$ αν και μόνο αν $x \equiv a + ms(b - a) \pmod{mn}$.

Απόδειξη:

$$x \equiv b \pmod{n}$$

$$\Leftrightarrow\ x \equiv a + b - a + nt(b - a) \pmod{n}$$

$$\Leftrightarrow\ x \equiv a + (1 + nt)(b - a) \pmod{n}$$

$$\Leftrightarrow\ x \equiv a + ms(b - a) \pmod{n}$$

Επίσης $x \equiv a \pmod{m} \Leftrightarrow x \equiv a + ms(b-a) \pmod{m}$. Αφού $(m,n) = 1$, έχουμε ότι $x \equiv b \pmod{n}$ και $x \equiv a \pmod{m}$ αν και μόνο αν $x \equiv a + ms(b-a) \pmod{mn}$

□

Θεώρημα 4.5.3:

Έστω m και n ακέραιοι > 1 σχετικά πρώτοι και $f(x)$ πολυώνυμο με ακέραιους συντελεστές. Αν η $f(x) \equiv 0 \pmod{m}$ έχει λυσεις $a_1, ..., a_p \pmod{m}$ και η $f(x) \equiv 0 \pmod{n}$ έχει λυσεις $b_1, ..., b_q \pmod{m}$, τότε η $f(x) \equiv 0 \pmod{mn}$ έχει ακριβώς pq λύσεις, αυτές που προκύπτουν από το Κινέζικο θεώρημα υπολοίπων για όλα τα δυνατά ζευγάρια $x \equiv a_i \pmod{m}$ και $x \equiv b_j \pmod{n}$.

Απόδειξη:

Αρκεί να δείξουμε ότι οι pq λύσεις που προκύπτουν από το Κινέζικο θεώρημα υπολοίπων είναι διαφορετικές $\pmod{mn}$. Αν

$$a_1 + ms(b_1 - a_1) \equiv a_2 + ms(b_2 - a_2) \pmod{mn}$$

τότε $a_1 \equiv a_2 \pmod{m}$ και

$$a_1 + (1+nt)(b_1 - a_1) \equiv a_2 + (1+nt)(b_2 - a_2) \pmod{n}$$

άρα $a_1 + b_1 - a_1 + nt(b_1 - a_1) \equiv a_2 + b_2 - a_2 + nt(b_2 - a_2) \pmod{n}$, δηλαδή $b_1 \equiv b_2 \pmod{n}$.

□

Από τα θεωρήματα 4.5.1 και 4.5.3 έχουμε

Θεώρημα 4.5.4:

Έστω D περιττός ακέραιος και $(a, D) = 1$, αν r το πλήθος των διακεκριμένων πρώτων διαιρετών του D, τότε η $x^2 \equiv a \pmod{D}$ ή δεν έχει καμία λύση ή έχει 2^r λύσεις.

Βιβλιογραφία

[1] W. S. Anglin: The Queen of Mathematics, An Introduction to Number Theory, Kluwer Academic Publishers, Dordrecht 1995.

[2] P. Bachmann: Zahlentheorie IV, Die Arithmetik der quadratischen Formen, Leipzig, 1898.

[3] D. A. Cox: Galois Theory, Wiley-Interscience, New Jersey 2004.

[4] Coxeter: Introduction to Geometry, second edition, Wiley Classics Library, New York 1969.

[5] D. W. DeTemple: Carlyle Circles and the Lemoine Simplicity of polygon constructions, The American Mathematical Monthly, Vol. 98, No 2. (Feb. 1991), pp 97-108.

[6] P. G. L. Dirichlet: Lectures on Number Theory, supplements by R. Dedekind, translated by J. Stillwell, American Mathematical society, London Mathematical Society, 1999.

[7] Euclid: The Thirteen Books of the Elements, translated with introduction and commentary by Sir Thomas L. Heath, Vol 1, second edition unabridged, New York 1956.

[8] J. B. Fraleigh: Εισαγωγή στην Άλγεβρα, Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο, 1999.

[9] C. F. Gauss: Disquisitiones Arithmeticae, English Edition, Springer-Verlag, New York, 1966.

[10] G. H. Hardy-E. M. Wright: An introduction to the Theory of Numbers, fifth edition, Oxford, 1979.

[11] J. Hermes: Ueber die Teilung des Kreises in 65537 gleiche Teile, Nachr. $K\ddot{o}nigl$. Gesellsch. $G\ddot{o}ttingen$, Math.-Phys. Klasse, pp. 170-186, 1894.

[12] K. Ireland and M. Rosen: A classical introduction to Modern Number Theory, second edition Springer-Verlag, Berlin 1990.

[13] G. A. Jones and J. M. Jones: Elementary Number Theory, Springer-Verlag, New York 2006.

[14] F. Lemmermeyer: Reciprocity Laws, From Euler to Eisenstein, Springer-Verlag, Berlin 2000.

[15] P. Morandi: Field and Galois Theory, Graduate Texts in Math. Springer-Verlag, New York 1996.

[16] T. Nagell: Introduction to Number Theory, second edition, Chelsea Publishing Company, New York, 1981.

[17] F. J. Richelot: De resolutione algebraica aequationis $x^{257} = 1$, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata, J. reine angew. Math. 9, 1-26, 146-161, 209-230 and 337-358, 1832.

[18] W. Scharlau-H. Opolka: From Fermat to Minkowski, Lectures on the Theory of Numbers and Its Historical Development Springer-Verlag, New York 1985.

[19] I. Stewart: Galois Theory, second edition, Chapman and Hall, London 1989.

[20] J. J. Tattersall: Elementary Number Theory in Nine Chapters, second edition, Cambridge 2005.

[21] B. A. Venkov: Elementary Number Theory, Wolters-Noordhoff Publishing Groningen, The Netherlands, 1970.

[22] B. L. Van Der Waerden: Η Αφύπνιση της Επιστήμης, Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο, 2000.

[23] Ι. Α. Αντωνιάδης: Θεωρία αριθμών και εφαρμογές, υπο έκδοση.

[24] Γ. Τσίντσιφα: Γεωμετρία, Τεύχος 1, Εκδόσεις Σύγχρονου Βιβλιοπωλείου.

[25] Ευκλείδη Στοιχεία, τομος 1, Κέντρο Έρευνας Επιστήμης και Εκπαίδευσης, Αθήνα 2001.