ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΤΜΗΜΑ ΜΕΘΟΔΟΛΟΓΙΑΣ, ΙΣΤΟΡΙΑΣ
ΚΑΙ ΘΕΩΡΙΑΣ ΤΗΣ ΕΠΙΣΤΗΜΗΣ
ΤΜΗΜΑ ΦΙΛΟΣΟΦΙΑΣ – ΠΑΙΔΑΓΩΓΙΚΗΣ & ΨΥΧΟΛΟΓΙΑΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΣΤΑΤΙΣΤΙΚΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΩΝ ΑΓΩΓΗΣ

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών
"ΔΙΔΑΚΤΙΚΗ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΚΕΡΑΙΟΙ GAUSS

ΘΑΝΑΣΗΣ ΤΖΙΩΤΖΙΟΣ

Επιβλέπων Καθηγητής:

ΕΥΑΓΓΕΛΟΣ ΡΑΠΤΗΣ

ΑΘΗΝΑ
ΙΟΥΝΙΟΣ 2011

Η παρούσα Διπλωματική Εργασία

εκπονήθηκε στα πλαίσια των σπουδών

για την απόκτηση του

Μεταπτυχιακού Διπλώματος Ειδίκευσης

που απονέμει το

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

«Διδακτική και Μεθοδολογία των Μαθηματικών»

Εγκρίθηκε την ……από Εξεταστική Επιτροπή αποτελούμενη από τους:

Ονοματεπώνυμο	Βαθμίδα	Υπογραφή
1) Ευάγγελος Ράπτης (επιβλέπων Καθηγητής)	Καθηγητής	……...
2) Δημήτριος Βάρσος	Αν. Καθηγητής	……..…….
3) Διονύσιος Λάππας	Αν. Καθηγητής	……...…….

ΑΚΕΡΑΙΟΙ

GAUSS

ΘΑΝΑΣΗΣ ΤΖΙΩΤΖΙΟΣ

Επιβλέπων Καθηγητής:

ΕΥΑΓΓΕΛΟΣ ΡΑΠΤΗΣ

ΑΘΗΝΑ
ΙΟΥΝΙΟΣ 2011

Ε Υ Χ Α Ρ Ι Σ Τ Ι Ε Σ

Η διπλωματική εργασία που ακολουθεί έχει εκπονηθεί στα πλαίσια της ολοκλήρωσης των σπουδών μου στο Διαπανεπιστημιακό - Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών «Διδακτική και Μεθοδολογία των Μαθηματικών». Στο τέλος αυτής της προσπάθειας αισθάνομαι την ανάγκη να εκφράσω τις **θερμές ευχαριστίες μου και την μεγάλη εκτίμησή μου** στους ανθρώπους που με βοήθησαν σε όλη αυτή την πορεία και ειδικότερα:

- ✶ Στον επιβλέποντα καθηγητή μου κ. **Ευάγγελο Ράπτη**, για την επιλογή του θέματος και την αμέριστη υποστήριξη που μου παρείχε ανά πάσα στιγμή.
- ✶ Στα μέλη της τριμελούς επιτροπής αν. Καθηγητές κ. **Δημήτριο Βάρσο** και κ. **Διονύσιο Λάπα**, για την ευγενική συμμετοχή τους και την προσοχή τους.
- ✶ Σε όλους τους **καθηγητές** που συνέβαλαν στην προσφορά γνώσεων και στην ανάπτυξη ιδεών κατά την διάρκεια των μαθημάτων. Αναδεικνύοντας κατά τον καλύτερο τρόπο την ρήση Leibnitz ότι το μέτρο της ελευθερίας και της άγνοιας μας είναι ταυτόσημο.
- ✶ Στους συμφοιτητές μου που άνοιγαν, με τις ιδέες τους και τις προτάσεις τους, νέες οδούς σκέψεις. Εκ των οποίων ιδιαίτερα θα σταθώ στους φίλους μου **Αγγελική Χόρτη** και **Νίκο Αντωνόπουλο** συνοδοιπόρους στην γόνιμη αυτή περιπλάνηση.

Ιούνιος 2011

Θανάσης Τζιώτζιος

«Αφιερωμένη στις
γλυκές μου κορούλες
Ναταλία και Ραφαέλα»

Π Ε Ρ Ι Ε Χ Ο Μ Ε Ν Α

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ ΚΑΙ ΠΙΝΑΚΩΝ

Ε Ι Σ Α Γ Ω Γ Η

Η συνισταμένη σχεδόν όλων των απαντήσεων από όσες έχουν δοθεί, στο ερώτημα τι είναι τα Μαθηματικά συγκλίνει στο ότι είναι η μελέτη των μετρικών σχέσεων και των ιδιοτήτων που τις διέπουν. Τα τελευταία χρόνια αυτές οι σχέσεις εξετάζονται ως δομικά συστήματα. Δηλαδή επιχειρείται η ομαδοποίηση τους σε συνεκτικές ενότητες σχέσεων. Με τον τρόπο αυτόν επιτυγχάνεται η κατανόηση της πραγματικότητας, όχι απλώς μέσω της γενίκευσης εμπειρικών αντικειμένων, αλλά έχοντας ως βάσεις θεωρητικές έννοιες που εκφράζουν σχέσεις δεδομένων. Είναι αυτό ακριβώς που αποκαλούμε θεωρητική προσέγγιση.

Οι ακέραιοι αριθμοί, όπως και το υποσύνολό τους οι φυσικοί, είναι οι αριθμοί που αποτελούν τη βάση πολυάριθμων καθημερινών εφαρμογών και συγχρόνως δίνουν λύσεις σε πλήθος προβλημάτων που προκύπτουν σε πολλούς και διαφορετικούς επιστημονικούς τομείς. Αναπόφευκτα λοιπόν απαρτίζουν και τα θεμέλια του αριθμητικού μας συστήματος. Αποτέλεσμα αυτού είναι η διδασκαλία τους σε όλες τις τάξεις της δευτεροβάθμιας εκπαίδευσης να είναι πρωτεύουσας βαρύτητας. Ο δε Μαθηματικός που επωμίζεται το φορτίο της διδασκαλίας τους θα πρέπει να έχει την κατάλληλη μαθηματική υποδομή, σε σχέση με το συγκεκριμένο αντικείμενο. Δηλαδή ένα κράμα ευρύτερων Μαθηματικών γνώσεων και ενδιαφερόντων. Με αποτέλεσμα να είναι σε θέση να παρέχει την απαιτούμενη δυνατότητα καλλιέργειας των μαθητών του στον θεωρητικό τρόπο σκέψης, που υπερβαίνει τον απλοϊκό εμπειρισμό της καθημερινής ζωής.

Σύγχρονες μελέτες που σχετίζονται με την βελτίωση στην απόκτηση Μαθηματικών γνώσεων έχουν επισημάνει την σημασία της εννοιολογικής κατανόησης τους. Η οποία δεν είναι εφικτό να αναπτυχθεί απλώς με την μηχανιστική εξάσκηση στους διαδικαστικούς χειρισμούς των Μαθηματικών.

Συνεπώς η γενίκευση του συνόλου των ακεραίων με υπερσύνολα που έχουν την δυναμική να διατηρούν τις ιδιότητες των και να τις επεκτείνουν δεν είναι απλά χρήσιμη αλλά απαραίτητη. Η πλήρης κατανόηση της δομής ενός από αυτά τα υπερσύνολα, θα διαλευκάνουν πολλές πτυχές του αρχικού συνόλου. Κατά αυτόν τον τρόπο οι ακέραιοι αριθμοί δεν θα είναι πλέον τίποτα άλλο παρά μια τετριμμένη περίπτωση. Ένα τέτοιο υπερσύνολο που περικλείει όλα τα προαναφερθέντα χαρακτηριστικά και είναι αρκετά εύχρηστο αποτελούν οι ακέραιοι Gauss. Το αντιπροσωπευτικότερο από όσα θα μπορούσαμε να επιλέξουμε.

Στον αντίποδα όλων των παραπάνω, το ίδιο ακριβώς σύνολο αποτελεί και την πιο προσιτή επιλογή πύλης εισόδου για μια πιο ενδελεχή περιπλάνηση και στον κόσμο των μιγαδικών αριθμών. Οι αριθμοί αυτοί που διδάσκονται στην τελευταία τάξη του Λυκείου, αποτέλεσαν για τους Μαθηματικούς ένα ιδιαίτερα δυσερμήνευτο πεδίο. Από την φάση της αμφισβήτησής τους (Gardano) μέχρι την φάση της αυστηρής εισαγωγής τους και πλέον της αποδοχής τους (Hamilton, Cauchy, Gauss, Riemann).

Η μοντελοποίησή τους με την βοήθεια του διατεταγμένου ζεύγους πραγματικών αριθμών, αποτέλεσε εννοιολογικό πρόβλημα που σχετίζεται με την πληρότητα των πραγματικών. Η εξίσωση $x^2 + 1 = 0$ που ζητούμε λύσεις είναι μιας μεταβλητής, ενώ οι μιγαδικοί που προκύπτουν είναι διδιάστατοι. Η προσέγγιση τέτοιου είδους προβλημάτων μπορεί να επιτευχθεί αρχίζοντας με την κατανόηση δομών πιο προσιτών, όπως οι αντίστοιχοι ακέραιοι που περιέχονται μέσα σε αυτό. Επίσης και οι επέκταση ορισμένων ιδιοτήτων καθώς και οι διαφοροποιήσεις στην άλγεβρά τους, είναι δυνατόν να γίνουν πιο σαφείς μέσω της εμπέδωσης των αρχικών ιδιοτήτων σε επιμέρους υποσύνολα τους.

Στην παρουσίαση που ακολουθεί σχετικά με τους ακεραίους Gauss έχει δοθεί βαρύτητα στην ανάλυση και επεξεργασία του συνόλου των αριθμών αυτών καθώς και στην διαμέρισή τους σε υποσύνολα με ευδιάκριτα χαρακτηριστικά. Στόχος της είναι η επίτευξη της αυστηρότητας και της βεβαιότητας που απαιτεί η μαθηματική επιστήμη ως a priori. Για τον λόγο

αυτόν ακολουθείται η αποδεικτική πορεία θεμελίωσης συμπερασμάτων. Η εργασία έχει χωρισθεί σε δύο ενότητες με σκοπό την καλύτερη ομαδοποίηση και ανάλυση των παρεχόμενων γνώσεων. Σε αρκετά σημεία της υπάρχουν αναφορές και αποδείξεις προαπαιτουμένων γνώσεων από τον χώρο της Άλγεβρας. Όπως επίσης και ανάλογες ιστορικές αναφορές σχετικά με τα αναφερόμενα μαθηματικά αντικείμενα και την προέλευσή τους.

Το πρώτο μέρος αρχίζει με την θεμελίωσή του συνόλου αυτού και τις εσωτερικές ιδιότητες που το διέπουν. Καθώς επίσης με τον ορισμό όσο και τον προσδιορισμό των πρώτων ακεραίων Gauss. Προσδίδεται μεγάλη σημασία στην μοναδική παραγοντοποίηση κάθε ακεραίου σε πρώτους και τα πλεονεκτήματα που παρουσιάζει η συγκεκριμένη ιδιότητα. Ακολούθως εμφανίζεται η απεικόνισή τους, μέσω της ομαδοποίησής που γίνεται σε ισοϋπόλοιπους. Ιδιαίτερη αναφορά υπάρχει στην βοήθεια που μας παρέχουν στην επίλυση κλασικών προβλημάτων της Θεωρίας Αριθμών καθώς και σε πλήθος άλλων εκκρεμών ζητημάτων. Με τον τρόπο αυτό είναι φανερή η χρήση τους και οι έξυπνες λύσεις που μπορούν να προσφέρουν σε τομείς που η απουσία τους θα τους έκανε ιδιαίτερα δύσκολους. Επίσης εκτίθενται σε προβλήματα που παραμένουν ακόμη άλυτα στα Μαθηματικά και σε εικασίες που έχουν διατυπωθεί σχετικά με τους πραγματικούς ακεραίους.

Το δεύτερο μέρος αποτελεί μια πιο εξειδικευμένη ανάλυση του συγκεκριμένου συνόλου. Αρχικά παρουσιάζονται αποδεικτικά πιο ειδικές προτάσεις της Άλγεβρας που θεωρούνται όμως υποχρεωτικές για την περαιτέρω μελέτη. Αφού γίνει η πλήρης παρουσίαση της πράξης της διαίρεσης των ακεραίων Gauss, ακολουθεί η δημιουργία ιδεωδών τους και των ομομορφισμών που τα συνοδεύουν. Στη συνέχεια εμφανίζονται οι δακτύλιοι πηλίκα που προέρχονται από τα ιδεώδη, με τις αντίστοιχες ιδιότητες τους. Στο τέλος συντίθεται, από τα προαναφερόμενα, το αρχικό σύνολο ώστε να γίνει πιο σαφής η δομή του.

Ως γνωστών ο χαρακτήρας της Μαθηματικής επιστήμης διακρίνεται από μια ατέρμονη προσπάθεια να επιτύχει το αδιάψευστο και αλάνθαστο, εγγενών (σύμφωνα με τον Πλάτωνα) ή κατασκευαστικών (κατά Αριστοτέλη)

γνώσεων. Όπως και να είναι ωθούμενος της προσπάθειας αυτής μου δίνεται η ευκαιρία να κλείσω την εισαγωγή της παρούσας εργασίας χρησιμοποιώντας μια φράση από τον David Tall. Η οποία πιστεύω ότι για τους επιστήμονες όσο και για τους μη ειδικούς που ασχολούνται με τα Μαθηματικά θεωρείται αξίωμα: «Τα μαθηματικά δεν είναι άθλημα για θεατές».

ΚΕΦΑΛΑΙΟ 1 | ΑΚΕΡΑΙΟΙ GAUSS

Η αίσθηση για τις αφηρημένες επιστήμες γενικά και ιδιαίτερα για τα μυστήρια των αριθμών, είναι κάτι το εξαιρετικά σπάνιο. Ο μέσος άνθρωπος δεν εκπλήσσεται μπροστά τους, η γοητεία αυτής της ανώτερης επιστήμης αποκαλύπτεται μόνο σε όσους έχουν το κουράγιο να προχωρήσουν βαθειά μέσα της.

CARL FRIEDRICH GAUSS

1.0 Εισαγωγικές Έννοιες της Άλγεβρας

Το περιβάλλον μέσα στο οποίο θα αναπτύξουμε τις έννοιες που θα μας απασχολήσουν στην συγκεκριμένη εργασία, μας το παρέχει η Άλγεβρα με την δυναμική που την χαρακτηρίζει λόγω της σημειολογικής αρχιτεκτονικής της. Συνεπώς μια πρώτη ξενάγηση στις βασικές ορολογίες και στους συμβολισμούς της, είναι απαραίτητη για την ευκολότερη και πιο ολοκληρωμένη κατανόηση των επόμενων βημάτων μας.

Ένας κανόνας μέσω του οποίου κάθε διατεταγμένο ζεύγος (α, β) δύο στοιχείων ενός συνόλου Σ αντιστοιχεί σε μοναδικό στοιχείο του Σ ονομάζεται **διμελής πράξη** ή απλά **πράξη**. Η απαίτηση σχετικά με το αποτέλεσμα να ανήκει πάλι στο ίδιο σύνολο είναι γνωστή ως **κλειστότητα**. Κάποιο σύνολο Σ μαζί με κάποιες διμελείς πράξεις μεταξύ των στοιχείων του συνόλου αυτού, αποτελούν μια **δομή.** Η κατάταξη των δομών που θα ακολουθήσουμε είναι από τις πιο γενικές και συγχρόνως πιο απλές σε πιο ειδικές και αναπόφευκτα πιο περίπλοκες. Η αρχή γίνεται με τον ορισμό της ομάδας.

Ομάδα $\langle G, * \rangle$ ονομάζεται η δομή που αποτελείται από ένα μη κενό σύνολο G και μια διμελή πράξη $*$ στο G που έχει τις εξής ιδιότητες:

- Προσεταιριστική: για κάθε $x, y, z \in G$ να ισχύει:

$$x * (y * z) = (x * y) * z.$$

- Ύπαρξη ουδετέρου στοιχείου: για κάθε $x \in G$ υπάρχει μοναδικό $e \in G$ ώστε να ισχύει:

$$e * x = x * e = x.$$

- Ύπαρξη αντίστροφου στοιχείου: για κάθε $x \in G$ υπάρχει μοναδικό $x' \in G$ ώστε να ισχύει:

$$x * x' = x' * x = e.$$

Αν επιπλέον η πράξη $*$ είναι αντιμεταθετική, δηλαδή για κάθε $x, y \in G$ να ισχύει:

$$x * y = y * x$$

τότε η ομάδα καλείται **αβελιανή** ή **αντιμεταθετική.**

Συνήθως στις ομάδες την πράξη που επισυνάπτουμε την ονομάζουμε πρόσθεση με σύμβολο το $+$ και ως ουδέτερο στοιχείο χρησιμοποιούμε το μηδενικό 0, ενώ ως αντίστροφο του στοιχείου x θα είναι ο αντίθετος του $-x$.

Δακτύλιος $<D, +, \cdot>$ ονομάζεται μια δομή που αποτελείται από ένα μη κενό σύνολο D και από δύο διμελείς πράξεις, την πρόσθεση $+$ και τον πολλαπλασιασμό $\cdot$ στο D, έτσι ώστε:

- Η δομή $<D, +>$ να είναι αβελιανή ομάδα.
- Ο πολλαπλασιασμός να υπακούει στην προσεταιριστική ιδιότητα, δηλαδή για κάθε $x, y, z \in D$ να ισχύει:

$$x\cdot(y\cdot z) = (x\cdot y)\cdot z.$$

- Ο πολλαπλασιασμός να είναι επιμεριστικός ως προς την πρόσθεση, δηλαδή για κάθε $x, y, z \in D$ να ισχύει:

$$x\cdot(y + z) = (x\cdot y) + (x\cdot z) \text{ και } (x + y)\cdot z = (x\cdot z) + (y\cdot z).$$

Σε κάθε δακτύλιο εύκολα αποδεικνύεται ότι ισχύουν οι εξής σχέσεις:

$$x\cdot 0 = 0\cdot x = 0 \text{ και } x\cdot(-y) = (-x)\cdot y = -(x\cdot y).$$

Κάθε μη κενό σύνολο H που είναι υποσύνολο ενός δακτυλίου D και είναι επίσης δακτύλιος με τις ίδιες πράξεις που υπάρχουν στον D, ονομάζεται **υποδακτύλιος.**

Αν σε έναν δακτύλιο $<D, +, \cdot>$ ο πολλαπλασιασμός υπακούει στην αντιμεταθετική ιδιότητα, δηλαδή για κάθε $x, y \in D$ να ισχύει:

$$x\cdot y = y\cdot x$$

τότε ονομάζεται **αντιμεταθετικός δακτύλιος.**

Αν τώρα σε έναν δακτύλιο $<D, +, \cdot>$ υπάρχει και το ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό, δηλαδή για κάθε $x \in D$ να υπάρχει μοναδικό e ώστε να ισχύει:

$$x \cdot e = e \cdot x = x$$

τότε ονομάζεται **δακτύλιος με μονάδα.** Το στοιχείο αυτό καλείται μοναδιαίο και το συμβολίζουμε με 1.

Σε έναν δακτύλιο $<D, +, \cdot>$ με μοναδιαίο, κάθε στοιχείο $x \in D$ για το οποίο υπάρχει μοναδικό $x^{-1} \in D$ ώστε:

$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$

θα ονομάζεται **αντιστρέψιμο.**

Ακέραια Περιοχή $<D, +, \cdot>$ λέγεται ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στον οποίο δεν υπάρχουν διαιρέτες του μηδενός, δηλαδή αν δύο στοιχεία $x, y \in D$ ώστε:

$$x \cdot y = 0 \text{ τότε } x = 0 \text{ ή } y = 0.$$

Τέλος μια ακέραια περιοχή $<D, +, \cdot>$ στην οποία η δομή $<D\backslash\{0\}, \cdot>$ είναι ομάδα, καλείται **σώμα.**

1.1 Θεμελίωση

Από το σύνολο των πραγματικών αριθμών έχουμε την δυνατότητα να επιλέξουμε ένα υποσύνολο, τους ακέραιους, που αποτελεί ακέραια περιοχή με πολλές και ενδιαφέρουσες ιδιότητες. Παρόλα αυτά όταν ο πρίγκιπας των Μαθηματικών Carl Friedrich Gauss στα 1829 προσπαθούσε να διατυπώσει τον νόμο της διτετραγωνικής αντιστροφής, δεν του ήταν κατάλληλο. Οπότε με αντίστοιχη διαδικασία από τους μιγαδικούς εφεύρε ένα εξίσου σημαντικό σύνολο το $\mathbb{Z}[i]$. Φυσιολογικά λοιπόν τα στοιχεία του συνόλου αυτού ονομάστηκαν **ακέραιοι Gauss** (Gaussian integers). Η μελέτη της άλγεβρας τους θα μας βοηθήσει να το ερευνήσουμε με μεγαλύτερη λεπτομέρεια, ώστε να προσεγγίσουμε πιο αναλυτικά, το ίδιο το $\mathbb{Z}$ που άλλωστε όπως θα δούμε αποτελεί υποσύνολο του. Δίνοντας μας έτσι την ευκαιρία να εμπλουτίσουμε

τα ήδη υπάρχοντα μέσα, με στόχο να διευρύνουμε και να ενοποιούμε τις ιδέες που περιέχονται και στα δύο σύνολα.

Ορισμός 1.1: Ως σύνολο των ακεραίων Gauss ορίζεται το:

$$\mathbb{Z}[i] = \{\alpha + \beta i \,/\, \alpha, \beta \in \mathbb{Z} \text{ και } i^2 = -1\}.$$

Αν $\zeta = \alpha + \beta i$ είναι στοιχείο του συνόλου $\mathbb{Z}[i]$ τότε τον πραγματικό ακέραιο $\alpha^2 + \beta^2$ τον ονομάζουμε **στάθμη** (norm) του ζ και τον συμβολίζουμε με $\mathbf{N(\zeta)}$.

Η σημαντικότητα της στάθμης γίνεται φανερή ήδη από τις παρακάτω ιδιότητες, οι οποίες ισχύουν για κάθε $\zeta, \xi \in \mathbb{Z}[i]$:

(I) $N(\zeta) \geq 0$.

(II) $N(\zeta) = 0 \Leftrightarrow \zeta = 0$

(III) $N(\zeta \cdot \xi) = N(\zeta) \cdot N(\xi)$.

Θέτοντας $\zeta = \alpha + \beta i$ και $\xi = \gamma + \delta i$ οι παραπάνω είναι άμεσα αποδείξιμες.

Θεώρημα 1.1: Η $\mathbb{Z}[i]$ αποτελεί ακέραια περιοχή.

Απόδειξη: Επισυνάπτουμε στο σύνολο $\mathbb{Z}[i]$ τις ήδη γνωστές από τους μιγαδικούς αριθμούς πράξεις:

- Πρόσθεση: για κάθε $\zeta, \xi \in \mathbb{Z}[i]$ τότε $(\zeta, \xi) \to \zeta + \xi$.
- Πολλαπλασιασμός: για κάθε $\zeta, \xi \in \mathbb{Z}[i]$ τότε $(\zeta, \xi) \to \zeta \cdot \xi$.

Ακολουθώντας τα παρακάτω τρία βήματα θα έχουμε:

(1) Η $<\mathbb{Z}[i], +>$ θα δείξουμε ότι είναι αβελιανή ομάδα, αφού για κάθε $\zeta, \xi, \varphi \in \mathbb{Z}[i]$ με $\zeta = \alpha + \beta i$, $\xi = \gamma + \delta i$ και $\varphi = \varepsilon + \eta i$, ισχύουν:

- $\zeta + \xi = (\alpha + \gamma) + (\beta + \delta)i \in \mathbb{Z}[i]$, δηλαδή η πράξη είναι εσωτερική.
- Για το στοιχείο $e = x + yi \in \mathbb{Z}[i]$ αν $\zeta + e = \zeta \Leftrightarrow \alpha + x + (\beta + y)i = \alpha + \beta i$. Άρα $\alpha + x = \alpha$ και $\beta + y = \beta$, οπότε $x = y = 0$. Επομένως υπάρχει ουδέτερο στοιχείο, το μηδενικό $0 = 0 + 0i$.
- Για το στοιχείο $\zeta' = x + yi \in \mathbb{Z}[i]$ αν $\zeta + \zeta' = 0 \Leftrightarrow \alpha + x + (\beta + y)i = 0 + 0i$. Άρα $\alpha + x = 0$ και $\beta + y = 0$, επιλύοντας $x = -\alpha$ και $y = -\beta$. Συνεπώς υπάρχει ο αντίθετος του ζ που είναι ο $-\zeta = -\alpha - \beta i$.

- $\zeta + (\xi + \varphi) = (\alpha + \beta i) + [(\gamma + \varepsilon) + (\delta + \eta)i] = (\alpha + \gamma + \varepsilon) + (\beta + \delta + \eta)i = [(\alpha + \gamma) + (\beta + \delta)i] + (\varepsilon + \eta i) = (\zeta + \xi) + \varphi$. Δηλαδή η πράξη είναι προσεταιριστική.
- $\zeta + \xi = (\alpha + \gamma) + (\beta + \delta)i = (\gamma + \alpha) + (\delta + \beta)i = \xi + \zeta$. Άρα η πράξη είναι αντιμεταθετική.

(2) Ο $<\mathbb{Z}[i], +, \cdot>$ θα δείξουμε ότι είναι αντιμεταθετικός δακτύλιος έχοντας και μοναδιαίο, αφού για κάθε $\zeta, \xi, \varphi \in \mathbb{Z}[i]$ με $\zeta = \alpha + \beta i$, $\xi = \gamma + \delta i$ και $\varphi = \varepsilon + \eta i$, ισχύουν:

- $\zeta \cdot \xi = (\alpha\gamma - \beta\delta) + (\beta\gamma + \alpha\delta)i \in \mathbb{Z}[i]$. Άρα η πράξη $(\cdot)$ είναι εσωτερική.
- $\zeta \cdot (\xi \cdot \varphi) = (\alpha + \beta i) \cdot [(\gamma\varepsilon - \delta\eta) + (\gamma\eta + \delta\varepsilon)i] = (\alpha\gamma\varepsilon - \alpha\delta\eta - \beta\gamma\eta - \beta\delta\varepsilon) + (\alpha\gamma\eta + \alpha\delta\varepsilon + \beta\gamma\varepsilon + \beta\delta\eta)i = [(\alpha\gamma - \beta\delta) + (\beta\gamma + \alpha\delta)i] \cdot (\varepsilon + \eta i) = (\zeta \cdot \xi) \cdot \varphi$. Δηλαδή η $(\cdot)$ είναι προσεταιριστική.
- $\zeta \cdot (\xi + \varphi) = (\alpha + \beta i) \cdot [(\gamma + \varepsilon) + (\delta + \eta)i] = (\alpha\gamma + \alpha\varepsilon - \beta\delta - \beta\eta) + (\alpha\delta + \alpha\eta + \beta\gamma + \beta\varepsilon)i = (\alpha\gamma - \beta\delta) + (\alpha\varepsilon - \beta\eta) + (\alpha\delta + \beta\gamma)i + (\alpha\eta + \beta\varepsilon)i = \zeta \cdot \xi + \zeta \cdot \varphi$. Οπότε ο πολλαπλασιασμός είναι επιμεριστική ως προς την πρόσθεση.
- $\zeta \cdot \xi = (\alpha\gamma - \beta\delta) + (\beta\gamma + \alpha\delta)i = (\gamma\alpha - \delta\beta) + (\gamma\beta + \delta\alpha)i = \xi \cdot \zeta$. Δηλαδή η $(\cdot)$ είναι αντιμεταθετική.
- Για το στοιχείο $e = x + yi \in \mathbb{Z}[i]$ και τον $\zeta \neq 0$, αν ισχύει ότι $\zeta \cdot e = \zeta \Leftrightarrow (\alpha x - \beta y) + (\alpha y + \beta x)i = \alpha + \beta i$. Άρα $\alpha x - \beta y = \alpha$ και $\alpha y + \beta x = \beta$, που επιλύοντας το σύστημα έχουμε μοναδικές λύσεις τις $x = 1$ και $y = 0$. Δηλαδή υπάρχει μοναδιαίο στοιχείο ως προς τον πολλαπλασιασμό και αυτό είναι το $1 = 1 + 0i$.

(3) Αρκεί πλέον να δείξουμε ότι ο $\mathbb{Z}[i]$ δεν περιέχει διαιρέτες του μηδενικού. Θεωρώντας τους $\zeta, \xi \in \mathbb{Z}[i]$, με $\zeta \cdot \xi = 0$, από τις ιδιότητες της στάθμης τους είναι: $N(\zeta)N(\xi) = N(\zeta \cdot \xi) = 0 \Leftrightarrow N(\zeta) = 0$ ή $N(\xi) = 0 \Leftrightarrow \zeta = 0$ ή $\xi = 0$. Αλλιώς, αφού το $\mathbb{Z}[i]$ είναι υποσύνολο των μιγαδικών, όπου γνωρίζουμε ότι ισχύει η σχέση $x \cdot y = 0 \Leftrightarrow x = 0$ ή $y = 0$, θα την επαληθεύει.

Συνεπώς ο $\mathbb{Z}[i]$ είναι ακέραια περιοχή. ♦

1.2 Παραγοντοποίηση σε Πρώτους Gauss

Μια σημαντική διαδικασία στους πραγματικούς ακέραιους είναι η παραγοντοποίησή τους σε μη αναλύσιμους περεταίρω ακέραιους, στους πρώτους. Όμως μπορούμε να παρατηρήσουμε ότι κάθε πρώτος πραγματικός ακέραιος δεν είναι υποχρεωτικά και μη αναλύσιμος σε γινόμενο παραγόντων και στο $\mathbb{Z}[i]$. Για παράδειγμα οι αριθμοί:

$$2 = (1 + i)(1 - i) \text{ ή } 5 = (2 + i)(2 - i).$$

Συνεπώς διαγράφεται μια καλή ευκαιρία να διερευνήσουμε την ανάλυση των ακεραίων Gauss σε παράγοντες. Μια ανάλυση η οποία είναι άραγε εφικτή για όλους και αν είναι, τότε με πόσους διαφορετικούς τρόπους μπορεί να επιτευχθεί;

Αρχικά η προσοχή μας εστιάζεται στους αριθμούς $\{1, -1, i, -i\}$ οι οποίοι προφανώς αποτελούν παράγοντες κάθε στοιχείου του $\mathbb{Z}[i]$. Οι αριθμοί αυτοί είναι οι μοναδικοί στο σύνολο αυτό που έχουν στάθμη ίση με 1. Γιατί αν θεωρήσουμε τον ακέραιο Gauss $\zeta = \alpha + \beta i$ με $N(\zeta) = 1$, τότε $\alpha^2 + \beta^2 = 1$ όμως τα $\alpha, \beta \in \mathbb{Z}$ οπότε:

$$\alpha = \pm 1 \text{ και } \beta = 0 \text{ είτε } \alpha = 0 \text{ και } \beta \pm 1.$$

$$\text{Δηλαδή } \zeta = 1 \text{ ή } \zeta = -1 \text{ ή } \zeta = i \text{ ή } \zeta = -i.$$

Μπορούμε λοιπόν τους αριθμούς αυτούς να τους τοποθετήσουμε στην ίδια κατηγορία με τους αριθμούς 1 και -1 του συνόλου $\mathbb{Z}$, και να τους ονομάσουμε **αντιστρέψιμους**.

Αναλυτικότερα λοιπόν σχετικά με την στάθμη κάθε ακεραίου Gauss ζ θα μπορούσαμε να πούμε ότι ισχύει:

$$N(\zeta) \in \mathbb{N} \begin{cases} = 0, & \text{αν } \zeta = 0. \\ = 1, & \text{αν } \zeta = 1, -1, i, -i. \\ > 1, & \text{στις υπόλοιπες περιπτώσεις.} \end{cases}$$

Επιχειρώντας στην παρούσα φάση την ανάλυση ενός ακέραιου Gauss σε πλήθος μη αντιστρέψιμων παραγόντων, αναρωτηθήκαμε πριν αν αυτή περατώνεται σε πεπερασμένα βήματα. Αν παρατηρήσουμε όμως ότι κάθε παραγοντοποίηση μπορεί να μας δώσει και ισότητα στις στάθμες των δύο

μελών τότε, λόγω της πολλαπλασιαστικής τους ιδιότητας (III), η στάθμη του αρχικού ακεραίου είναι ίση με το γινόμενο από τις στάθμες των παραγόντων του. Αλλά η στάθμη του αρχικού ακεραίου καθώς και των παραγόντων που προκύπτουν είναι φυσικοί αριθμοί. Από την αρχή της καθόδου, το πρώτο συμπέρασμα που συνάγεται είναι ότι το πλήθος των παραγόντων θα είναι περατούμενο. Άρα για κάθε ακέραιο $\alpha + \beta i$ η ανάλυση του θα έχει μια μορφή όπως η ακόλουθη:

$$\alpha + \beta i = (\alpha_1 + \beta_1 i)\cdot(\alpha_2 + \beta_2 i)\cdot \ldots \cdot(\alpha_v + \beta_v i).$$

Προφανώς η στάθμη καθενός παράγοντα $(\alpha_\kappa + \beta_\kappa i)$ με $\kappa = 1, 2, \ldots, v$ θα είναι αυστηρά μικρότερη από την στάθμη του αρχικού ακεραίου.

Όταν οι παράγοντες αυτοί δεν αναλύονται περεταίρω και έχουν την μικρότερη μη μοναδιαία στάθμη καλούνται **πρώτοι Gauss** (Gaussian prime). Με άλλα λόγια ο ακέραιος Gauss g είναι ένας πρώτος Gauss:

i. Αν έχει στάθμη μεγαλύτερη της μονάδας.
ii. Αν ο $\alpha \in \mathbb{Z}[i]$ είναι παράγοντας του, τότε θα ισχύει $N(\alpha) = 1$ ή $g = \alpha\cdot\kappa$, με $N(\kappa) = 1$.

Τονίζουμε στο σημείο αυτό ότι οι αντιστρέψιμοι, παρότι δεν αναλύονται περαιτέρω, δεν θεωρούνται πρώτοι.

Επίσης λόγω της πολλαπλασιαστικής ιδιότητας της στάθμης, συμπεραίνουμε ότι κάθε ακέραιος Gauss με στάθμη ίση με έναν πρώτο φυσικό θα είναι πρώτος ακέραιος Gauss. Αυτό ισχύει γιατί στην περίπτωση που θα ήταν δυνατή η παραγοντοποιήσή του σε τουλάχιστον δύο παράγοντες, θα είχαμε την στάθμη του ίση με το γινόμενο από τις στάθμες των επιμέρους παραγόντων. Οπότε ένας τουλάχιστον από αυτούς θα είχε στάθμη ίση με 1, δηλαδή όπως έχουμε αποδείξει θα ήταν αντιστρέψιμος. Το αντίστροφο φυσικά δεν ισχύει. Αναλυτικότερη μελέτη των πρώτων Gauss θα γίνει σε επόμενη παράγραφο.

Μια ενδιαφέρουσα ομάδα ακέραιων Gauss είναι αυτοί που έχουν ως παράγοντα τον πρώτο $1 + i$ και αποκαλούνται **άρτιοι.** Όπως θα δείξουμε στην ακόλουθη πρόταση αυτοί οι αριθμοί είναι και οι μόνοι οι οποίοι έχουν στάθμη άρτιο αριθμό.

Θεώρημα 1.2: Ένας ακέραιος Gauss έχει στάθμη άρτιο αριθμό αν και μόνο αν είναι πολλαπλάσιος του $1 + i$.

Απόδειξη: Επειδή $N(1 + i) = 2$, τότε κάθε πολλαπλάσιος του $1 + i$ θα έχει στάθμη πολλαπλάσια του 2, δηλαδή άρτια. Αντίστροφα, θεωρούμε τον ακέραιο Gauss $\alpha + \beta i$ με $N(\alpha + \beta i) = \alpha^2 + \beta^2$ να είναι άρτιος. Τότε οι α και β θα είναι και οι δύο άρτιοι ή και οι δύο περιττοί. Οπότε και στις δύο περιπτώσεις το $\alpha \pm \beta$ θα είναι άρτιος.

Αν γράψουμε τον $\alpha + \beta i = (1 + i)(\gamma + \delta i)$, αρκεί να δείξουμε ότι $\gamma, \delta \in \mathbb{Z}$. Επειδή ισχύει: $\alpha + \beta i = (\gamma - \delta) + (\gamma + \delta)i$, θα είναι $\alpha = \gamma - \delta$ και $\beta = \gamma + \delta$ που δίνει $\gamma = \frac{\alpha + \beta}{2}$ και $\delta = \frac{\alpha - \beta}{2}$. Άρα $\gamma, \delta \in \mathbb{Z}$. ♦

Πρέπει εδώ να σημειώσουμε ότι και ο $1 - i$ έχει στάθμη 2, όμως προκύπτει από το γινόμενο $-i(1+ i)$. Επίσης από την απόδειξη που είδαμε μπορούμε να συμπεράνουμε πως ένα εύκολο κριτήριο για να αναγνωρίσουμε αν ο $\alpha + \beta i$ αποτελεί άρτιο είναι αν το 2 διαιρεί το $\alpha + \beta$, ή με άλλα λόγια αν οι α, β είναι και οι δύο άρτιοι ή και οι δύο περιττοί ακέραιοι.

Το πρωτεύον ερώτημα που έχουμε θέσει από την αρχή και συνεχίζει να παραμένει ακόμη αναπάντητο είναι αν η ανάλυση κάθε ακεραίου Gauss σε πρώτους Gauss γίνεται κατά μοναδικό τρόπο. Δηλαδή αν το σύνολο $\mathbb{Z}[i]$ αποτελεί μια περιοχή μοναδικής παραγοντοποίησης (unique factorization domain). Στο σημείο αυτό όμως θα πρέπει για μια ακόμη φορά να ανατρέξουμε σε ορισμούς και προτάσεις της Άλγεβρας που θα μας βοηθήσουν να δομήσουμε την έννοια μιας τέτοιας περιοχής.

1.3 Περιοχές Μοναδικής Παραγοντοποίησης

Αν θεωρήσουμε κάποια τυχαία ακέραια περιοχή D η οποία έχει ως μηδενικό στοιχείο το 0, μοναδιαίο στοιχείο το 1 και τα $\alpha, \beta \in D$, τότε:

Ορισμός 1.2: Παράγοντας του α είναι το $\beta \neq 0$ (ή το β διαιρεί το α) αν υπάρχει $\gamma \in D$ τέτοιο ώστε: $\alpha = \beta\gamma$ και συμβολίζουμε β/α.

Ορισμός 1.3: Μοναδιαίος (αντιστρέψιμος) Παράγοντας είναι κάθε στοιχείο $e \in D$ ώστε $e/1$, δηλαδή έχει πολλαπλασιαστικό αντίστροφο.

Ορισμός 1.4: Ισοδύναμοι Παράγοντες ονομάζονται τα στοιχεία α, β αν $\alpha = \beta e$, όπου e κάποιος μοναδιαίος (αντιστρέψιμος) παράγοντας.

Ορισμός 1.5: Ανάγωγο Στοιχείο είναι κάθε στοιχείο $p \in D$ ώστε $p \neq 0$, $p \neq 1$ και κάθε παραγοντοποίηση του μέσα στην D, της μορφής $p = \alpha\beta$ να δίνει $\alpha = e$ ή $\beta = e$.

Ορισμός 1.6: Περιοχή Μοναδικής Παραγοντοποίησης είναι η ακέραια περιοχή D στην οποία για κάθε μη μηδενικό και μη μοναδιαίο στοιχείο της α ισχύουν τα εξής:

- Το α να είναι ίσο με ένα γινόμενο ανάγωγων στοιχείων $p_1, p_2, \ldots, p_n$.
- Αν το α επίσης ισούται με το γινόμενο κάποιων άλλων ανάγωγων στοιχείων $q_1, q_2, \ldots, q_m$, τότε πρέπει $n = m$ και κάθε p_i να είναι ισοδύναμο με ένα q_j.

Συνεπώς με την προϋπόθεση ότι δύο ισοδύναμα στοιχεία ταυτίζονται, η παραγοντοποίηση κάθε στοιχείου της D σε ανάγωγους παράγοντες είναι μοναδική.

Σύμφωνα λοιπόν με τους παραπάνω ορισμούς στην ακέραια περιοχή $\mathbb{Z}$ οι μοναδιαίοι παράγοντες είναι $\{-1, 1\}$ και δύο οποιοιδήποτε αντίθετοι πραγματικοί ακέραιοι είναι ισοδύναμοι παράγοντες. Συνεπώς η ανάλυση ενός πραγματικού ακέραιου θεωρείται μονοσήμαντη αν κάποιοι από τους παράγοντες του είναι αντίθετοι, δηλαδή:

$$36 = 2\cdot2\cdot3\cdot3 = \cdot2\cdot(-2)\cdot(-3)\cdot3.$$

Αλλά και η μεταβολή του πρόσημου σε κάποιους παράγοντες λόγω της παρουσίας του -1 δεν αλλοιώνει την μοναδικότητα της παραγοντοποίησης αυτής, δηλαδή:

$$36 = 2\cdot2\cdot3\cdot3 = (-1)\cdot(-2)\cdot(-2)\cdot(-3)\cdot3.$$

Αυτό αποτελεί άλλωστε και το **θεμελιώδες θεώρημα της Αριθμητικής** που διατυπώνεται ως εξής:

«Κάθε μη μηδενικός και μη μοναδιαίος πραγματικός ακέραιος μπορεί να παραγοντοποιηθεί με μοναδικό τρόπο σε γινόμενο πρώτων παραγόντων με

την επιφύλαξη της μη συμμετοχής των μονάδων». Συνεπώς η ακέραια περιοχή $\mathbb{Z}$ είναι μια περιοχή μοναδική παραγοντοποίησης. Ο βασικός ρόλος του θεωρήματος αυτού για την θεωρία αριθμών είναι εμφανής από τον χαρακτηρισμό του ως θεμελιώδες.

Ορισμός 1.7: Ευκλείδεια Περιοχή (Euclidean domain) ορίζεται μια ακέραια περιοχή D εφοδιασμένη με μια απεικόνιση $\varphi: D\setminus\{0\} \to \mathbb{N}^*$ η οποία ικανοποιεί τις παρακάτω ιδιότητες:

i. Για κάθε μη μηδενικά στοιχεία $\alpha, \beta \in D$, ισχύει: $\varphi(\alpha) \leq \varphi(\alpha\beta)$.
ii. Για κάθε στοιχεία $\alpha, \beta \in D$, με $\beta \neq 0$, να υπάρχουν $\kappa, \upsilon \in D$ τέτοια ώστε $\alpha = \beta\kappa + \upsilon$ όπου $\upsilon = 0$ είτε $\varphi(\upsilon) < \varphi(\beta)$.

Η συνάρτηση φ ονομάζεται **Ευκλείδεια συνάρτηση** (ή εκτίμηση) του D και είναι φανερό ότι σε μια Ευκλείδεια περιοχή μπορεί να υπάρχουν πολλές Ευκλείδειες συναρτήσεις.

Θεώρημα 1.3: Κάθε Ευκλείδεια Περιοχή είναι περιοχή μοναδικής παραγοντοποίησης.

Η απόδειξη του θεωρήματος αυτού (Βάρσος – Δεριζιώτης – Εμμανουήλ – Μαλιάκας - Ταλέλη, «Μια εισαγωγή στην Άλγεβρα» σελ. 217 – 219) έχει παραλειφθεί στην παρούσα εργασία αφού χρησιμοποιούμε μέσα που ξεφεύγουν από το αντικείμενο παρουσίασης της.

Θεώρημα 1.4: Σε κάθε Ευκλείδεια Περιοχή E με Ευκλείδεια συνάρτηση φ, αν $\alpha \in E$ με $\alpha \neq 0$ τότε το $\varphi(1)$ είναι το ελάχιστο από όλα τα $\varphi(\alpha)$ και το α είναι **αντιστρέψιμο** αν και μόνο αν $\varphi(\alpha) = \varphi(1)$.

Απόδειξη: Αφού $\alpha \in E$ με $\alpha \neq 0$ τότε:

$$\varphi(1) \leq \varphi(1\alpha) = \varphi(\alpha).$$

Αν θεωρήσουμε ότι το αντίστροφο του α είναι το α^{-1} τότε ισχύει:

$$\varphi(\alpha) \leq \varphi(\alpha\alpha^{-1}) = \varphi(1) \Rightarrow \varphi(\alpha) = \varphi(1).$$

Αντίστροφα αφού $\varphi(\alpha) = \varphi(1)$ υπάρχουν $\kappa, \upsilon \in E$ ώστε:

$$1 = \alpha\kappa + \upsilon \text{ με } \upsilon = 0 \text{ είτε } \varphi(\upsilon) < \varphi(\kappa).$$

Αν $\upsilon \neq 0$, τότε $1/\upsilon$ και $\varphi(1) < \varphi(\upsilon)$, πράγμα άτοπο. Άρα καταλήγουμε στο $\upsilon = 0$ και $\alpha\kappa = 1$, δηλαδή $\kappa = \alpha^{-1}$. ♦

Η σημασία του παραπάνω θεωρήματος είναι προφανής για την ύπαρξη καθώς και για την εύρεση των αντίστροφων στοιχείων σε μια Ευκλείδεια Περιοχή. Στην συνέχεια θα ασχοληθούμε με τους κοινούς διαιρέτες δύο στοιχείων μιας τέτοιας περιοχής και ειδικά με τον μεγαλύτερο από αυτούς.

Ορισμός 1.8: Μέγιστος Κοινός Διαιρέτης (μ.κ.δ.) δύο στοιχείων α, β μιας περιοχής μοναδικής παραγοντοποίησης D είναι το στοιχείο $\delta \in D$ που πληρεί τις εξής προϋποθέσεις:

- δ/α και δ/β.
- Αν $\gamma \in D$ με γ/α και γ/β τότε γ/δ.

Άμεσο λοιπόν είναι και το επόμενο θεώρημα ύπαρξης – εύρεσης του μ.κ.δ. δύο στοιχείων μιας Ευκλείδειας Περιοχής.

Θεώρημα 1.5: Σε κάθε Ευκλείδεια Περιοχή E με Ευκλείδεια συνάρτηση φ, αν $\alpha, \beta \in E$ με $\alpha, \beta \neq 0$ τότε υπάρχει $\delta \in E$ που είναι μ.κ.δ.$(\alpha, \beta) = \delta$ καθώς επίσης υπάρχουν στοιχεία $\nu, \lambda \in E$ τέτοια ώστε $\delta = \nu\alpha + \lambda\beta$.

Απόδειξη: Σύμφωνα με τον ορισμό της Ευκλείδειας Περιοχής υπάρχουν $\kappa_1, \upsilon_1 \in E$ τέτοια ώστε: $\alpha = \beta\kappa_1 + \upsilon_1$ με $\upsilon_1 = 0$ είτε $\varphi(\upsilon_1) < \varphi(\beta)$. Στην περίπτωση που $\upsilon_1 = 0$ το $\beta = \delta$ και ισχύει $\beta = 0\alpha + 1\beta$.

Όταν $\upsilon_1 \neq 0$, αν ένας κοινός διαιρέτης των α, β είναι ο $\delta_1 \in E$ θα έχουμε:

$$\delta_1/\alpha \text{ και } \delta_1/\beta \text{ άρα } \delta_1/(\alpha - \beta\kappa_1) \Rightarrow \delta_1/\upsilon_1.$$

Δηλαδή οι κοινοί διαιρέτες των α, β διαιρούν και το υ_1. Συνεχίζοντας υπάρχουν $\kappa_2, \upsilon_2 \in E$ τέτοια ώστε: $\beta = \upsilon_1\kappa_2 + \upsilon_2$ με $\upsilon_2 = 0$ είτε $\varphi(\upsilon_2) < \varphi(\upsilon_1)$. Στην περίπτωση που $\upsilon_2 \neq 0$ αποδεικνύεται αντίστοιχα ότι οι όλοι οι κοινοί διαιρέτες των $\alpha, \beta, \upsilon_1$ είναι και διαιρέτες του υ_2.

Επαναλαμβάνοντας την ίδια διαδικασία θα δημιουργηθεί μια σειρά στοιχείων του E τα $\upsilon_1, \upsilon_2, \upsilon_3, \ldots$, για τα οποία ισχύουν $\varphi(\upsilon_i) < \varphi(\upsilon_{i-1})$ και $\varphi(\upsilon_i) \in \mathbb{N}^*$ για κάθε i, οπότε η σειρά αυτή θα είναι περατούμενη. Αν το τελευταίο μη μηδενικό στοιχείο είναι το υ_n τότε τα υ_{n-1} και υ_n θα έχουν τους ίδιους διαιρέτες με όλα τα προηγούμενα υ_i συνεπώς και με τα α, β. Όμως υπάρχει μη μηδενικό $\kappa_{n+1} \in E$ ώστε $\upsilon_{n-1} = \kappa_{n+1} \cdot \upsilon_n$, άρα ο μ.κ.δ. των υ_{n-1} και υ_n επομένως και των α, β θα είναι ο υ_n. Δηλαδή $\delta = \upsilon_n$.

Αντικαθιστώντας τώρα το υ_{n-1} στην σχέση: $\delta = \upsilon_n = \upsilon_{n-1} - \upsilon_{n-2}\cdot\kappa_n$ από την αμέσως προηγούμενη $\upsilon_{n-1} = \upsilon_{n-2} - \upsilon_{n-3}\cdot\kappa_{n-1}$ και ακολουθώντας την ίδια ακριβώς διαδικασία με αντίστροφη πορεία, καταλήγουμε στην εύρεση των δύο στοιχείων $\nu, \lambda \in E$ ώστε $\delta = \nu\alpha + \lambda\beta$. ♦

1.4 Μοναδική Παραγοντοποίηση στο $\mathbb{Z}[i]$.

Επανερχόμαστε τώρα στο σύνολο $\mathbb{Z}[i]$ με σκοπό να αποδείξουμε ότι η παραγοντοποίηση των στοιχείων του σε πρώτους Gauss γίνεται με μοναδικό τρόπο καθώς και τα βασικά συμπεράσματα που προκύπτουν από την ανάλυση αυτή. Σύμφωνα λοιπόν με τον ορισμό της στάθμης, αν θεωρήσουμε την συνάρτηση φ έτσι ώστε $\varphi(\alpha) = N(\alpha)$ για κάθε $\alpha \in \mathbb{Z}[i]$ και $\alpha \neq 0$, τότε η $\varphi: \mathbb{Z}[i]\setminus\{0\} \to \mathbb{N}^*$, οπότε έχουμε μια απεικόνιση ικανή να μας βοηθήσει να δείξουμε ότι το $\mathbb{Z}[i]$ είναι Ευκλείδεια Περιοχή.

Θεώρημα 1.6: Το σύνολο $\mathbb{Z}[i]$ είναι Ευκλείδεια Περιοχή με Ευκλείδεια συνάρτηση την φ.

Απόδειξη: Για τα μη μηδενικά $\alpha, \beta \in \mathbb{Z}[i]$ ισχύει:

$$\varphi(\alpha) = N(\alpha) \geq 1 \text{ και } \varphi(\beta) = N(\beta) \geq 1. \text{ Άρα:}$$

$$\varphi(\alpha) \leq \varphi(\alpha)\varphi(\beta) = N(\alpha)N(\beta) = N(\alpha\beta) = \varphi(\alpha\beta).$$

Επομένως έχει αποδειχθεί η πρώτη προϋπόθεση του ορισμού 1.7.

Τώρα θα πρέπει να αποδείξουμε τον **αλγόριθμο της διαίρεσης στο $\mathbb{Z}[i]$**:

«Για δύο ακεραίους Gauss α, β, με $\beta \neq 0$ υπάρχουν $\kappa, \upsilon \in \mathbb{Z}[i]$, τέτοιοι ώστε:

$$\alpha = \kappa\beta + \upsilon \text{ και } \varphi(\upsilon) = N(\upsilon) < \varphi(\beta) = N(\beta)».$$

Θεωρούμε ότι $\frac{\alpha}{\beta} = \lambda_1 + \lambda_2 i \in \mathbb{C}$, προφανώς $\lambda_1, \lambda_2 \in \mathbb{Q}$. Έστω ότι οι $\kappa_1, \kappa_2 \in \mathbb{Z}$ είναι οι πλησιέστεροι ακέραιοι στους ρητούς αριθμούς λ_1 και λ_2 αντίστοιχα. Αν δεχθούμε ως $\kappa = \kappa_1 + \kappa_2 i$ τότε $\kappa \in \mathbb{Z}[i]$ και υπάρχει αριθμός $\upsilon = \alpha - \kappa\beta$ ο οποίος είναι ακέραιος Gauss. Αρκεί να δείξουμε: $\varphi(\upsilon) = N(\upsilon) < \varphi(\beta) = N(\beta)$.

Επειδή $\frac{\upsilon}{\beta} = \frac{\alpha}{\beta} - \kappa$ τότε έχουμε:

$$N(\frac{\upsilon}{\beta}) = N(\frac{\alpha}{\beta} - \kappa) = N(\lambda_1 - \kappa_1 + \lambda_2 i - \kappa_2 i) =$$

$$(\lambda_1 - \kappa_1)^2 + (\lambda_2 - \kappa_2)^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 \leq \frac{1}{2} < 1.$$

Δηλαδή $N(\upsilon) < N(\beta)$. ♦

Σύμφωνα λοιπόν με το θεώρημα που μόλις αποδείχθηκε, αρχικά συμπεραίνουμε ότι:

«Κάθε ακέραιος Gauss παραγοντοποιείται κατά
μοναδικό τρόπο σε γινόμενο πρώτων Gauss».

Αυτή η πρόταση αποτελεί το **θεώρημα μοναδικής παραγοντοποίησης σε πρώτους του Gauss** (unique prime factorization theorem). Βέβαια πρέπει να εστιάσουμε στο γεγονός ότι έχουμε αποβάλλει από την παραγοντοποίηση τους αντιστρέψιμους. Αυτό είναι απαραίτητο μια και οι πρώτοι παράγοντες μεταβάλλονται σε ισοδύναμους από τον πολλαπλασιασμό τους με τους αντιστρέψιμους, οπότε το αποτέλεσμα απλώς θα εμφανιζόταν ως διαφορετικό, χωρίς όμως στην ουσία να είναι. Για παράδειγμα:

$$3 - i = (1 - 2i)(1 + i) = -i(2 + i)(1 + i).$$

Ένα δεύτερο συμπέρασμα που προκύπτει είναι ότι οι μοναδικοί αντιστρέψιμοι ακέραιοι στο $\mathbb{Z}[i]$ είναι αυτοί που ήδη έχουμε δει. Αυτό είναι άμεσα προερχόμενο από το θεώρημα 1.4, αφού μόνο αυτοί έχουν στάθμη ίση με 1.

Επίσης με τον αλγόριθμο της διαίρεσης στο $\mathbb{Z}[i]$ είδαμε πως μπορούμε να εκφράσουμε έναν ακέραιο Gauss με την βοήθεια ενός άλλου. Μπορούμε όμως να συμπεράνουμε πότε ο δεύτερος δεν είναι παράγοντας του πρώτου;

Πόρισμα 1.1: Αν για τους μη μηδενικούς ακέραιους Gauss $\alpha, \beta, \kappa, \upsilon$ ισχύει ότι: $\alpha = \beta\kappa + \upsilon$ και $0 < N(\upsilon) < N(\beta)$ τότε ο β δεν είναι παράγοντας του α.

Απόδειξη: Αν ο β είναι παράγοντας του α, τότε θα υπάρχει $\lambda \in \mathbb{Z}[i]$ ώστε $\alpha = \lambda\beta$. Επομένως θα έχουμε:

$$\lambda\beta = \kappa\beta + \upsilon \text{ ή } (\lambda - \kappa)\beta = \upsilon.$$

Από πολλαπλασιαστική ιδιότητα της στάθμης ισχύει ότι:

$$N(\kappa - \lambda)N(\beta) = N(\upsilon) < N(\beta)$$

$$\text{ή } N(\kappa - \lambda) < 1, \text{ άτοπο.}$$

Επομένως ο β δεν είναι παράγοντας του α. ♦

Όμως χάριν του θεωρήματος 1.6 έχουμε και την ύπαρξη – εύρεση του μ.κ.δ. δύο ακεραίων Gauss. Και στο σύνολο αυτό ακολουθούμε παρόμοια πορεία, διαδοχικών διαιρέσεων, όπως στους πραγματικούς ακέραιους (Ευκλείδειος αλγόριθμος). Σύμφωνα λοιπόν με τον αλγόριθμο της διαίρεσης στο $\mathbb{Z}[i]$ οι διαδοχικές διαιρέσεις που θα προκύψουν, αν ξεκινούσαμε με δύο συγκεκριμένους ακεραίους Gauss, θα έδιναν υπόλοιπα με γνήσια φθίνουσα τιμή της στάθμης τους. Οπότε μετά από κάποιες επαναλήψεις η διαδικασία αυτή θα τελείωνε, μια και οι στάθμες των υπολοίπων είναι φυσικός αριθμός. Έτσι σύμφωνα με το θεώρημα 1.5 θα είχαμε υπολογίσει τον μ.κ.δ. των δύο αρχικών ακεραίων. Αυτός όπως έχουμε δείξει θα είναι το τελευταίο μη μηδενικό υπόλοιπο.

Πόρισμα 1.2: Μέγιστος Κοινός Διαιρέτης (μ.κ.δ.) δύο μη μηδενικών στοιχείων του $\mathbb{Z}[i]$ είναι ο κοινός τους διαιρέτης με την μεγαλύτερη στάθμη που προκύπτει από τον Ευκλείδειο αλγόριθμο. Κάθε άλλος κοινός διαιρέτης με την ίδια στάθμη είναι πολλαπλάσιος του μ.κ.δ με κάποιον αντιστρέψιμο.

Απόδειξη: Έστω οι μη μηδενικοί $\zeta, \xi \in \mathbb{Z}[i]$ και $\mu.\kappa.\delta(\zeta, \xi) = \delta$ και δ' ένας άλλος κοινός διαιρέτης των ζ και ξ με $N(\delta') = N(\delta)$. Από τον ορισμό του μ.κ.δ. έχουμε δ'/δ άρα $\delta = \delta' \cdot \kappa$, με $\kappa \in \mathbb{Z}[i]$, τότε:

$$N(\delta) = N(\delta')N(\kappa) \Leftrightarrow N(\kappa) = 1.$$

Επομένως ο κ είναι αντιστρέψιμος. ♦

Βάση λοιπόν των παραπάνω συμπεραίνουμε ότι και για τους ακέραιους Gauss ισχύει το αντίστοιχο του θεωρήματος του Bezout στους πραγματικούς ακέραιους. Δηλαδή αν για τους μη μηδενικούς $\zeta, \xi \in \mathbb{Z}[i]$, ο $\mu.\kappa.\delta.(\zeta, \xi) = \delta$, τότε μπορούμε να υπολογίσουμε $\lambda, \mu \in \mathbb{Z}[i]$ ώστε να ισχύει: $\delta = \lambda\zeta + \mu\xi$.

Κλείνοντας την συγκεκριμένη ενότητα θα επισημάνουμε ότι τα σύνολα στα οποία ισχύει η μοναδική παραγοντοποίηση αποτελούσαν για πολλά χρόνια πεδίο έρευνας των Μαθηματικών. Παρότι η ιδιότητα αυτή, για το σύνολο των φυσικών αριθμών, ήταν γνωστή ήδη από τους Αρχαίους Έλληνες. Είναι άλλωστε γνωστό ότι στην Πρόταση IX. 14 των Στοιχείων, ο Ευκλείδης αποδείκνυε ότι:

> «*Εάν ελάχιστος αριθμός υπό πρώτων αριθμών μετρήται, υπ' ουδενός άλλου πρώτου αριθμού μετρηθήσεται παρέξ των εξ αρχής μετρούντων*».

Η μοναδικά περατή διαδικασία παραγοντικής ανάλυσης ενός αριθμού δεν είναι αυτονόητη όμως και σε άλλα σύνολα. Ο Euler στην απόδειξή που έδωσε σχετικά με το τελευταίο θεώρημα του Fermat για την περίπτωση που το $n = 3$ χρησιμοποίησε την μοναδικότητα παραγοντοποίησης σε κάποιο σύνολο αριθμών, δίχως όμως να της δώσει την απαιτούμενη προσοχή. Επίσης ο Gabriel Lame στην απόδειξη που παρουσίασε το 1847 στην Ακαδημία του Παρισιού πάνω στο ίδιο θεώρημα υπέθεσε ότι κάποια σύνολα μιγαδικών ήταν εφοδιασμένα με την ιδιότητα αυτή, αλλά χωρίς δυστυχώς να ισχύει κάτι τέτοιο. Αυτό το μοιραίο λάθος επισήμανε τότε ο Joseph Liouville και η απόδειξή του απορρίφθηκε. Υπάρχουν ιστορικοί που αποδίδουν το συγκεκριμένο λάθος και στην περίφημη «απόδειξη» του θεωρήματος αυτού από τον ίδιο τον Fermat.

Αυτοί όμως που συνέβαλαν σημαντικά προς την κατεύθυνση θεμελίωσης των συνόλων μοναδικής παραγοντοποίησης ήταν ο Ernst Kummer (1810 – 1893) μια και εισήγαγε για πρώτη φορά την θεωρία των «κυρίων ιδεωδών». Ακολούθησαν οι Richard Dedeckind (1831 – 1916) και Emanuel Lasker (1868 – 1941) οι οποίοι τα όρισαν με τον σημερινό αποδεικτικό τους τρόπο. Αργότερα η Emmy Noether (1882 – 1935) ενοποίησε όλες αυτές τις έννοιες, θέτοντας τις βάσεις της αντιμεταθετικής Άλγεβρας.

Πάντως χάριν της πληρότητας της παρουσίασης μας σχετικά με την μοναδικότητα ανάλυσης σε γινόμενο παραγόντων, οφείλουμε να αναφέρουμε ένα παράδειγμα ακέραιας περιοχής η οποία να μην αποτελεί περιοχή

μοναδικής παραγοντοποίησης. Το χαρακτηριστικότερο δείγμα μιας τέτοιας περιοχής είναι ο γνωστός ως **δακτύλιος του Dedekind**, δηλαδή το σύνολο:

$$\mathbb{Z}[\sqrt{-5}] = \{\alpha + \beta\sqrt{-5} \,/\, \alpha, \beta \in \mathbb{Z}\}.$$

Ορίζουμε ως συνάρτηση την $\varphi: \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}^*$ όπου $\varphi(\alpha + \beta\sqrt{-5}) = \alpha^2 + 5\beta^2$.

Προφανώς ισχύει ότι $\varphi(x\cdot y) = \varphi(x)\cdot\varphi(y)$ για κάθε $x, y \in \mathbb{Z}[\sqrt{-5}]$. Ας υποθέσουμε τώρα ότι το $e \in \mathbb{Z}[\sqrt{-5}]$ είναι αντιστρέψιμο, τότε από την σχέση $e\cdot e' = 1$ έχουμε $\varphi(e\cdot e') = \varphi(e)\cdot\varphi(e') = \varphi(1) = 1$ και επειδή $\varphi(e)\cdot\varphi(e') \in \mathbb{N}^*$ τότε $\varphi(e) = 1$. Έστω $e = u + v\sqrt{-5}$, με $u, v \in \mathbb{Z}$ οπότε ισχύει ότι $u^2 + 5v^2 = 1$. Οι μοναδικές λύσεις της Διοφαντικής είναι $(u, v) = (\pm 1, 0)$. Άρα τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι τα 1 και -1.

Είναι επίσης φανερό ότι στον $\mathbb{Z}[\sqrt{-5}]$ ισχύει ότι:

$$6 = 2\cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Τα στοιχεία $\{2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}\}$ φυσικά δεν είναι αντιστρέψιμα και ούτε ισοδύναμα ανά δύο. Όπως τώρα θα δείξουμε κάθε ένα από αυτά, είναι ανάγωγο. Για $x, y \in \mathbb{Z}[\sqrt{-5}]$ αν ισχύει $2 = x\cdot y$ τότε $\varphi(2) = \varphi(x\cdot y)$ ή $4 = \varphi(x)\cdot\varphi(y)$. Αφού όμως $\varphi(x), \varphi(y) \in \mathbb{N}^*$ τότε $\varphi(x) = 1$ ή 2 ή 4. Η περίπτωση $\varphi(x) = 1$ απορρίπτεται γιατί τότε $x = \pm 1$, όπως επίσης και η περίπτωση $\varphi(x) = 4$ απορρίπτεται γιατί δίνει καταλήγει σε $y = \pm 1$. Άρα απομένει μόνο το $\varphi(x) = 2$, αν τώρα $x = u + v\sqrt{-5}$, με $u, v \in \mathbb{Z}$ τότε ισχύει ότι $u^2 + 5v^2 = 2$. Η εξίσωση που προέκυψε όμως είναι αδύνατη, οπότε το 2 είναι ανάγωγο. Με παρόμοιο τρόπο δείχνουμε ότι και τα υπόλοιπα στοιχεία είναι ανάγωγα στο $\mathbb{Z}[\sqrt{-5}]$.

Σε αντίθεση όμως με το προηγούμενο σύνολο, στο $\mathbb{Z}[\sqrt{-2}] = \{\alpha + \beta\sqrt{-2} \,/\, \alpha, \beta \in \mathbb{Z}\}$ αποδεικνύεται ότι ισχύει η μοναδική ανάλυση. Μια διαφορετική προσέγγιση των συνόλων αυτών, αλλά με σκοπό την ιδιότητα της μοναδικής παραγοντοποίησης, θα γίνει και στο επόμενο κεφάλαιο.

1.5 Προσδιορισμός των Πρώτων Gauss

Έχοντας την εμπειρία από την έλξη που έχουν προκαλέσει οι πρώτοι πραγματικοί αριθμοί στις Μαθηματικές κοινότητες όλων των εποχών μπορούμε να κατανοήσουμε την δυναμική που παρουσιάζουν και οι πρώτοι του συνόλου $\mathbb{Z}[i]$. Ήδη αναφερθήκαμε σε κάποιες αρχικές έννοιες που τους αφορούν όπως, ότι οι αντιστρέψιμοι δεν θεωρούνται πρώτοι και ότι για κάθε $\zeta \in \mathbb{Z}[i]$ με $N(\zeta)$ πραγματικό πρώτο, τότε ο ζ είναι πρώτος Gauss. Επίσης έχουμε επισημάνει ότι κάποιοι πραγματικοί πρώτοι σταματούν να είναι πρώτοι στο $\mathbb{Z}[i]$. Οπότε αρχικά είναι αυτονόητη η απορία μας που σχετίζεται με το πλήθος αυτών των αριθμών μέσα στο σύνολο.

Θεώρημα 1.7: Υπάρχουν άπειροι πρώτοι ακέραιοι Gauss.

Απόδειξη: Ας υποθέσουμε ότι οι πρώτοι Gauss είναι πεπερασμένου πλήθους, δηλαδή μπορούμε να θεωρήσουμε τους: $g_1, g_2, \ldots, g_n$. Η ύπαρξη τουλάχιστον ενός από αυτούς, που μας είναι απαραίτητη, καλύπτεται από τον $1 + i$ ο οποίος είναι πρώτος Gauss, αφού $N(1 + i) = 2$, οπότε αν ο $1 + i$ είχε παράγοντα τότε η στάθμη του θα έπρεπε να διαιρεί τον πρώτο ακέραιο 2, πράγμα αδύνατο.

Τότε ο αριθμός $G = g_1 \cdot g_2 \cdot \ldots \cdot g_n + 1$ θα είναι επίσης ακέραιος Gauss, φυσικά διάφορος από κάθε έναν από τους g_i με $i = 1, 2, \ldots, n$. Επίσης δεν θα έχει παράγοντα κανέναν από τους g_i. Το τελευταίο ισχύει από την Πόρισμα 1.1 επειδή $G = g_i \cdot k + 1$, όπου k είναι το γινόμενο των αρχικών πρώτων και $N(g_i) > N(1) = 1$. Συνεπώς θα είναι και αυτός πρώτος Gauss. ♦

Η απόδειξη που παρουσιάσαμε στο θεώρημα 1.7 είναι αντίστοιχη της απόδειξης του Ευκλείδη στην πρόταση IX. 20, η οποία αναφέρει ότι:

«*Οι πρώτοι αριθμοί πλείους εισί του προτεθέντος πλήθους πρώτων αριθμών*».

Μια απόδειξη προ είκοσι δύο και πλέον αιώνων που αποτελεί υπόδειγμα κομψότητας και αρτιότητας.

Ένα ακόμη σημαντικό θεώρημα που σχετίζεται με τους πρώτους είναι και η **ιδιότητα των πρώτων διαιρετών του Gauss** (Gaussian prime divisor property).

Θεώρημα 1.8: Αν ένας πρώτος Gauss διαιρεί ένα γινόμενο ακεραίων αριθμών Gauss τότε θα διαιρεί και έναν τουλάχιστον από τους παράγοντες του γινομένου.

Απόδειξη: Υποθέτουμε ότι $\alpha, \beta, g \in \mathbb{Z}[i]$ με g να είναι πρώτος, ώστε: $g/\alpha\beta \Leftrightarrow \alpha\beta = \kappa g$, $\kappa \in \mathbb{Z}[i]$ και g δεν διαιρεί τον α. Υπάρχουν τότε $\lambda, \mu \in \mathbb{Z}[i]$ ώστε: $1 = \lambda\alpha + \mu g$. Πολλαπλασιάζοντας την ισότητα με τον β έχουμε:

$$\beta = \lambda\alpha\beta + \mu g\beta = \lambda\kappa g + \mu g\beta = g(\lambda\kappa + \mu\beta).$$

Όμως ο αριθμός $\lambda\kappa + \mu\beta \in \mathbb{Z}[i]$, επομένως g/β.

Με επαγωγή μπορούμε να δείξουμε ότι ισχύει και για περισσότερους των δύο παραγόντων. ♦

Τώρα είμαστε στην θέση να ταξινομήσουμε τους πρώτους Gauss, μια κατηγοριοποίηση η οποία κάθε άλλο παρά εύκολη εμφανίζεται. Φυσικά ένα μέρος του προβλήματος μας θα είναι να ελέγξουμε και ποιοι πραγματικοί πρώτοι είναι επίσης πρώτοι Gauss. Αρχικά όμως θα πρέπει να αποδείξουμε μια σειρά προτάσεων της θεωρίας αριθμών, που θα μας βοηθήσουν στην απόδειξη του βασικού μας θεωρήματος ταξινόμησης τους.

Λήμμα 1.1: Αν δύο οποιοιδήποτε πραγματικοί ακέραιοι του συνόλου $A = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ διαιρούμενοι με τον ακέραιο m δίνουν διαφορετικό υπόλοιπο, τότε το ίδιο θα συμβαίνει και για κάθε ζευγάρι ακέραιων του συνόλου $B = \{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_m\}$, με την προϋπόθεση ότι μ.κ.δ.$(\alpha, m) = 1$.

Απόδειξη: Οι διαιρέσεις δύο ακεραίων $\alpha_i, \alpha_j \in A$ θα δίνουν προφανώς κάποια διαφορετικά υπόλοιπα $\upsilon_1, \upsilon_2 \in \{0, 1, 2, \ldots, m-1\}$. Αν θεωρήσουμε ότι οι διαιρέσεις των $\alpha\alpha_i, \alpha\alpha_j \in B$ δια m δίνουν το ίδιο υπόλοιπο, τότε ισχύει $m/(\alpha\alpha_i - \alpha\alpha_j) \Leftrightarrow m/\alpha(\alpha_i - \alpha_j)$. Επειδή όμως μ.κ.δ.$(\alpha, m) = 1$, τότε $m/(\alpha_i - \alpha_j)$, δηλαδή $\upsilon_1 = \upsilon_2$, άτοπο. ♦

Θεώρημα 1.9: (**Wilson**). Αν ο p είναι πρώτος τότε $p/[(p-1)! + 1]$.

Απόδειξη: Στην περίπτωση που $p = 2$ ή $p = 3$ το συμπέρασμα είναι προφανές, επομένως θα αποδείξουμε για $p > 3$. Θεωρούμε το σύνολο $A = \{1, 2, \ldots, p-1\}$ και έναν ακέραιο $\alpha \in A$, οπότε μ.κ.δ.$(\alpha, p) = 1$. Από Λήμμα 1.1

για κάθε $\beta, \gamma \in A$ με $\beta \neq \gamma$ οι $\alpha\beta, \alpha\gamma$ διαιρούμενοι με τον p θα δίνουν διαφορετικό υπόλοιπο μέσα στο A. Συνεπώς η εξίσωση $p/(\alpha x - 1)$ δέχεται μοναδική λύση ως προς x στο σύνολο A. Για την περίπτωση που $x = \alpha$ θα έχουμε ότι:

$$p/(\alpha^2 - 1) \Leftrightarrow p/(\alpha - 1)(\alpha + 1) \Leftrightarrow p/(\alpha - 1) \text{ είτε } p/(\alpha + 1).$$

Αν ο p διαιρούσε και τα δύο τότε θα διαιρούσε και την διαφορά τους δηλαδή $p/2$, αδύνατο. Επειδή $\alpha \in A$ η παραπάνω σχέση δίνει $\alpha = 1$ είτε $\alpha = p - 1$.

Συμπεραίνουμε λοιπόν ότι τα υπόλοιπα στοιχεία $\{2, 3, \ldots, p-2\}$ μπορούν να χωριστούν σε ζεύγη που το γινόμενο των μελών κάθε ζεύγους διαιρούμενο με τον p να δίνει υπόλοιπο 1. Οπότε και το γινόμενο τους διαιρούμενο με τον p θα δίνει υπόλοιπο 1. Άρα υπάρχει $\kappa \in \mathbb{Z}$ ώστε:

$$(2\cdot 3\cdot 4\cdot \ldots \cdot p-2) - 1 = \kappa p \Leftrightarrow (p-1)! - p + 1 = \kappa p$$
$$\Leftrightarrow p/[(p-1)! + 1] \qquad \blacklozenge$$

Λήμμα 1.2: Αν για τους πρώτους αριθμούς $p \in \mathbb{Z}$ και $g \in \mathbb{Z}[i]$ ισχύει ότι g/p, τότε $N(g) = p$ είτε $N(g) = p^2$.

Απόδειξη: Αφού g/p θα ισχύει ότι $g = p\cdot f$, με $f \in \mathbb{Z}[i]$. Βάση της πολλαπλασιαστικής ιδιότητας της στάθμης έχουμε:

$$N(p) = N(g)N(f) \Rightarrow p^2 = N(g)N(f).$$

Αλλά επειδή ο p είναι πραγματικός πρώτος από την μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}$ θα έχουμε: $N(g) = p$ είτε $N(g) = p^2$.

Θεώρημα 1.10: (**δύο τετραγώνων του Fermat**). Κάθε φυσικός πρώτος της μορφής $p = 4n + 1$, μπορεί να γραφεί ως άθροισμα δύο τετραγώνων φυσικών αριθμών με μοναδικό τρόπο.

Απόδειξη: Χρησιμοποιώντας το θεώρημα 1.9 έχουμε ότι:

$$p/[(4n)! + 1] \Leftrightarrow p/[(2n)!\cdot(2n+1)\cdot \ldots \cdot(4n-1)\cdot 4n + 1].$$

Επειδή όμως τα ζεύγη των αριθμών $(m, m - p)$ δίνουν το ίδιο υπόλοιπο αν διαιρεθούν με τον p, τότε μπορούμε την παραπάνω σχέση να την γράψουμε:

$$p/[(2n)!\cdot(-2n)\cdot \ldots \cdot(-2)\cdot(-1) + 1] \Leftrightarrow p/\{[(2n)!]^2(-1)^{2n} + 1\} \Leftrightarrow$$
$$p/\{[(2n)!]^2 + 1\} \Leftrightarrow p/(k^2 + 1) \text{ με } k = (2n)!.$$

Όμως ο αριθμός $k^2 + 1 = (k + i)(k – i)$, χωρίς ο p να διαιρεί κανέναν από τους δύο παράγοντες αφού $(\frac{k}{p} \pm \frac{i}{p}) \notin \mathbb{Z}[i]$. Άρα ο p δεν είναι πρώτος Gauss.

Θεωρούμε ότι ο p έχει ως γνήσιο διαιρέτη τον πρώτο Gauss $g = \alpha + \beta i$, από το Λήμμα 1.2 θα είναι $N(g) = p$ είτε $N(g) = p^2$ και επειδή $N(g)$ είναι πραγματικός πρώτος τότε $N(g) = \alpha^2 + \beta^2 = p$.

Αντίστροφα αν $p = \alpha^2 + \beta^2$, με α, β φυσικοί ακέραιοι, βάση της μοναδικής παραγοντοποίησης του στο $\mathbb{Z}[i]$, αναλύεται ως $p = (\alpha + \beta i)(\alpha – \beta i)$, με κάθε παράγοντα του να είναι πρώτος Gauss αφού η στάθμη τους είναι πρώτος αριθμός. Συνεπώς οι φυσικοί ακέραιοι α, β θα είναι οι μοναδικοί που το άθροισμα των τετραγώνων τους να ισούται με τον p. ♦

Η πρώτη απόδειξη, του θεωρήματος που προηγήθηκε και θεωρείτε από τα ωραιότερα της Αριθμητικής, δόθηκε από τον Fermat με μια ιδιοφυή όσο και επίπονη μέθοδο που ονομάζεται «άπειρη κάθοδος». Ακολούθησε ο Euler το 1749 μετά από αγώνα επτά χρόνων το απέδειξε με αρκετά περίπλοκο τρόπο. Αργότερα το απέδειξαν ο Lagrange, ο Gauss και ο Dedekind.

Το σημαντικό αυτό θεώρημα καταδεικνύει ποιοι πραγματικοί πρώτοι γράφονται μοναδικά ως άθροισμα δύο τετραγώνων. Εκτός από αυτούς, ως γνωστών, πρώτοι είναι ο 2 και όσοι είναι της μορφής $4n + 3$. Άρα μπορούμε τώρα να παρουσιάσουμε το κεντρικό θεώρημα κατάταξης των πρώτων Gauss.

Θεώρημα 1.11: (**ταξινόμηση των πρώτων Gauss**). Οι πρώτοι ακέραιοι του Gauss χωρίζονται στις εξής κλάσεις:

- Οι φυσικοί πρώτοι της μορφής $4n + 3$, και οι ισοδύναμοί τους στο $\mathbb{Z}[i]$.
- Ο ακέραιος $1 + i$ και οι ισοδύναμοί του $1 – i, -1 + i, -1 – i$.
- Οι ακέραιοι και οι ισοδύναμοί τους $\alpha + \beta i, \alpha – \beta i$, $\alpha, \beta \in \mathbb{Z}$ αν ο $\alpha^2 + \beta^2$ είναι φυσικός πρώτος της μορφής $4n + 1$.

Απόδειξη: Αρχικά πρέπει να τονίσουμε το προφανές ότι δεν υπάρχουν άλλοι πραγματικοί πρώτοι, εκτός των κατηγοριών που έχουμε να εξετάσουμε. Επίσης θα δείξουμε ότι κάθε πρώτος Gauss g διαιρεί πάντα έναν μοναδικό πραγματικό πρώτο. Αυτό ισχύει γιατί $g \cdot \bar{g} = N(g) \Rightarrow g/N(g)$, με $N(g)$

πραγματικό πρώτο. Αν τώρα g/p και g/q, όπου p, q πραγματικοί πρώτοι και επειδή υπάρχουν $κ, λ \in \mathbb{Z}$ ώστε: $κp + λq = 1$ το $g/1$, αδύνατο. Επομένως όλοι οι πρώτοι Gauss καλύπτονται από τις προαναφερθείσες τάξεις.

- Αν θεωρήσουμε ότι ένας πρώτος Gauss $g = x = yi$ διαιρεί τον πραγματικό πρώτο $p = 4n + 3$, τότε από Λήμμα 1.2 έχουμε ότι $N(g) = p$ ή $N(g) = p^2$. Ας δεχθούμε ότι $N(g) = p \Leftrightarrow x^2 + y^2 = 4n + 3$, οπότε ένας από τους x, y θα είναι περιττός και ένας άρτιος, έστω $x = 2α$ και $y = 2β + 1$, $α, β \in \mathbb{N}$, τότε:

  $$4n + 3 = 4α^2 + (2β + 1)^2 = 4(α^2 + β^2 + β) + 1 = 4m + 1, \text{ άτοπο.}$$

  Οπότε $N(g) = p^2 = N(p)$ και επειδή g/p τότε $p = g \cdot f$, $f \in \mathbb{Z}[i]$. Επομένως και $N(p) = N(g)N(f) \Rightarrow N(f) = 1$, δηλαδή ο f είναι μοναδιαίος ανάγωγος πράγμα που σημαίνει ότι ο $g = p$ η ο g ισοδύναμος του p.
- Ο μόνος πραγματικός πρώτος που είναι άρτιος είναι ο 2. Αλλά ισχύει ότι: $2 = (1 + i)(1 – i)$, με $N(1 + i) = N(1 – i) = 2$. Οπότε αφού η στάθμη τους είναι πρώτος ακέραιος, τότε αυτοί και οι ισοδύναμοί τους $-1 + i$ και $-1 – i$ θα είναι πρώτοι Gauss.
- Από το θεώρημα 1.10 έχουμε συμπεράνει ότι οι πραγματικοί ακέραιοι της μορφής $4n + 1$ δεν είναι πρώτοι Gauss, αφού μπορούν να γραφούν με τον τρόπο $p = α^2 + β^2$. Όμως οι παράγοντες τους $α + βi$ και $α – βi$, είναι πρώτοι Gauss. Προφανώς το ίδιο θα συμβαίνει και για τους ισοδύναμους τους αφού είναι ακέραιοι Gauss της ίδιας κατηγορίας. ♦

Για να ολοκληρώσουμε τα συμπεράσματα που συνάγονται από το θεώρημα, πρέπει να σημειώσουμε ότι αν ο πρώτος Gauss $α + βi$ περιέχεται σε οποιαδήποτε από τις προηγούμενες κλάσεις, τότε ο συζυγής του $α – βi$ θα είναι και αυτός πάντα πρώτος. Επομένως και οι ισοδύναμοι παράγοντες του συζυγή θα είναι πρώτοι Gauss, δηλαδή και ο $β + αi$ αφού $(α - βi) \cdot i = β + αi$.

Στο τέλος της εργασίας σε ειδικούς πίνακες γίνεται παρουσίαση όλων των πρώτων Gauss με στάθμη μικρότερη ή ίση του 1000. Όπως επίσης και η γραφική παράστασή τους στο μιγαδικό επίπεδο. Ακόμη υπάρχει πίνακας που περιέχει όλους τους ακέραιους Gauss με στάθμη μικρότερη ίση του 200 και την μοναδική τους ανάλυση σε γινόμενο πρώτων παραγόντων.

1.6 Σχετικά Πρώτοι Ακέραιοι Gauss.

Ορισμός 1.9: Δύο ακέραιοι Gauss που έχουν ως μ.κ.δ. αντιστρέψιμο, ονομάζονται **σχετικά πρώτοι.**

Στην περίπτωση που δύο ακέραιοι Gauss έχουν στάθμες σχετικά πρώτους πραγματικούς ακέραιους, τότε είναι οι ίδιοι σχετικά πρώτοι στο $\mathbb{Z}[i]$. Αυτό είναι φανερό γιατί αν είχαν έναν κοινό διαιρέτη μη αντιστρέψιμο, τότε η στάθμη αυτού θα έπρεπε να διαιρεί τις στάθμες των δύο αρχικών ακεραίων Gauss. Πράγμα άτοπο, αφού όπως είπαμε αυτές οι δύο είναι σχετικά πρώτοι πραγματικοί ακέραιοι. Το αντίστροφο όμως δεν ισχύει. Για παράδειγμα ας επιλέξουμε τους αριθμούς $1 + 2i$, $1 + 3i$ οι οποίοι είναι σχετικά πρώτοι, όμως οι στάθμες τους που είναι 5, 10 αντίστοιχα δεν είναι σχετικά πρώτοι πραγματικοί ακέραιοι.

Θεώρημα 1.12: Δύο ακέραιοι Gauss α, β είναι σχετικά πρώτοι αν και μόνο αν ισχύει $\alpha\kappa + \beta\lambda = 1$, για $\kappa, \lambda \in \mathbb{Z}[i]$.

Απόδειξη: Αν οι α, β είναι σχετικά πρώτοι τότε από την επέκταση του θεωρήματος του Bezout στους ακέραιους Gauss υπάρχουν οι $\kappa, \lambda \in \mathbb{Z}[i]$ ώστε $\alpha\kappa + \beta\lambda = 1$. Αντίστροφα αν ισχύει $\alpha\kappa + \lambda\beta = 1$ τότε κάθε κοινός διαιρέτης των α, β θα διαιρεί το 1, οι διαιρέτες του 1 όμως είναι μόνο οι αντιστρέψιμοι. Όποτε μόνο αυτοί θα διαιρούν και τα α, β. Δηλαδή οι α, β είναι σχετικά πρώτοι. ♦

Πόρισμα 1.3. Αν α, β, γ είναι ακέραιοι Gauss με $\alpha/\beta\gamma$ και α, β είναι σχετικά πρώτοι τότε α/γ.

Απόδειξη: Αφού $\alpha/\beta\gamma$ τότε υπάρχει $x \in \mathbb{Z}[i]$ ώστε $\beta\gamma = \alpha x$. Επίσης από θεώρημα 1.12 ισχύει ότι $\alpha\kappa + \beta\lambda = 1$, για $\kappa, \lambda \in \mathbb{Z}[i]$. Πολλαπλασιάζοντας την τελευταία σχέση με γ είναι:

$$\gamma = \gamma\alpha\kappa + \gamma\beta\lambda = \alpha\gamma\kappa + \alpha x\lambda = \alpha(\gamma\kappa + x\lambda).$$

Επειδή $\gamma\kappa + x\lambda \in \mathbb{Z}[i]$ τότε α/γ. ♦

Πόρισμα 1.4. Αν α, β, γ είναι ακέραιοι Gauss με α/γ, β/γ και α, β είναι σχετικά πρώτοι τότε $\alpha\beta/\gamma$.

Απόδειξη: Υπάρχουν $x, y \in \mathbb{Z}[i]$ ώστε $\gamma = \alpha x$ και $\gamma = \beta y$. Επίσης από θεώρημα 1.12 ισχύει ότι $\alpha\kappa + \beta\lambda = 1$, για $\kappa, \lambda \in \mathbb{Z}[i]$. Πολλαπλασιάζοντας την τελευταία σχέση με γ είναι:

$$\gamma = \gamma\alpha\kappa + \gamma\beta\lambda = \beta y\alpha\kappa + \alpha x\beta\lambda = \alpha\beta(y\kappa + x\lambda).$$

Αφού $y\kappa + x\lambda \in \mathbb{Z}[i]$ τότε $\alpha\beta/\gamma$. ♦

Πόρισμα 1.5. Αν α, β, γ είναι ακέραιοι Gauss τότε οι $\alpha\beta$ και γ είναι σχετικά πρώτοι αν και μόνο αν ο καθένας από τους α, β είναι σχετικά πρώτος με τον γ.

Απόδειξη: Υπάρχουν λοιπόν $\kappa, \lambda \in \mathbb{Z}[i]$ ώστε $\alpha\beta\kappa + \gamma\lambda = 1$. Η σχέση ισοδύναμα γράφεται $\alpha(\beta\kappa) + \gamma\lambda = 1$ και $\beta(\alpha\kappa) + \gamma\lambda = 1$. Αφού $\beta\kappa, \alpha\kappa \in \mathbb{Z}[i]$, από θεώρημα 1.12 καθένα από τα α, β είναι σχετικά πρώτος με τον γ. ♦

Αν πάρουμε τώρα την περίπτωση που έχουμε δύο σχετικά πρώτους ακεραίους Gauss και το γινόμενο τους είναι τέλειο τετράγωνο, μπορούμε να συμπεράνουμε ότι ο καθένας από αυτούς είναι τέλειο τετράγωνο; Βέβαια δεν πρέπει να ξεχνάμε ότι στο σύνολο $\mathbb{Z}$ κάτι τέτοιο δεν ισχύει πάντα, όπως για παράδειγμα το $36 = (-4)(-9)$, που φυσικά οι -4 και -9 δεν είναι τέλεια τετράγωνα. Στο $\mathbb{Z}[i]$ υπάρχουν αντιστρέψιμοι που είναι τέλεια τετράγωνα όπως οι $1 = 1^2 = (-1)^2$ και $-1 = i^2 = (-i)^2$, οι οποίοι προφανώς μπορούν να εκφραστούν μέσα σε κάθε τετραγωνικό παράγοντα, αλλά υπάρχουν επίσης και οι $i, -i$ που δεν γράφονται ως τετράγωνα. Οπότε οι σχετικά πρώτοι ακέραιοι Gauss των οποίων το γινόμενο είναι τέλειο τετράγωνο ο καθένας θα είναι τέλειο τετράγωνο ή θα είναι ένα γινόμενο τέλειων τετραγώνων επί i.

Κάτι αντίστοιχο όμως δεν μπορούμε να πούμε ότι συμβαίνει και στην περίπτωση που το γινόμενό τους είναι κύβος. Οι αντιστρέψιμοι είναι όλοι κύβοι αφού ισχύουν:

$$1 = 1^3, -1 = (-1)^3, i = (-i)^3, -i = i^3.$$

Οπότε αυτοί μπορούν να ενσωματωθούν μέσα σε έναν κύβο. Συνεπώς αν το γινόμενο δύο σχετικά πρώτων ακέραιων Gauss είναι ένας κύβος τότε κάθε ένας από αυτούς θα είναι κύβος.

Όσον αφορά το πλήθος των σχετικά πρώτων ακεραίων Gauss, έχει υπολογισθεί ότι η πιθανότητα στην τυχαία επιλογή δύο στοιχείων του συνόλου α, β να είναι μεταξύ τους πρώτοι είναι:

$$P = \frac{6}{\pi^2 G} = 0{,}6637\ldots$$

Στον τύπο με G συμβολίζεται η σταθερά Catalan. Έχει πάρει το όνομα της από τον Μαθηματικό Eugene Charles Catalan (1814 – 1894) και συνήθως εμφανίζεται σε εκτιμήσεις συναρτήσεων συνδυαστικής, ή σε ορισμένα ολοκληρώματα. Η σταθερά αυτή είναι ίση με:

$$G = \beta(2) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^2} = 0{,}9159\ldots,$$

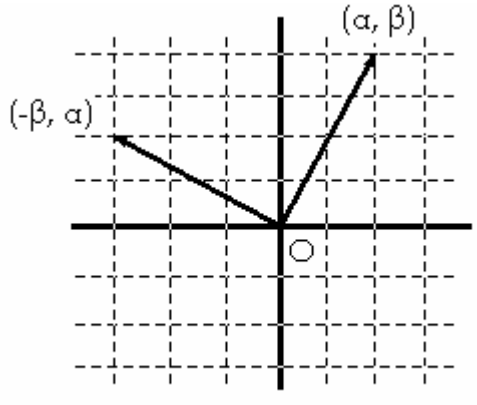
όπου $\beta(2)$ είναι η τιμή της βήτα συνάρτησης του Dirichlet $\beta(s) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s}$.

1.7 Ισοϋπόλοιποι στο $\mathbb{Z}[i]$

Ας επανέλθουμε τώρα στον πολλαπλασιασμό μεταξύ δύο ακεραίων Gauss, αλλά εστιάζοντας τον από μια διαφορετική οπτική γωνία. Έναν εναλλακτικό τρόπο παρουσίασης του, ο οποίος θα βοηθήσει αρχικά ώστε να έχουμε την δυνατότητα και μιας απεικόνισης του στο επίπεδο. Για τα στοιχεία $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ ισχύει ότι:

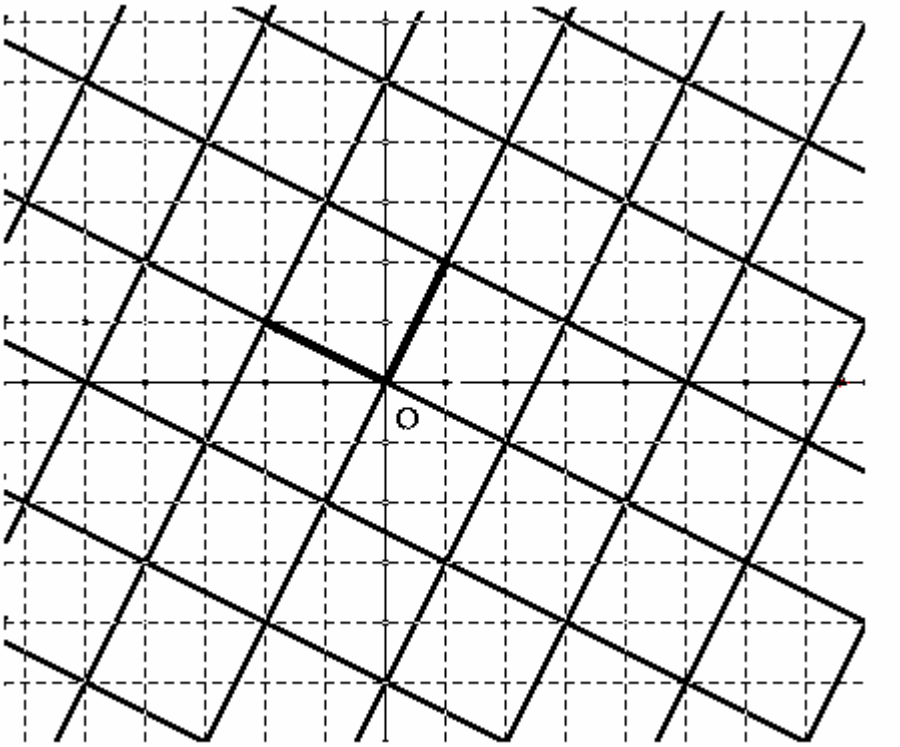
$$(\alpha + \beta i)(\gamma + \delta i) = (\alpha + \beta i)\gamma + (\alpha + \beta i)\delta i = \gamma(\alpha + \beta i) + \delta(-\beta + \alpha i).$$

Παρατηρούμε λοιπόν ότι το γινόμενο των δύο παραπάνω μιγαδικών γράφεται ως ακέραιος γραμμικός συνδυασμός των $\alpha + \beta i$ και $-\beta + \alpha i$.



Σχήμα 1.1

Η γραφική απεικόνιση αυτών των δύο αριθμών στο $\mathbb{R}^2$ απεικονίζεται στο σχήμα 1.1 με την βοήθεια των διανυσμάτων (α, β) και $(-\beta, \alpha)$. Ο πολλαπλασιασμός τους λοιπόν ως ακέραιος γραμμικός συνδυασμός των διανυσμάτων του σχήματος 1.1, διαμορφώνει στο επίπεδο ένα διχτυωτό πλέγμα τετραγώνων, όπως στο σχήμα 1.2. Κάθε κορυφή των τετραγώνων αυτών αντιστοιχεί σε ένα πολλαπλάσιο του $\alpha + \beta i$.

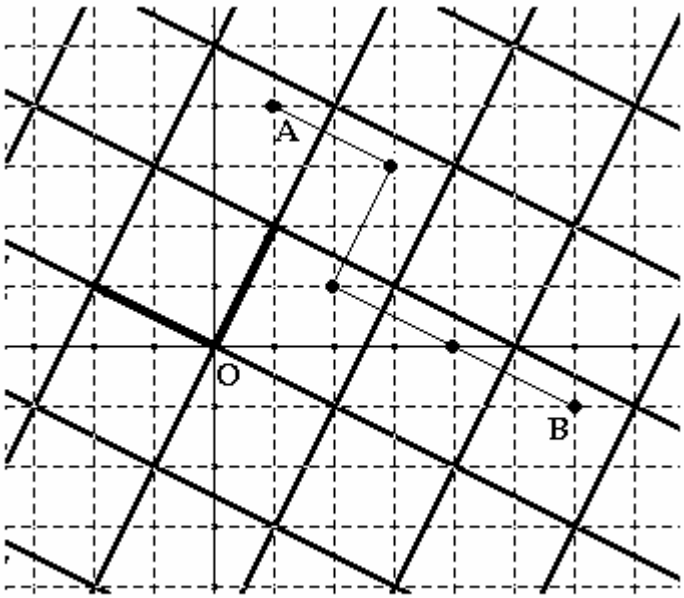


Σχήμα 1.2

Αν ξεκινήσουμε από μια συγκεκριμένη κορυφή και κινηθούμε προς τις διπλανές της, ουσιαστικά προσθέτουμε στον αριθμό που αντιπροσωπεύει έναν από τους ακεραίους $\alpha + \beta i$, $-(\alpha + \beta i)$, $i(\alpha + \beta i)$, $-i(\alpha + \beta i)$.

Επιλέγοντας τώρα δύο ακέραιους Gauss που απεικονίζονται σε δύο σημεία A και B στο εσωτερικό διαφορετικών τετραγώνων, ώστε οι θέσεις τους όμως να είναι σχετικά ίδιες εντός κάθε τετράγωνου στο οποίο ανήκουν, θα μπορούσε να υπάρχει κάποια σχέση που να τους συνδέει; Όπως έχουμε ήδη δει για τις κορυφές των τετραγώνων, έτσι και για τα σημεία αυτά, αν ανήκουν σε διπλανά τετράγωνα περνάμε από το ένα στο άλλο προσθέτοντας στους ακέραιους στους οποίους αντιστοιχούν έναν από τους ακόλουθους αριθμούς $\alpha + \beta i$, $-(\alpha + \beta i)$, $i(\alpha + \beta i)$, $-i(\alpha + \beta i)$.

Επομένως κινούμενοι τώρα από το σημείο Α προς το Β, μέσω των σημείων που βρίσκονται σε αντίστοιχες θέσεις αλλά σε διπλανά τετράγωνα, όπως φαίνεται στο σχήμα 1.3, τότε ουσιαστικά έχουμε μια μεταφορά του αρχικού ακεραίου με την προσθήκη άλλου ακέραιου Gauss πολλαπλάσιου του $\alpha + \beta i$.



Σχήμα 1.3

Επειδή όμως ο αρχικός ακέραιος δεν είναι πολλαπλάσιος του $\alpha + \beta i$, από τον αλγόριθμο της διαίρεσης γνωρίζουμε ότι αν διαιρεθεί με αυτόν θα δίνει κάποιο υπόλοιπο. Ακριβώς το ίδιο υπόλοιπο θα πάρουμε αν διαιρέσουμε και τον δεύτερο ακέραιο με τον $\alpha + \beta i$, αφού ουσιαστικά είναι το άθροισμα του πρώτου με ένα ακέραιο πολλαπλάσιο του $\alpha + \beta i$. Δηλαδή οι δύο αυτοί ακέραιοι Gauss συνδέονται με μια σχέση ισοϋπόλοιπου ως προς τον $\alpha + \beta i$.

Ορισμός 1.10: Δύο ακέραιοι Gauss α, β ονομάζονται **ισοϋπόλοιποι** ως προς έναν τρίτο γ αν $\gamma/(\alpha - \beta)$ και τους συμβολίζουμε $\alpha \equiv \beta(\mathrm{mod}\gamma)$.

Η σχέση ισοϋπόλοιπων είναι μια σχέση ισοδυναμίας, αφού για κάθε $\alpha, \beta, \gamma, \upsilon \in \mathbb{Z}[i]$ ισχύουν οι τρεις γνωστές προϋποθέσεις:

- $\alpha \equiv \alpha(\mathrm{mod}\upsilon)$, ανακλαστικότητα.
- $\alpha \equiv \beta(\mathrm{mod}\upsilon) \Rightarrow \beta \equiv \alpha(\mathrm{mod}\upsilon)$, συμμετρικότητα.
- $\alpha \equiv \beta(\mathrm{mod}\upsilon)$ και $\beta \equiv \gamma(\mathrm{mod}\upsilon) \Rightarrow \alpha \equiv \gamma(\mathrm{mod}\upsilon)$, μεταβατικότητα.

Επίσης με την βοήθεια του ορισμού που δόθηκε είναι άμεσα αποδείξιμο ότι ισχύει η ακόλουθη συνεπαγωγή:

$$\alpha \equiv \beta(\mathrm{mod}\upsilon) \text{ και } \gamma \equiv \delta(\mathrm{mod}\upsilon) \Rightarrow$$

$$\alpha \pm \gamma \equiv (\beta \pm \delta)(\mathrm{mod}\upsilon) \text{ και } \alpha\cdot\gamma \equiv (\beta\cdot\delta)(\mathrm{mod}\upsilon).$$

Η οποία επεκτείνεται και για περισσότερες των δύο ισοδυναμιών.

Η θεμελίωση της έννοιας καθώς και οι ιδιότητες των ισοϋπόλοιπων ή ισότιμων αριθμών είναι μια ακόμη σημαντική προσφορά του Gauss. Πρωτοεμφανίστηκε το 1801 στο περίφημο έργο του Disquitiones Arithmeticae και αποτελούν από τότε ένα πολύτιμο εργαλείο στην Θεωρία Αριθμών αλλά και στην Άλγεβρα.

Θεώρημα 1.13. Αν οι αριθμοί $\alpha, \beta, \gamma \in \mathbb{Z}$, ισχύει ότι $\alpha \equiv \beta(\mathrm{mod}\gamma)$ στο $\mathbb{Z}$ αν και μόνο αν $\alpha \equiv \beta(\mathrm{mod}\gamma)$ στο $\mathbb{Z}[i]$.

Απόδειξη: Το ισοδύναμο της πρότασης είναι:

$$\gamma/(\alpha - \beta) \text{ στο } \mathbb{Z} \Leftrightarrow \gamma/(\alpha - \beta) \text{ στο } \mathbb{Z}[i].$$

Αυτό ισχύει αφού αν ο $c \in \mathbb{Z}$ και $c/(x + yi)$ ισοδύναμα c/x και c/y. ♦

Παρατηρούμε λοιπόν ότι είναι αλληλένδετα συνδεδεμένοι οι ισοϋπόλοιποι ακέραιοι στα δύο αυτά σύνολα. Όμως γνωρίζουμε ότι για τους ισοϋπόλοιπους πραγματικούς ακέραιους ισχύουν κάποιες σημαντικές προτάσεις όπως οι παρακάτω:

(I) «Αν p πρώτος και $(\alpha, p) = 1$ τότε $\alpha^{p-1} \equiv 1(\mathrm{mod}p)$».

(II) «Αν p πρώτος τότε για κάθε ακέραιο α ισχύει $\alpha^p \equiv \alpha(\mathrm{mod}p)$».

Αυτές είναι γνωστές ως το **μικρό θεώρημα του Fermat**, που διατυπώθηκαν από τον ίδιο, χωρίς να δώσει απόδειξη. Η πρώτη απόδειξη τους εμφανίστηκε από τον Leibniz, αν και φαίνεται ότι υπήρχε και μια ακόμη γνωστή πριν από το 1963. Ας εξετάσουμε όμως και την αντίστοιχη πρόταση στο $\mathbb{Z}[i]$ που είναι το θεώρημα που ακολουθεί.

Θεώρημα 1.14: Αν g είναι πρώτος Gauss και $\alpha \in \mathbb{Z}[i]$ σχετικά πρώτος του g, τότε: $\alpha^{N(g)-1} \equiv 1(\mathrm{mod}g)$.

Απόδειξη: Θεωρούμε τον μοναδικό πραγματικό πρώτο p, για τον οποίον ισχύει g/p, αντίστοιχα με την απόδειξη του θεωρήματος 1.11, θα έχουμε τις εξής περιπτώσεις:

- Αν $p = 4n + 3$, τότε $N(g) = p^2$. Πρέπει να δείξουμε ότι $\alpha^{p^2-1} \equiv 1(\mathrm{mod} g)$. Αλλά είναι το ίδιο να αποδείξουμε ότι $\alpha^{p^2} \equiv \alpha(\mathrm{mod} p)$, γιατί:

$$g/p \text{ και } p/(\alpha^{p^2} - \alpha) \Rightarrow g/\alpha(\alpha^{p^2-1} - 1),$$

$$\text{επειδή } g \not/ \alpha \text{ άρα } g/(\alpha^{p^2-1} - 1).$$

Αν λοιπόν $\alpha = x + yi$ τότε:

$$\alpha^p \equiv (x + yi)^p(\mathrm{mod} p) \Leftrightarrow \alpha^p \equiv (x^p + y^p i^p)(\mathrm{mod} p).$$

Αυτό ισχύει γιατί από το διώνυμο του Νεύτωνα $(x + yi)^p = \sum_{k=0}^{p} \binom{p}{k} x^k (yi)^{p-k}$

με τον p να διαιρεί όλους τους διωνυμικούς συντελεστές εκτός από τον πρώτο και τον τελευταίο. Επίσης ισχύουν $i^p = i^{4n+3} = -i$ όπως και από την σχέση (II) στους πραγματικούς ακέραιους $x^p \equiv x(\mathrm{mod} p)$, $y^p = y\ (\mathrm{mod} p)$. Οπότε έχουμε:

$$\alpha^p \equiv (x - yi)(\mathrm{mod} p) \Leftrightarrow \alpha^p \equiv \bar{\alpha}\ (\mathrm{mod} p)$$

$$\text{υψώνοντας στη } p\text{: } \alpha^{p^2} \equiv \bar{\alpha}^p(\mathrm{mod} p).$$

Αντίστοιχα όμως ισχύει η σχέση για τον συζυγή $\bar{\alpha}^p \equiv \alpha(\mathrm{mod} p)$. Άρα

$$\alpha^{p^2} \equiv \bar{\alpha}^p(\mathrm{mod} p) \equiv \alpha(\mathrm{mod} p).$$

- Αν $p = 2$, τότε $g = 1 \pm i$ ή $g = -1 \pm i$, με $N(g) = 2$. Οπότε πρέπει να δειχθεί ότι $\alpha^{N(g)-1} = \alpha \equiv 1(\mathrm{mod} g) \Leftrightarrow g/(\alpha - 1)$. Όμως οι $g \not/ \alpha$, οπότε από τον αλγόριθμο της διαίρεσης έχουμε:

$$\alpha = \kappa g + \upsilon,\ \kappa, \upsilon \in \mathbb{Z}[i] \text{ με } 0 < N(\upsilon) < N(g) = 2. \quad (*)$$

Επομένως $N(\upsilon) = 1$, δηλαδή $\upsilon = \pm 1$ ή $\upsilon = \pm i \Leftrightarrow \upsilon - 1 = 0$ ή -2 ή $-1 \pm i$. Άρα $g/(\upsilon - 1)$, με αποτέλεσμα η (*) να δίνει: $\alpha - 1 = \kappa g + (\upsilon - 1) = \lambda g \Leftrightarrow g/(\alpha - 1)$.

- Αν $p = 4n + 1$, τότε $N(g) = p$. Πρέπει να δείξουμε ότι $\alpha^{p-1} \equiv 1(\mathrm{mod} g)$. Επειδή g/p και οι α, g σχετικά πρώτοι, ισοδύναμα πρέπει να δείξουμε ότι $\alpha^p \equiv \alpha(\mathrm{mod} p)$. Αν $\alpha = x + yi$ τότε, όπως στην πρώτη περίπτωση:

$$\alpha^p \equiv (x + yi)^p (\mathrm{mod} p) \Leftrightarrow \alpha^p \equiv (x^p + y^p i^p)(\mathrm{mod} p).$$

Αλλά $i^p = i^{4n+1} = i$, δηλαδή ισχύει $\alpha^p \equiv \alpha(\mathrm{mod} p)$. ♦

Από την επέκταση του μικρού θεωρήματος του Fermat βγάζουμε και το συμπέρασμα ότι η εξίσωση $\alpha x \equiv \beta(\mathrm{mod} g)$, με τους ακέραιους Gauss α, g σχετικά πρώτους, έχει ως λύση την $x \equiv \alpha^{N(g)-1}\beta(\mathrm{mod} g)$.

1.8 Από τον Διόφαντο έως τον Euler

Μια από τις πιο σύγχρονες Μαθηματικές τεχνικές αποτελεί η συστέγαση κοινών εννοιών σε όσο είναι δυνατόν πιο ευρεία σύνολα. Με τον τρόπο αυτό αποκτούμε νέες δομές με πιο πλούσια εργαλεία που μας βοηθούν στην εξερεύνηση και στην επίλυση παλαιότερων και νεότερων προβλημάτων. Αυτό έγινε ήδη εμφανές στην απόδειξη που δώσαμε στο θεώρημα των δύο τετραγώνων του Fermat. Με την ίδια φιλοσοφία θα αντιμετωπίσουμε και τις επόμενες προκλήσεις.

Ο Διόφαντος, ο πατέρας της Άλγεβρας όπως έχει χαρακτηριστεί, στο έργο του «Αριθμητικά» και ειδικότερα το πρόβλημα 19 του Βιβλίου ΙΙΙ αναφέρει:

«*Ευρείν τέσσαρας αριθμούς όπως ο από του*
συγκειμένο εκ των τεσσάρων τετράγωνος, εάν
τε προσλάβη έκαστον τε λείψη ποιή τετράγωνον».

Η απόδειξη που είχε δοθεί από τον ίδιο, χρησιμοποιώντας ορθογώνια τρίγωνα, υπάκουε στις μεθόδους της εποχής του. Όμως αν εστιάσουμε στο συμπέρασμα που προκύπτει από το πρόβλημα αυτό καταλήγουμε στην γνωστή ταυτότητα:

$$(\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = (\alpha\gamma - \beta\delta)^2 + (\beta\gamma + \alpha\delta)^2, \text{ με } \alpha, \beta, \gamma, \delta \in \mathbb{Z}.$$

Η οποία με την βοήθεια της μοναδικής παραγοντοποίησης στο $\mathbb{Z}[i]$ είναι:

$$\alpha^2 + \beta^2 = (\alpha + \beta i)(\alpha - \beta i)$$
$$\gamma^2 + \delta^2 = (\gamma + \delta i)(\gamma - \delta i)$$

Πολλαπλασιάζοντας κατά μέλη και λόγω της αντιμεταθετικής έχουμε:

$$(\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = (\alpha + \beta i)(\gamma + \delta i)(\alpha - \beta i)(\gamma - \delta i)$$
$$= [(\alpha\gamma - \beta\delta) + (\beta\gamma + \alpha\delta)i][(\alpha\gamma - \beta\delta) - (\beta\gamma + \alpha\delta)i]$$

$$= (\alpha\gamma - \beta\delta)^2 + (\beta\gamma + \alpha\delta)^2.$$

Ουσιαστικά βέβαια έχουμε αποδείξει την πολλαπλασιαστική ιδιότητα της στάθμης, μια και η ταυτότητα δεν είναι τίποτα άλλο παρά

$$N(\alpha + \beta i)N(\gamma + \delta i) = N((\alpha + \beta i)(\gamma + \delta i)).$$

Η ιδιότητα αυτή του Διόφαντου άνοιξε τον δρόμο για νέες αναζητήσεις και προβληματισμούς. Γνωρίζουμε λοιπόν ότι ο πολλαπλασιασμός των αθροισμάτων δύο τετραγώνων δίνει ως γινόμενο άθροισμα δύο τετραγώνων. Τώρα είναι φυσικό να αναρωτηθούμε αν οι διαιρέτες ενός αθροίσματος δύο τετραγώνων είναι και αυτοί αντίστοιχης μορφής. Στην περίπτωση βέβαια που επιλέξουμε ως διαιρετέο έναν αριθμό $\alpha^2 + \beta^2$ και υπάρχει κοινός διαιρέτης των $\alpha, \beta \in \mathbb{Z}$ έστω το δ, τότε προφανώς μπορούμε διαλέξουμε ως διαιρέτη το τετριμμένο άθροισμα τετραγώνων $0^2 + \delta^2$. Αν όμως ο μ.κ.δ.$(\alpha, \beta) = 1$ είναι εφικτό οι διαιρέτες του $\alpha^2 + \beta^2$ να γράφονται ως άθροισμα δύο τετραγώνων;

Ο Euler το 1747 διατύπωσε το σχετικό θεώρημα που ακολουθεί. Η απόδειξη, που θα παρουσιάσουμε, παρέχει ακόμη ένα τεκμήριο σχετικό με την θέση που προαναφέραμε για την χρησιμότητα των ακεραίων Gauss. Ένα σύνολο εμπλουτισμένο με εργαλεία που μας παρέχουν καλύτερη κατανόηση και ευκολότερη προσέγγιση στα χαρακτηριστικά των πραγματικών ακεραίων.

Θεώρημα 1.15: (**διαιρέτες αθροίσματος δύο τετραγώνων**). Για τους ακεραίους α, β με μ.κ.δ.$(\alpha, \beta) = 1$ κάθε διαιρέτης του $\alpha^2 + \beta^2$ είναι της μορφής $\gamma^2 + \delta^2$, με μ.κ.δ.$(\gamma, \delta) = 1$.

Απόδειξη: Γνωρίζουμε ότι ισχύει $\alpha^2 + \beta^2 = (\alpha + \beta i)(\alpha - \beta i)$. Από την ιδιότητα των πρώτων διαιρετών στο $\mathbb{Z}[i]$, κάθε πρώτος Gauss g που διαιρεί το $\alpha^2 + \beta^2$ θα είναι διαιρέτης του $\alpha + \beta i$ είτε του $\alpha - \beta i$. Ο g αποκλείεται να είναι πραγματικός ακέραιος, γιατί θα έπρεπε το $\frac{\alpha}{g} \pm \frac{\beta}{g} i \in \mathbb{Z}[i]$. Το οποίο δεν μπορεί να ισχύει αφού μ.κ.δ.$(\alpha, \beta) = 1$.

Από την μοναδικότητα παραγοντοποίησης στο $\mathbb{Z}[i]$ κάθε πραγματικός ακέραιος διαιρέτης του $\alpha^2 + \beta^2$ θα γράφεται ως γινόμενο κάποιων από τους g πρώτους διαιρέτες Gauss καθώς και των συζυγών τους. Οπότε από τα

ζευγάρια αυτά αν συμβολίσουμε με $\gamma + \delta i$ τους διαιρέτες του $\alpha + \beta i$, τότε αντίστοιχα οι ακέραιοι $\gamma - \delta i$ θα είναι οι διαιρέτες του $\alpha - \beta i$. Συνεπώς ο πραγματικός ακέραιος διαιρέτης του $\alpha^2 + \beta^2$ θα έχει την ακόλουθη μορφή: $(\gamma + \delta i)(\gamma - \delta i) = \gamma^2 + \delta^2$.

Επίσης αν ο μ.κ.δ.$(\gamma, \delta) = \kappa \in \mathbb{Z}$, τότε $\kappa/(\gamma + \delta i)$ δηλαδή $\kappa/(\alpha + \beta i)$ οπότε κ/α και κ/β. Όμως μ.κ.δ$(\alpha, \beta) = 1$, συνεπώς $\kappa = 1$. ♦

Μια ακόμη εφαρμογή των ακεραίων Gauss, σε απόδειξη ενός κλασικού προβλήματος φυσικών αριθμών, σχετίζεται με την εύρεση των Πυθαγόρειων τριάδων. Ο Πρόκλος στο έργο του «Σχόλια στο Πρώτο Βιβλίο των Στοιχείων του Ευκλείδη» αναφέρει δύο μεθόδους εύρεσής των, η μια αποδίδεται στους Πυθαγόρειους και η άλλη στον Πλάτωνα, χωρίς όμως να είναι σε θέση να τις υπολογίσουν όλες. Η φόρμα που τις παράγει συναντάτε πρώτη φορά στην απόδειξη της Πρόταση Χ.29 των Στοιχείων:

«*Ευρείν δύο ρητάς δυνάμει συμμέτρους,*
ώστε την μείζονα της ελάσσονος μείζον
δύνασθαι τω από συμμέτρου εαυτή μήκει».

Την ίδια μορφή με του Ευκλείδη χρησιμοποίησε αργότερα και ο Διόφαντος στο Πρόβλημα ΙΙ. 8 των Αριθμητικών:

«*Τον επιταχθέντα τετράγωνον διελείν εις δύο τετράγωνους*».

Στο περιθώριο της επίλυσης αυτού του προβλήματος σε ένα αντίτυπο του Bachet έγραψε ο Fermat το 1637 την περίφημη φράση του: «Είναι αδύνατον μια κυβική δύναμη να γραφεί ως άθροισμα δύο κυβικών δυνάμεων ή μια τέταρτη δύναμη να γραφεί ως άθροισμα δύο τέταρτων δυνάμεων και γενικά οποιαδήποτε δύναμη μεγαλύτερη του τετραγώνου είναι αδύνατον να γραφεί ως άθροισμα δύο ίδιων δυνάμεων. Έχω ανακαλύψει μια πραγματικά υπέροχη απόδειξη, που αυτό το περιθώριο είναι πολύ στενό για να την χωρέσει». Αυτό που χαρακτηρίστηκε αργότερα ως το τελευταίο θεώρημα του Fermat και έμελε να στοιχειώσει πολλές γενιές μαθηματικών πριν αποδειχθεί από τον Andrew Wiles τον Ιούνιο του 1993.

Το ζητούμενο λοιπόν του προβλήματος είναι η εύρεση των ακέραιων λύσεων της εξίσωσης $\alpha^2 + \beta^2 = \gamma^2$. Εστιάζοντας την αναζήτηση μας σε

φυσικούς ακέραιους οι οποίοι δεν έχουν κοινό διαιρέτη μεταξύ τους, που θα τις αποκαλούμε **αρχικές**. Υπολογίζοντας αυτές τις τριάδες αριθμών και πολλαπλασιάζοντας με οποιοδήποτε ακέραιο, θα έχουμε νέες Πυθαγόρειες τριάδες. Αν βέβαια δύο από τους α, β, γ έχουν έναν κοινό διαιρέτη, τότε προφανώς και ο τρίτος θα έχει τον ίδιο κοινό διαιρέτη. Επομένως είναι αρκετό οι δύο από αυτούς, έστω οι α και β, να είναι σχετικά πρώτοι. Επίσης οι α, β δεν θα μπορούσαν να είναι και οι δύο περιττοί. Αν συμβεί κάτι τέτοιο τότε $\alpha^2 = 8\kappa + 1$ και $\beta^2 = 8\lambda + 1$, με $\kappa, \lambda \in \mathbb{Z}$, οπότε το $\gamma^2 = 8\mu + 2$, $\mu \in \mathbb{Z}$. Αυτό είναι αδύνατο γιατί δεν υπάρχουν τετράγωνα ακεραίων τέτοιας μορφής. Επομένως ό ένας από αυτούς θα είναι περιττός και ο άλλος άρτιος, οπότε και το γ θα είναι περιττός.

Θεώρημα 1.16: Κάθε **αρχική Πυθαγόρεια τριάδα** (α, β, γ), με τον α περιττό, έχει την μορφή:

$$\alpha = m^2 - n^2,\ \beta = 2mn,\ \gamma = m^2 + n^2,\ \text{όπου}\ m > n > 0,$$

σχετικά πρώτοι, χωρίς να μπορεί να είναι και οι δύο περιττοί ή και οι δύο άρτιοι. Επίσης κάθε διαφορετική επιλογή του ζεύγους (m, n) δίνει πάντα μια αρχική Πυθαγόρεια τριάδα.

Απόδειξη: Η εξίσωση μπορεί να γραφεί και ως εξής:

$$\alpha^2 + \beta^2 = (\alpha + \beta i)(\alpha - \beta i) = \gamma^2.$$

Αν δεχθούμε πως υπάρχει κάποιος ακέραιος Gauss δ που να είναι κοινός διαιρέτης των $\alpha + \beta i$, $\alpha - \beta i$, τότε ο δ θα διαιρεί το άθροισμα τους και την διαφορά τους. Άρα $\delta/2\alpha$ και $\delta/2\beta$, όπως επίσης:

$$\delta^2/\gamma^2 \Rightarrow N(\delta^2)/N(\gamma^2) \Rightarrow N(\delta^2)/\gamma^4,$$

με γ^4 περιττό. Συμπεραίνουμε λοιπόν ότι το $\delta \not/ 2$, οπότε δ/α και δ/β. Επειδή $\mu.\kappa.\delta.(\alpha, \beta) = 1$ τότε θα υπάρχουν ακέραιοι κ, λ ώστε $\kappa\alpha + \lambda\beta = 1$. Από θεώρημα 1.12 οι α, β είναι σχετικά πρώτοι στο $\mathbb{Z}[i]$, επομένως ο δ είναι αντιστρέψιμος. Πράγμα που σημαίνει ότι οι $\alpha + \beta i$, $\alpha - \beta i$ είναι σχετικά πρώτοι. Αφού λοιπόν το γινόμενο δύο σχετικά πρώτων γράφεται ως τέλειο τετράγωνο, όπως έχουμε ήδη αναφέρει στην παράγραφο 1.6, καθένας από αυτούς ή θα είναι τέλειο τετράγωνο ή θα είναι γινόμενο τετράγωνου επί i.

Δηλαδή γνωρίζουμε πλέον ότι υπάρχουν πραγματικοί ακέραιοι m, n τέτοιοι ώστε:

$$\alpha + \beta i = (m + ni)^2 \text{ ή } \alpha + \beta i = i(m + ni)^2 \Rightarrow$$

$$\alpha + \beta i = (m^2 - n^2) + 2mni \text{ ή } \alpha + \beta i = -2mn + (m^2 - n^2)i.$$

Επειδή όμως επιλέξαμε τον α περιττό και τον β άρτιο, τότε:

$$\alpha = m^2 - n^2, \ \beta = 2mn \text{ και}$$

$$\gamma^2 = \alpha^2 + \beta^2 = (m^2 - n^2)^2 + 4m^2n^2 = (m^2 + n^2)^2$$

$$\text{αφού } \gamma > 0 \text{ τότε } \gamma = m^2 + n^2.$$

Από την επιλογή του $\beta > 0$ έχουμε ότι τα m, n πρέπει να είναι ομόσημοι, οπότε χωρίς βλάβη της γενικότητας επιλέγουμε να είναι και οι δύο θετικοί. Ακόμη επειδή $\alpha > 0$ τότε $m > n$. Επίσης το α είναι περιττός, συνεπώς ένας από τους m, n θα είναι άρτιος και ο άλλος περιττός. Αν τώρα οι m, n είχαν κάποιον κοινό διαιρέτη τότε και οι α, β δεν θα ήταν σχετικά πρώτοι, οπότε $\mu.\kappa.\delta.(m, n) = 1$.

Αντίστροφα τώρα θα δείξουμε ότι κάθε τριάδα $(m^2 - n^2, 2mn, m^2 + n^2)$ με $m > n$, θετικούς και σχετικά πρώτους ακεραίους, αποτελούν πάντα αρχική Πυθαγόρεια τριάδα. Επειδή ισχύει ότι:

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2,$$

ας υποθέσουμε ότι η τριάδα αυτή δεν είναι αρχική. Τότε υπάρχει κάποιος πρώτος $p \neq 2$ που διαιρεί και τους τρεις. Από την σχέση:

$$p/2mn \text{ έχουμε } p/m \text{ ή } p/n.$$

Έστω δεχόμαστε ότι ισχύει το πρώτο, όμως:

$$p/(m^2 - n^2) \Rightarrow p/n^2 \Rightarrow p/n.$$

Αντίστοιχα αν επιλέγαμε p/n θα καταλήγαμε ότι p/m. Αυτό είναι αδύνατο μια και $\mu.\kappa.\delta.(m, n) = 1$.

Άρα η τριάδα που επιλέξαμε είναι αρχική και οι παράμετροι m, n ουσιαστικά είναι το πραγματικό και φανταστικό μέρος των τετραγωνικών ριζών του $\alpha + \beta i$. Όμως υπάρχουν μόνο δύο τέτοιες ρίζες που διαφέρουν κατά το πρόσημο, οπότε η επιλογή της θετικότητας των παραμέτρων μας παρέχει συγχρόνως και την ύπαρξη της μοναδικότητας για κάθε αρχική Πυθαγόρεια τριάδα. ♦

Μπορούμε λοιπόν βάση του παραπάνω να υπολογίσουμε αρχικές Πυθαγόρειες τριάδες και με τον εξής απλό τρόπο. Επιλέγουμε έναν μη μηδενικό ακέραιο Gauss α έτσι ώστε το πραγματικό και το φανταστικό μέρος του να είναι πραγματικοί ακέραιοι σχετικά πρώτοι. Αν το τετράγωνό του γράφεται στην μορφή:

$$\alpha^2 = x + yi, \text{ τότε η τριάδα } (|x|, |y|, N(\alpha)),$$

θα αποτελεί μια αρχική Πυθαγόρεια τριάδα.

Η εφαρμογή που ακολουθεί και αποδεικνύεται με την χρήση των ακεραίων Gauss αφορά μια ακόμη γνωστή Διοφαντική εξίσωση, με επεκτάσεις στην Αναλυτική Γεωμετρία.

Θεώρημα 1.17: Η εξίσωση $x^3 - y^2 = 1$, έχει μοναδική ακέραια λύση την $(x, y) = (1, 0)$.

Απόδειξη: Η εξίσωση γράφεται: $x^3 = y^2 + 1 = (y + i)(y - i)$. Αν υπάρχει $\delta \in \mathbb{Z}[i]$ κοινός διαιρέτης των $y + i$, $y - i$ τότε διαιρεί και τη διαφορά τους, δηλαδή $\delta / 2i \Rightarrow \delta / (1 + i)^2$. Από την μοναδική παραγοντοποίηση στο $\mathbb{Z}[i]$ ο δ θα είναι αντιστρέψιμος ή ίσος με $1 + i$ ή $(1 + i)^2$. Αν θεωρήσουμε ότι δεν είναι αντιστρέψιμος τότε ισχύει:

$$(1 + i)/x^3 \Rightarrow N(1 + i)/N(x^3) \Rightarrow 2/x^6.$$

Οπότε ο x είναι άρτιος και επειδή $x^3 = y^2 + 1$ τότε $y^2 = 8\kappa - 1$, με $\kappa \in \mathbb{Z}$, πράγμα αδύνατο αφού κανένα τετράγωνο ακεραίου δεν έχει αυτή την μορφή. Συνεπώς ο δ είναι αντιστρέψιμος και οι $y + i$, $y - i$ σχετικά πρώτοι.

Το γινόμενο των δύο αυτών σχετικά πρώτων ακεραίων Gauss μας δίνει έναν κύβο. Επομένως ο καθένας από αυτούς θα είναι κύβος ή θα είναι κύβος επί κάποιον αντιστρέψιμο. Όμως κάθε αντιστρέψιμος είναι και ο ίδιος κύβος όπως έχουμε δει στην παράγραφο 1.6, οπότε κάθε ένας από τους $y + i$, $y - i$ είναι κύβος. Υπάρχουν λοιπόν πραγματικοί ακέραιοι m, n ώστε:

$$y + i = (m + ni)^3 = m(m^2 - 3n^2) + n(3m^2 - n^2)i.$$

Από την εξίσωση $n(3m^2 - n^2) = 1$, έχουμε $n = \pm 1$. Αν $n = 1$ τότε $3m^2 - 1 = 1 \Rightarrow 3m^2 = 2$, αδύνατη στους ακεραίους. Αν $n = -1$ τότε $3m^2 - 1 = -1 \Rightarrow m = 0$.

Οπότε $y = 0$ και $x^3 = 0 + 1 \Rightarrow x = 1$. ♦

Με την χρήση των ακεραίων Gauss το 1850 ο V. A. Lebesgue απέδειξε ότι η εξίσωση $y^2 = x^n - 1$ με $n \geq 2$ δεν έχει μη μηδενικές λύσεις. Επίσης με αντίστοιχους τρόπους μπορούμε να λύσουμε και τις ακόλουθες Διοφαντικές εξισώσεις, με τις οποίες ασχολήθηκε και ο Fermat:

- $2x^3 = y^2 + 1$, οι ρίζες της είναι $(x, y) = (1, \pm 1)$.
- $x^3 = y^2 + 4$, οι ρίζες της είναι $(x, y) = (2, \pm 2)$ ή $(5, \pm 11)$.

Όπως ήταν αναμενόμενο κατά την επίλυση προβλημάτων σαν αυτά που είδαμε, προέκυψαν και άλλα που αφορούν τους ίδιους τους ακεραίους Gauss. Χαρακτηριστικό είναι το ακόλουθο.

Θεώρημα 1.18: Αν ο μη μηδενικός z είναι ακέραιος Gauss τότε υπάρχει φυσικός αριθμός $\nu \neq 0$ ώστε $z^\nu \in \mathbb{Z}$ αν και μόνο αν $\mathrm{Im}(z) = 0$ ή $\mathrm{Re}(z) = 0$ ή $\mathrm{Im}(z) = \pm \mathrm{Re}(z)$.

Απόδειξη: Στην περίπτωση που ο z είναι ανάγωγος, έχουμε: $(\pm 1)^\nu \in \mathbb{Z}$ για κάθε $\nu \in \mathbb{N}^*$ και $(\pm i)^\nu \in \mathbb{Z}$ για κάθε $\nu = 4\kappa$, με $\kappa \in \mathbb{N}^*$. Στην περίπτωση που ο z δεν είναι πρώτος, από την μοναδική παραγοντοποίηση θα υπάρχουν πρώτοι $g_1, g_2, \ldots, g_\lambda$ ώστε $z = g_1 \cdot g_2 \cdot \ldots \cdot g_\lambda$. Οπότε αρκεί να δείξουμε ότι $g_i^{\kappa_i} \in \mathbb{Z}$ με $\kappa_i \in \mathbb{N}^*$, για κάθε $i = 1, 2, \ldots, \lambda$ και έτσι το $\nu = \kappa_1 \cdot \kappa_2 \cdot \ldots \cdot \kappa_\lambda$.

Εύκολα λοιπόν η γενική περίπτωση εξειδικεύεται μόνο αν ο z είναι πρώτος Gauss. Θεωρούμε τώρα ότι ο $z^\nu = m \in \mathbb{Z}$, προφανώς z/m και επομένως για τον συζυγή του ισχύει ότι $\bar{z}/\bar{m} = m$, αφού $m \in \mathbb{Z}$. Δηλαδή $\bar{z}/z^\nu$ και επειδή ο $\bar{z}$ είναι πρώτος τότε $\bar{z}/z$. Αυτό σημαίνει ότι $z = \bar{z}$, δηλαδή $\mathrm{Im}(z) = 0$ ή ότι οι z και $\bar{z}$ είναι ισοδύναμοι. Στην περίπτωση αυτή αν $z = -\bar{z}$, τότε $\mathrm{Re}(z) = 0$, ενώ αν $z = \pm i\bar{z}$, τότε $\mathrm{Im}(z) = \pm \mathrm{Re}(z)$.

Για την απόδειξη του αντίστροφου έχουμε: Αν $\mathrm{Im}(z) = 0$, τότε $z^\nu \in \mathbb{Z}$ για κάθε $\nu \in \mathbb{N}^*$. Αν $\mathrm{Re}(z) = 0$, τότε $z^\nu \in \mathbb{Z}$ για $\nu = 2\kappa$ με $\kappa \in \mathbb{N}^*$. Αν $\mathrm{Im}(z) = \pm \mathrm{Re}(z)$, τότε $z^\nu \in \mathbb{Z}$ για $\nu = 4\kappa$ με $\kappa \in \mathbb{N}^*$.

1.9 Άλυτα Προβλήματα και Εικασίες

Πέραν όμως των προβλημάτων που έχουν λυθεί με την βοήθεια των ακεραίων του Gauss, μέσα στο σύνολο αυτό έχουν διαμορφωθεί ή καλύτερα μετεξελιχθεί και προβλήματα που ακόμη δεν έχουν αποδειχθεί. Γνωστές εικασίες της θεωρίας αριθμών έχουν διατυπωθεί και για τους αριθμούς που μελετάμε. Μια παράλληλη παράθεση αυτών των υποθέσεων με τις αντίστοιχες για τους πραγματικούς ακέραιους θα παρουσιάσουμε στην συνέχεια.

Πρωτίστως θα εστιάσουμε σε σύνολα πρώτων Gauss που παρουσιάζουν ιδιαίτερο ενδιαφέρον. Οι ορισμοί αυτών των αριθμών, που θα δοθούν άμεσα, είναι επιλεγμένοι λόγω του ότι χαρακτηρίζονται ως οι πιο περιοριστικοί από όσους έχουν δοθεί.

Ορισμός 1.11: Δύο πρώτοι Gauss ονομάζονται **δίδυμοι** (twin) αν η διαφορά τους είναι ίση με $(1 + i)e$, όπου $N(e) = 1$.

Στους πραγματικούς πρώτους οι δίδυμοι γνωρίζουμε ότι έχουν διαφορά ίση με ± 2 και επίσης ο μικρότερος περιττός από αυτούς που δεν είναι δίδυμος είναι ο 23. Επίσης στους ακέραιους Gauss οι μόνοι άρτιοι πρώτοι είναι οι $(\pm 1 \pm i)$. Ακόμη παρατηρούμε μια έλλειψη δίδυμων μέχρι τους αριθμούς $17 \pm 12i$, των οποίων το μέτρο τους (η τετραγωνική ρίζα της στάθμης τους) είναι περίπου 20,8 αρκετά κοντά στον 23. Αλλά και στο $\mathbb{Z}[i]$ ο 23 είναι δίδυμος με τον $24 + i$. Υπάρχει λοιπόν μια ενδεχόμενη σύνδεση των δίδυμων στα δύο αυτά συστήματα.

Ορισμός 1.12: Τρεις πρώτοι Gauss g_1, g_2, g_3 ονομάζονται **τρίδυμοι** (triplet) αν $g_1 - g_2 = g_2 - g_3 = (1 + i)e$, όπου $N(e) = 1$.

Στους πραγματικούς πρώτους είναι γνωστό ότι οι μοναδικοί τρίδυμοι είναι οι ακέραιοι 3, 5, 7. Μια τέτοια τριάδα αριθμών αντίστοιχα στο $\mathbb{Z}[i]$ είναι οι $20 + 3i$, $21 + 4i$, $22 + 5i$. Επίσης ένας εναλλακτικός, αλλά λιγότερο περιοριστικός, ορισμός που θα μπορούσαμε να δώσουμε για τους τρίδυμους θα ήταν να ίσχυε η ισότητα των στάθμεων τους, δηλαδή $N(g_1 - g_2) = N(g_2 - g_3) = N(1 + i)$. Βάση αυτού του ορισμού τρίδυμοι θα είναι και οι πρώτοι $10 + i$, 11, $10 – i$, όπως και οι $19 + 10i$, $20 + 11i$, $21 + 10i$.

Ορισμός 1.13: Τέσσερεις πρώτοι Gauss g_1, g_2, g_3, g_4 ονομάζονται **τετράδυμοι** (quadruplet) αν $g_1 - g_2 = g_2 - g_3 = g_3 - g_4 = (1 + i)e$, με $N(e) = 1$.

Τέτοιες τετράδες πρώτων Gauss είναι οι $31 + 26i$, $32 + 27i$, $33 + 28i$, $34 + 29i$ καθώς και οι $16 + 19i$, $17 + 18i$, $18 + 17i$, $19 + 16i$. Αντίστοιχα με τους τρίδυμους μπορούμε και εδώ να δώσουμε λιγότερο περιοριστικό ορισμό, αν θέσουμε ως προϋπόθεση την ισότητα των στάθμεων τους, δηλαδή $N(g_1 - g_2) = N(g_2 - g_3) = N(g_3 - g_4) = N(1 + i)$. Στην περίπτωση αυτή δεχόμαστε ως τετράδυμους και τους $25 + 112i$, $26 + 11i$, $27 + 10i$, $25 + 9i$ ή και τους $24 + 5i$, $25 + 4i$, $26 + 5i$, $25 + 6i$. Επίσης ένας ακόμη ορισμός που δίνει πολύ μεγαλύτερη ελευθερία και επιτρέπει τετράδες όπως οι $43 + 10i$, $44 + 9i$, $45 + 8i$, $43 + 8i$ να χαρακτηριστούν τετράδυμοι είναι αν ίσχυε: $N(g_i - g_k) = N(1 + i)$ για $i \neq k$. Κάτι τέτοιο βέβαια απέχει αρκετά από την χρηστική οριοθέτηση τέτοιων συνόλων ακεραίων Gauss, οπότε δεν θα επεκταθούμε σε μορφές αυτού του είδους.

Ορισμός 1.14: Πέντε πρώτοι Gauss g_1, g_2, g_3, g_4, g_5 ονομάζονται **πεντάδυμοι** (quintuplet) αν $g_1 - g_2 = g_2 - g_3 = g_3 - g_4 = g_4 - g_5 = (1 + i)e$, με $N(e) = 1$.

Και σε αυτούς τους αριθμούς θα επιμείνουμε στον πιο περιοριστικό ορισμό και όχι σε αντίστοιχους όπως είδαμε παραπάνω. Έτσι λοιπόν ισχύει και το θεώρημα που ακολουθεί.

Θεώρημα 1.19: Υπάρχουν πεπερασμένες πεντάδες πρώτων Gauss που είναι πεντάδυμοι και αποτελούνται από τους αριθμούς: $\pm 5 \pm 2i$, $\pm 4 \pm i$, ± 3, $\pm 2 \pm i$, $\pm 1 \pm 2i$, $\pm 3i$, $\pm 1 \pm 4i$, $\pm 2 \pm 5i$.

Απόδειξη: Σύμφωνα με τον ειδικό αλγόριθμο (J. H. Jordan and C. J. Potratz: Residue System in the Gaussian Integers, Mathematics Magazine τεύχος 38 του 1965 σελ. 1 – 12) για κάθε ακέραιο Gauss α που διαιρείται με τον $2 + i$ υπάρχουν $\kappa, \upsilon \in \mathbb{Z}[i]$ ώστε $\alpha = (2 + i)\kappa + \upsilon$ με $N(\upsilon) \leq 1$, δηλαδή $\upsilon = 0$ ή $\upsilon = \pm 1$ ή $\upsilon = \pm i$. Αν θεωρήσουμε τώρα ότι $g_1 = (2 + i)\kappa + \upsilon$ με $N(\upsilon) \leq 1$ και ας επιλέξουμε το e του ορισμού ίσο με -1, τότε:

- Για $\beta = 0$ το $g_1 = (2 + i)\kappa$.
- Για $\beta = 1$ το $g_2 = (2 + i)(\kappa + 1)$.

- Για $\beta = -i$ το $g_3 = (2 + i)(\kappa + 1)$.
- Για $\beta = i$ το $g_4 = (2 + i)(\kappa + 2\,i)$.
- Για $\beta = -1$ το $g_5 = (2 + i)(\kappa + 2 + i)$.

Παρατηρούμε λοιπόν ότι σε κάθε περίπτωση ένας από τους g_i έχει παράγοντα τον $2 + i$ δηλαδή δεν είναι πρώτος, εκτός της περίπτωσης που $g_i = (2 + i)\kappa$ με $N(\kappa) = 1$. Αυτό λοιπόν συμβαίνει όταν οι επιλεγμένοι αριθμοί είναι αυτοί τοι θεωρήματος. Ανάλογα αποτελέσματα προκύπτουν και για τις επιλογές των $e = 1$ ή $e = \pm i$. ♦

Σύμφωνα λοιπόν με τους ορισμούς που επιλέχθηκαν, σχετικά με τα σύνολα των αριθμών που προαναφέραμε, προκύπτουν οι εξής εικασίες:

Εικασία (1): Υπάρχουν άπειρα ζεύγη δίδυμων πρώτων Gauss.

Εικασία (2): Υπάρχουν άπειρες τριάδες τρίδυμων πρώτων Gauss.

Εικασία (3): Υπάρχουν άπειρες τετράδες τετράδυμων πρώτων Gauss.

Οι τρεις υποθέσεις που διατυπώθηκαν μπορούν σίγουρα να ελεγχθούν αυτόνομα. Όμως είναι εμφανής και η σχέση που τις συνδέει. Αν για παράδειγμα δειχθεί ότι η εικασία (1) δεν ισχύει, αυτόματα δεν ισχύουν και οι άλλες δύο. Επίσης αν δειχθεί ότι η εικασία (3) ισχύει τότε συμβαίνει το ίδιο και για την (2) και (1).

Η εικασία (1) είναι μια επέκταση στο $\mathbb{Z}[i]$ του γνωστού **άλυτου προβλήματος των δίδυμων** πραγματικών πρώτων ακεραίων. Σύμφωνα με το οποίο ζητείται να αποδειχθεί ότι υπάρχουν άπειροι πρώτοι ακέραιοι p ώστε και ο $p + 2$ να είναι και αυτός πρώτος. Το πρόβλημα αυτό διατυπώθηκε στην γενική του μορφή το 1849 από τον de Polignac που είκαζε ότι: «Για κάθε μη μηδενικό φυσικό αριθμό v υπάρχουν άπειρα ζεύγη πρώτων p, p' ώστε $p - p' = 2v$». Φυσικά για $v = 1$ προκύπτει η εικασία των δίδυμων πραγματικών πρώτων. Η πιο πρόσφατη προσπάθεια επίλυσης του αιτήματος των δίδυμων έχει γίνει από τον καθηγητή του πανεπιστημίου του Vanderbilt τον Richard Arenstorf στις 26/3/2004, αλλά επειδή προέκυψαν λάθη στην επίλυση, αποσύρθηκε για να διορθωθεί.

Ένα επίσης πολύ γνωστό άλυτο πρόβλημα, αγαπημένο πολλών λογοτεχνών, που έχει σχέση με τους πραγματικούς ακέραιους είναι και η

εικασία του Goldbach. Ο Πρώσος μαθηματικός Christian Goldbach (1690 – 1764) σε μια επιστολή που έστειλε στις 7/6/1742 στον Euler διατύπωνε την εικασία πως: «Κάθε άρτιος ακέραιος αριθμός μεγαλύτερος του 2 γράφεται ως άθροισμα δύο πρώτων». Μιας εικασίας που φυσικά ακόμη παραμένει αναπόδεικτη παρόλες τις προσπάθειες που κατά καιρούς επιχειρήθηκαν. Μάλιστα ο εκδοτικός οίκος Faber and Faber είχε προσφέρει έπαθλο 1.000.000 δολαρίων σε όποιον το αποδείκνυε από τις 10/3/2000 έως τις 20/3/2002. Σήμερα με την βοήθεια των υπολογιστών έχει επαληθευτεί για αριθμούς έως τον 10^{14}. Αλλά όπως θα δούμε υπάρχουν πολλές δυνατότητες γενίκευσης της εικασίας αυτής και στο σύνολο των ακέραιων Gauss.

Εικασία (4): Για κάθε άρτιο ακέραιο Gauss α υπάρχουν πρώτοι Gauss p και q τέτοιοι ώστε p + q = α.

Η διατύπωση αυτή δεν είναι τίποτα άλλο παρά μια απλή μεταφορά της εικασίας του Goldbach στο σύνολο $\mathbb{Z}[i]$. Όμως περισσότερο προσεγγίζει την ακόλουθη πρόταση: «Κάθε άρτιος ακέραιος είναι άθροισμα ή διαφορά δύο θετικών πρώτων». Δεδομένου ότι η θετικότητα είναι χωρίς νόημα στους ακέραιους Gauss, θα μπορούσαμε να θέσουμε ως προϋπόθεση οι p και q να ανήκουν στο ίδιο ημιεπίπεδο ή ότι οι στάθμες τους να είναι μικρότερες ή ίσες από την στάθμη του α, τότε έχουμε την εξής διατύπωση:

Εικασία (5): Για κάθε άρτιο ακέραιο Gauss α, με N(α) > 2, υπάρχουν πρώτοι Gauss p και q τέτοιοι ώστε p + q = α και κάθε μια από τις γωνίες POA και AOQ να είναι μικρότερες των 45°, όπου P, Q οι εικόνες των p, q αντίστοιχα, O η αρχή των αξόνων και A εικόνα του α.

Είναι φανερό ότι η εικασία (5) περιέχει την (4) για κάθε μια από τις προϋποθέσεις που τέθηκαν. Επίσης έχει ελεγχθεί για τους άρτιους αριθμούς στο $\mathbb{Z}[i]$. Ακόμη ισχυρότερους όρους μπορούμε να θέσουμε μειώνοντας την γωνία. Συγχρόνως πρέπει όμως να αυξηθεί η στάθμη του άρτιου για να αποφύγουμε κάποιες εξαιρέσεις, οπότε καταλήγουμε στην ακόλουθη:

Εικασία (6): Αν α είναι άρτιος ακέραιος Gauss με στάθμη μεγαλύτερη του 10, τότε υπάρχουν πρώτοι p και q ώστε α = p + q και κάθε μια από τις

γωνίες POA και AOQ να είναι μικρότερες των $30°$, όπου P, Q οι εικόνες των p, q αντίστοιχα, O η αρχή των αξόνων και A εικόνα του $α$.

Μια πρόταση που επίσης έχει ελεγχθεί για τους άρτιους ακέραιους στο $\mathbb{Z}[i]$. Τονίζουμε ακόμη ότι οι $1 + 3i$, $3 + i$, 2 και οι ισοδύναμοί τους έχουν ανάγκη γωνίας $45°$. Για γωνία $0°$ ή $4°$ δεν είναι δυνατόν να υπάρχουν αριθμοί τέτοιοι ώστε να είναι άθροισμα δύο πρώτων Gauss. Πιθανόν όμως τέτοιες προτάσεις θα μπορούσαμε να έχουμε για κατάλληλη μείωση της γωνίας με αντίστοιχη κάθε φορά περιοριστική επιλογή της στάθμης του άρτιου. Παρατηρούμε λοιπόν ότι γενικεύοντας κάποιες φημισμένες εικασίες στους πραγματικούς ακέραιους, οδηγούμαστε σε ένα πλήθος άλλων εικασιών στο σύνολο των ακεραίων Gauss.

Έχοντας τεκμηριώσει μια πρώτη ψηλάφηση του συνόλου των ακεραίων Gauss παρατηρούμε ότι η Αριθμητική τους διαφοροποιείται σημαντικά από την Άλγεβρα των μιγαδικών αριθμών, παρότι αποτελούν υποκλάση τους. Χωρίς λοιπόν να αποτελούν μια τετριμμένη λεπτομέρεια παρουσιάζουν μια δυναμική χρηστική ακόμη και σε πεδία που φαινομενικά είναι ξένα προς αυτούς. Άλλωστε αυτός είναι ο λόγος που τους έκανε ένα αξιοπρόσεχτο πολυεργαλείο σε πολλούς τομείς των Μαθηματικών.

ΚΕΦΑΛΑΙΟ 2 ΔΑΚΤΥΛΙΟΙ ΣΤΟ $\mathbb{Z}[i]$

«Τα ίδια λάθη μπορούν κάλλιστα να επαναληφθούν. Πρόσφατα κατάφερε να δοθεί λύση σε ένα θεώρημα που επί αιώνες δεν κατάφερναν να λύσουν. Μπορεί να μην το έλυναν, ανακάλυπταν όμως πράγματα τα οποία τους κατηύθυναν κάπου και μάθαιναν από αυτά. Τελικώς, έτσι κατάφεραν να βρουν την απόδειξη και να τη δημοσιεύσουν. Βασίστηκαν στη δουλειά και στα λάθη άλλων επιστημόνων, που είχαν προηγηθεί. Στην έρευνα αλλά και στη ζωή μπορεί άλλος να ανακαλύψει την πόρτα και άλλος το κλειδί».

JOHN FORBES NASH

2.1 Ομομορφισμοί Δακτυλίων

Κατά την διάρκεια της παρουσίασης σχετικά με την μοναδική ανάλυση σε πρώτους, μέσα στο σύνολο των ακεραίων Gauss, αναφερθήκαμε και στον αλγόριθμό της διαίρεσης. Στο κεφάλαιο αυτό θα ασχοληθούμε πιο αναλυτικά με την πράξη της διαίρεσης στο $\mathbb{Z}[i]$ καθώς και με την μελέτη των επιμέρους δακτυλίων που εμφανίζονται μέσα στο σύνολο αυτό. Η προσέγγιση όλων αυτών, όπως άλλωστε έχουμε κάνει και έως τώρα, θα γίνει με την βοήθεια των αλγεβρικών δομών που απαιτούνται και των απεικονίσεων που τις συνδέουν. Σε πρώτη φάση θα ορίσουμε τα συγκεκριμένα αλγεβρικά μέσα, όπως επίσης θα αποδείξουμε και μια σειρά θεωρημάτων που τα διέπουν και απαιτούνται για την τεκμηριωμένη παρουσίαση τους. Τα παραδείγματα που θα χρησιμοποιηθούν για την καλύτερη κατανόηση των προτάσεων θα είναι επιλεγμένα από τα ίδια πάντα γνωστά μας χρηστικά σύνολα.

Ορισμός 2.1: Σε δύο δακτυλίους $<D, \oplus, \otimes>$ και $<D', +, \times>$ κάθε απεικόνιση $\varphi: D \to D'$ με τις ιδιότητες:

$$\varphi(\alpha \oplus \beta) = \varphi(\alpha) + \varphi(\beta) \text{ και}$$

$$\varphi(\alpha \otimes \beta) = \varphi(\alpha) \times \varphi(\beta).$$

για όλα τα στοιχεία $\alpha, \beta \in D$, ονομάζεται **ομομορφισμός.**

Η ορολογία των ομομορφισμών εξειδικεύεται ως ακολούθως. Ένας ομομορφισμός που είναι επί στον D' λέγεται **επιμορφισμός**, ενώ στην περίπτωση που είναι 1-1 ονομάζεται **μονομορφισμός**. Όταν είναι 1-1 και συγχρόνως επί καλείται **ισομορφισμός.** Σε έναν ισομορφισμό οι δακτύλιοι D και D' λέγονται **ισόμορφοι** και συμβολίζονται $D \cong D'$**.**

Σύμφωνα λοιπόν με τον ορισμό που δόθηκε μπορούμε να συμπεράνουμε ότι ο ομομορφισμός των δακτυλίων είναι μια **απεικόνιση που διατηρεί τη δομή**. Αυτό είναι εμφανές από την συσχέτιση που υπάρχει στην προσθετική καθώς και στην πολλαπλασιαστική ιδιότητά τους. Ακόμη για έναν ισομορφισμό $D \cong D'$ παρατηρούμε ότι ισχύουν οι εξής σχέσεις:

- $D \cong D$, μέσω της ταυτοτικής απεικόνισης.
- Αν $D \cong D'$ τότε $D' \cong D$, μέσω της αντίστροφης απεικόνισης.
- Αν $D \cong D'$ και $D' \cong D''$ τότε $D \cong D''$, επειδή η σύνθεση ισομορφισμών είναι ισομορφισμός.

Επομένως ο ισομορφισμός έχει όλες τις ιδιότητες μιας σχέσης ισοδυναμίας στην «κλάση» όλων των δακτυλίων. Δεν χρησιμοποιούμε την έκφραση «στο σύνολο των δακτυλίων» επειδή αυτό δεν είναι επιτρεπτό στην συνολοθεωρία που αναπτύσσεται στο αξιωματικό σύστημα των Zermelo – Fraenkel.

Ορισμός 2.2: Για κάθε ομομορφισμό φ ενός δακτυλίου D σε έναν δακτύλιο D', το σύνολο $\varphi(D) = \{\varphi(\alpha)/\alpha \in D\} = \{\alpha' \in D'/\text{υπάρχει } \alpha \in D \text{ ώστε } \alpha' = \varphi(\alpha)\}$ καλείται **εικόνα του ομομορφισμού φ** και συμβολίζεται με **Imφ**.

Ως **παράδειγμα** ομομορφισμού θα χρησιμοποιήσουμε μια απεικόνιση που συνδέει τον δακτύλιο των πραγματικών ακεραίων $\mathbb{Z}$ με τον δακτύλιο $\mathbb{Z}_n$. Ο τελευταίος αποτελείται από το σύνολο

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\},$$

που περιέχει όλα τα δυνατά υπόλοιπα κάθε ακεραίου, κατά την διαίρεσή του με κάποιον ακέραιο $n > 1$. Κάθε στοιχείο $x \in \mathbb{Z}_n$ είναι ο αντιπρόσωπος μιας κλάσης ισοδυναμίας (δηλαδή κανονικά θα έπρεπε να γράφεται ως $[x]$) όλων των ακεραίων m που αν διαιρεθούν με τον n θα δώσουν ως υπόλοιπο τον

x. Οι ακέραιοι αυτοί καλούνται ισοϋπόλοιποι του x κατά modulo n και όπως άλλωστε έχουμε δει στο θεώρημα 1.13 θα συμβολίζουμε $m \equiv x(\mathrm{mod} n)$ αν και μόνο αν $n/(m - x)$. Επίσης ως πράξεις της δομής αυτής χρησιμοποιούμε αφενός την πρόσθεση: $\alpha + \beta$ = υπόλοιπο της διαίρεσης του $\alpha + \beta$ με τον n και αφετέρου τον πολλαπλασιασμό: $\alpha \cdot \beta$ = υπόλοιπο της διαίρεσης του $\alpha \cdot \beta$ με τον n, για κάθε στοιχείο $\alpha, \beta \in \mathbb{Z}_n$. Εύκολα τώρα μπορούμε να διαπιστώσουμε ότι η δομή $<\mathbb{Z}_n, +, \cdot>$ αποτελεί έναν δακτύλιο με μηδενικό στοιχείο το 0, αντίθετο για κάθε $x \in \mathbb{Z}_n$ το $n - x \in \mathbb{Z}_n$ και αντιστρέψιμο στοιχείο το $1 \in \mathbb{Z}_n$.

Αν λοιπόν ορίσουμε την απεικόνιση $f: \mathbb{Z} \to \mathbb{Z}_n$ με $f(m) = \upsilon$, όπου υ το υπόλοιπο που δίνει ο αλγόριθμος της διαίρεσης του $m \in \mathbb{Z}$ με το n, τότε για κάθε ακέραιο α, β από τον αλγόριθμο της διαίρεσης έχουμε:

- $\alpha = \kappa n + \upsilon_1$ και $\beta = \lambda n + \upsilon_2$, με $0 \le \upsilon_i < n$ για $i = 1, 2$. Προσθέτοντας:
$$\alpha + \beta = (\kappa + \lambda)n + \upsilon_1 + \upsilon_2.$$
Αν $\upsilon_1 + \upsilon_2 = \mu n + \upsilon_3$, με $0 \le \upsilon_3 < n$, τότε:
$$\alpha + \beta = (\kappa + \lambda + \mu)n + \upsilon_3.$$
Από τα παραπάνω βλέπουμε ότι $f(\alpha) + f(\beta) = \upsilon_1 + \upsilon_2 = \upsilon_3 = f(\alpha + \beta)$.
- Αντίστοιχα τώρα αν πολλαπλασιάσουμε αντί να προσθέσουμε τις δύο αρχικές ισότητες είναι:
$$\alpha\beta = (\kappa\lambda + \kappa\upsilon_2 + \lambda\upsilon_1)n + \upsilon_1\upsilon_2.$$
Αν $\upsilon_1\upsilon_2 = \mu' n + \upsilon_3'$, με $0 \le \upsilon_3' < n$, τότε:
$$\alpha\beta = (\kappa\lambda + \kappa\upsilon_2 + \lambda\upsilon_1 + \mu')n + \upsilon_3'.$$
Οπότε $f(\alpha)f(\beta) = \upsilon_1\upsilon_2 = \upsilon_3' = f(\alpha + \beta)$.

Συνεπώς η απεικόνιση f αποτελεί έναν ομομορφισμό των δακτυλίων $\mathbb{Z}$ και $\mathbb{Z}_n$. Ας κρατήσουμε όμως από το παράδειγμα αυτό και κάτι άλλο που είναι ιδιαίτερα σημαντικό. Ο ομομορφισμός αυτός συνέδεσε δύο δακτυλίους από τους οποίους ο μεν πρώτος έχει μη πεπερασμένου πλήθους στοιχείων ενώ ο δεύτερος έχει πεπερασμένου πλήθους, οπότε είναι πιο εύκολα προσβάσιμος.

Θεώρημα 2.1: Σε έναν ομομορφισμό δακτυλίων $\varphi: D \to D'$ ισχύουν οι παρακάτω ιδιότητες:

(1) Αν το μηδενικό του D είναι 0 και $0'$ το μηδενικό του D' τότε $\varphi(0) = 0'$.

(2) Αν $\alpha \in D$ με αντίθετο το $-\alpha$, τότε $\varphi(-\alpha) = -\varphi(\alpha)$.

(3) Αν $1, 1'$ αντιστρέψιμα του D, D' αντίστοιχα και $\varphi(1) \neq 0'$ τότε $\varphi(1) = 1'$.

(4) Αν ο H είναι υποδακτύλιος του D τότε ο $\varphi(H)$ είναι υποδακτύλιος του D'. Δηλαδή οι υποδακτύλιοι αντιστοιχούν σε υποδακτυλίους.

Απόδειξη: Οι δακτύλιοι D, D' είναι εφοδιασμένοι με τις πράξεις που έχουμε εμφανίσει στον ορισμό του ομομορφισμού.

(1) $\varphi(0) = \varphi(0 \oplus 0) = \varphi(0) + \varphi(0)$. Απλοποιώντας μεταξύ του πρώτου και του τελευταίου μέλους έχουμε $\varphi(0) = 0'$.

(2) Από το προηγούμενο είναι $0' = \varphi(0) = \varphi(\alpha \oplus (-\alpha)) = \varphi(\alpha) + \varphi(-\alpha)$. Από το μονοσήμαντο του αντίθετου είναι $\varphi(-\alpha) = -\varphi(\alpha)$.

(3) Για $\alpha \in D$ είναι: $\varphi(\alpha) = \varphi(1 \otimes \alpha) = \varphi(\alpha \otimes 1) = \varphi(1) \times \varphi(\alpha) = \varphi(\alpha) \times \varphi(1)$. Αν $\varphi(1) \neq 0'$ τότε $\varphi(1) = 1'$.

(4) Έστω $\varphi(\alpha)$ και $\varphi(\beta)$ είναι δύο στοιχεία του $\varphi(H)$, τότε ισχύει $\varphi(\alpha) + \varphi(\beta) = \varphi(\alpha \oplus \beta) \in \varphi(H)$ και $\varphi(\alpha) \times \varphi(\beta) = \varphi(\alpha \otimes \beta) \in \varphi(H)$. Άρα το $\varphi(H)$ είναι κλειστό και ως προς τις δύο πράξεις. Επίσης λόγω των (1), (2) και (3) ο $\varphi(H)$ είναι υποδακτύλιος του D'. ♦

Με αντίστοιχο τρόπο όπως της ιδιότητας (4) μπορούμε να δείξουμε ότι αν ο H' είναι υποδακτύλιος του D' τότε η αντίστροφη εικόνα του $\varphi^{-1}(H')$ θα είναι υποδακτύλιος του D. Η έννοια της αντίστροφης εικόνας ενός ομομορφισμού ορίζεται αντίστοιχα με τον ορισμό που δόθηκε για την εικόνα, κάνοντας χρήση της αντίστροφης απεικόνισης, που την συμβολίζουμε με φ^{-1}. Επίσης άμεσα από την ιδιότητα (4) συμπεραίνουμε ότι η εικόνα $\mathrm{Im}\varphi$ ενός ομομορφισμού $\varphi: D \to D'$ είναι υποδακτύλιος του D.

Ορισμός 2.3: Έστω η $\varphi: D \to D'$ είναι ομομορφισμός δακτυλίων. Ο υποδακτύλιος $\varphi^{-1}(\{0'\}) = \{\alpha \in D / \varphi(\alpha) = 0'\}$, δηλαδή όλα τα στοιχεία του D που απεικονίζονται μέσω της φ στο μηδενικό στοιχείο $0'$ του D', ονομάζεται **πυρήνας** (Kernel) του φ και συμβολίζεται με **Ker(φ).**

Επειδή μέσω ενός ομομορφισμού δυο δακτυλίων μπορούμε να απεικονίσουμε πολλά διαφορετικά στοιχεία του πρώτου στο μηδενικό του δεύτερου, τότε το πλήθος των στοιχείων του πυρήνα μας δίνει το ποσοστό της συγκέντρωσης των στοιχείων του αρχικού δακτυλίου τα οποία απεικονίζονται στο μηδενικό του δεύτερου δακτυλίου. Ας επανέλθουμε όμως στο **παράδειγμα** που δώσαμε στην αρχή του κεφαλαίου. Είναι εύκολο να δούμε ότι ο ομομοφρισμός $f: \mathbb{Z} \to \mathbb{Z}_n$ έχει ως πυρήνα τον:

$$Ker(f) = f^{-1}(0) = \{. . ., -3n, -2n, -n, 0, n, 2n, 3n, . . .\} = n\mathbb{Z}.$$

Έχουμε κατά αυτόν τον τρόπο μια εικόνα της συγκέντρωσης των στοιχείων του $\mathbb{Z}$ στο μηδενικό του $\mathbb{Z}_n$.

Ορισμός 2.4: Θεωρούμε έναν δακτύλιο $<D, +, \cdot>$ και τον υποδακτύλιό του H, αν $x \in D$ τότε το σύνολο:

$$x + H = \{x + h / h \in H\}$$

λέγεται **σύμπλοκο** (coset) του υποδακτυλίου H με αντιπρόσωπο το x και είναι υποσύνολο του D. Επειδή επίσης η ομάδα $(D, +)$ είναι αβελιανή ισχύει ότι $x + H = H + x$. Το σύνολο που περιέχει όλα τα σύμπλοκα της H το συμβολίζουμε $\mathbf{D/H = \{x + H / x \in D\}}$.

Σύμφωνα με τον παραπάνω ορισμό σε έναν ομομορφισμό $\varphi: D \to D'$ αν επιλέξουμε ως $H = Ker(\varphi)$ και $x \in D$ τότε $\varphi^{-1}\{\varphi(x)\} = \{\alpha \in D / \varphi(\alpha) = \varphi(x)\} = x \oplus H$. Συνεπώς μπορούμε να συμπεράνουμε ότι:

- Το μέγεθος του πυρήνα του ομομορφισμού $Ker(\varphi)$ στην πραγματικότητα μετράει το ποσοστό της συγκέντρωσης, μέσω της φ, σε κάθε στοιχείο της εικόνας $Im\varphi$ της D'.
- Ο φ είναι μονομορφισμός αν και μόνο αν ο $Ker(\varphi)$ περιέχει μόνο το μηδενικό στοιχείο του D.

Θεώρημα 2.2: Έστω δακτύλιος $<D, +, \cdot>$ με υποδακτύλιο του τον H, για τα $x, y \in D$ ισχύει ότι $x + H = y + H$ αν και μόνο αν $x - y \in H$.

Απόδειξη: Αφού ισχύει $x + H = y + H$ και επειδή $x + 0 = x \in x + H$, τότε το $x \in y + H$. Δηλαδή:

$$x = y + h \text{ με } h \in H. \text{ Άρα } x - y = h \in H.$$

Αντίστροφα επειδή $x - y \in H$ το $x - y = h \in H$. Αν θεωρήσουμε ότι για ένα $\omega \in x + H$ είναι $\omega = x + h_1$, με $h_1 \in H$ δηλαδή:

$$\omega = y + h + h_1 \text{ ή } \omega \in y + H.$$

Άρα $x + H \subseteq y + H$. Αντίστοιχα αποδεικνύουμε ότι $y + H \subseteq x + H$. Οπότε από τα παραπάνω ισχύει ότι $x + H = y + H$. ♦

Θεώρημα 2.3: Έστω δακτύλιος $<D, +, \cdot>$ με υποδακτύλιο του τον H, για τα $x, y \in D$ είναι $x + H = y + H$ είτε $(x + H) \cap (y + H) = \varnothing$.

Απόδειξη: Ας υποθέσουμε αρχικά ότι $(x + H) \cap (y + H) \neq \varnothing$, τότε θα υπάρχει ένα στοιχείο $\omega \in (x + H) \cap (y + H)$ και επομένως:

$$\omega = x + h_1 = y + h_2, \text{ με } h_1, h_2 \in H,$$

$$\text{δηλαδή } x - y = h_2 - h_1 \in H.$$

Οπότε από θεώρημα 2.2 έχουμε $x + H = y + H$. Στην άλλη περίπτωση ισχύει ότι $(x + H) \cap (y + H) = \varnothing$. ♦

Η γραφική ερμηνεία που θα μπορούσαμε να δώσουμε για την μορφή του συμπλόκου $x + H$ είναι ως την παράλληλη μεταφορά του αρχικού δακτυλίου κατά x.

2.2 Δακτύλιοι Πηλίκα

Στο τέλος της προηγούμενης παραγράφου είχαμε ορίσει ένα σύνολο που περιέχει όλα τα σύμπλοκα ενός υποδακτυλίου ο οποίος προέρχεται από έναν αρχικό δακτύλιο. Στην παράγραφο αυτή θα ξεκινήσουμε επιχειρώντας να δημιουργήσουμε μια δομή για το σύνολο αυτό και να την συσχετίσουμε με τον αρχικό δακτύλιο.

Θεώρημα 2.4: Έστω ένας δακτύλιος D και ο υποδακτύλιος του H, τότε η πράξη του πολλαπλασιασμού των συμπλόκων είναι καλά ορισμένη μέσω της ισότητας:

$$(x + H) \otimes (y + H) = (xy) + H,$$

αν και μόνο αν για κάθε $x, y \in D$ και $h \in H$ τα $xh, hy \in H$.

Απόδειξη: Για να δείξουμε ότι ο πολλαπλασιασμός είναι καλά ορισμένος θα χρησιμοποιήσουμε αντιπροσώπους. Αν λοιπόν επιλέξουμε τα στοιχεία h_1, h_2 που περιέχονται στον υποδακτύλιο H, τότε το $x + h_1$ είναι ο

αντιπρόσωπος του συμπλόκου $x + H$ ενώ αντίστοιχα το $y + h_2$ θα είναι του $y + H$, με $x, y \in D$. Επομένως ισχύει ότι:

$$(x + h_1) \otimes (y + h_2) = xy + xh_2 + h_1y + h_1h_2.$$

Όμως το $(xh_2 + h_1y + h_1h_2) \in H$ οπότε $(x + h_1) \otimes (y + h_2) \in (xy) + H$.

Αντίστροφα αν δεχθούμε ότι ο πολλαπλασιασμός είναι καλά ορισμένος και επιλέξουμε ένα στοιχείο $x \in (x + H)$ και $h \in H$ τότε από το γινόμενο:

$$(x + H) \oplus H = x0 + H = H, \text{ ισχύει ότι } xh \in H.$$

Αντίστοιχα με τη βοήθεια του γινομένου $H \oplus (y + H) = H$ και $h \in H$, δείχνουμε ότι το $hy \in H$. ♦

Θεώρημα 2.5: Θεωρούμε έναν δακτύλιο D και H έναν υποδακτύλιο του D, ώστε για κάθε $x, y \in D$, $h \in H$ τα $xh, hy \in H$. Στο σύνολο των σύμπλοκων D/H ορίζουμε τις εξής πράξεις:

Πρόσθεση: $(x + H) \oplus (y + H) = (x + y) + H$.

Πολλαπλασιασμό: $(x + H) \otimes (y + H) = (xy) + H$.

Το D/H αποτελεί δακτύλιο.

Απόδειξη: Αρχικά θα ασχοληθούμε με την πράξη της πρόσθεσης, η οποία έχει δοθεί με επιλογή στοιχείων. Συνεπώς το πρωτεύον που πρέπει να δείξουμε είναι η ανεξαρτησία της πράξης αυτής από τις συγκεκριμένες επιλογές, δηλαδή αν είναι **καλά ορισμένη**.

Έστω ότι ισχύουν:

$(x + H) \oplus (y + H) = (x + y) + H$ και $(x' + H) \oplus (y' + H) = (x' + y') + H$.

Αρκεί όταν ισχύει $x + H = x' + H$ και $y + A = y' + H$ να αποδείξουμε ότι:

$$(x + y) + H = (x' + y') + H.$$

Από το ευθύ και το αντίστροφο του θεωρήματος 2.2 έχουμε ότι $x - x' \in H$ και $y - y' \in H$ και επειδή ο H είναι υποδακτύλιος του D συμπεραίνουμε πως τα στοιχεία $(x + y), (-x' - y') \in H$. Επομένως:

$$(x + y) - (x' + y') \in H \text{ ή } (x + y) + H = (x' + y') + H.$$

Η **προσεταιριστικότητα** και η **αντιμεταθετικότητα** που διέπουν την πράξη της πρόσθεσης προκύπτουν άμεσα από τις αντίστοιχες ιδιότητες του δακτυλίου D, ως εξής:

- $(x + H) \oplus [(y + H) \oplus (z + H)] = (x + H) \oplus [(y + z) + H)] = (x + y + z) + H = [(x + y) + z] + H = [(x + y) + H] \oplus (z + H) = [(x + H) \oplus (y + H)] \oplus (z + H)$.
- $(x + H) \oplus (y + H) = (x + y) + H = (y + x) + H = (y + H) \oplus (x + H)$.

Όσον αφορά τώρα το **μηδενικό στοιχείο**, είναι το **(0 + H)**, αφού

$$(x + H) \oplus (0 + H) = (x + 0) + H = x + H.$$

Όπως επίσης για την ύπαρξη του **αντίθετου στοιχείου** του $(x + H)$ έχουμε το $(-x + H)$, μια και ισχύει:

$$(x + H) \oplus (-x + H) = (x - x) + H = 0 + H.$$

Για τον πολλαπλασιασμό έχουμε ήδη αποδείξει ότι είναι καλά ορισμένος στο θεώρημα 2.4, οπότε απομένει να δούμε αν ισχύουν οι επόμενες ιδιότητες.

Για την **προσεταιριστική ιδιότητα του πολλαπλασιασμού**, όπως και για τον **επιμεριστικό νόμο** θα δειχθούν άμεσα:

- $(x + H) \otimes [(y + H) \otimes (z + H)] = (x + H) \otimes [(yz) + H)] = (xyz) + H = (x\ y)z + H = [(xy) + H] \otimes (z + H) = [(x + H) \otimes (y + H)] \otimes (z + H)$.
- $(x + H) \otimes [(y + H) \oplus (z + H)] = (x + H) \otimes [(y + z) + H)] = x(y + z) + H = (xy + xz) + H = [(xy) + H] \oplus [(xz) + H] = [(x + H) \otimes (y + H)] \oplus [(x + H) \otimes (z + H)]$.

Συνεπώς το $D/H = \{x + H / x \in D\}$ εφοδιασμένο με τις πράξεις $\oplus, \otimes$ αποτελεί έναν δακτύλιο. ♦

Στα δύο θεωρήματα που προηγήθηκαν παρατηρούμε ότι για να οροθετηθεί σωστά η πράξη του πολλαπλασιασμού, οπότε κατ' επέκταση και η θεμελίωση του δακτύλιου D/H απαιτήθηκαν οι προϋποθέσεις $xH \subseteq H$ και $Hy \subseteq H$ για κάθε $x, y \in D$, όπου $xH = \{xh / h \in H\}$ και $Hy = \{hy / h \in H\}$. Οι υποδομές που πληρούν αυτές ακριβώς τις συνθήκες είναι αξιοσημείωτες, γιαυτό και θα τις διαχωρίσουμε. Τις συμβολίζουμε με I και θα οριστούν αμέσως παρακάτω.

Ορισμός 2.5: Κάθε υποδακτύλιος I ενός δακτυλίου D που έχει την ιδιότητα:

$$xI \subseteq I \text{ και } Iy \subseteq I \text{ για κάθε } x, y \in D,$$

ονομάζεται **ιδεώδες** (ideal) του D.

Σύμφωνα με τον ορισμό των ιδεωδών ενός δακτυλίου μπορούμε να κάνουμε τις ακόλουθες τρεις παρατηρήσεις.

- Σε κάθε δακτύλιο D υπάρχουν πάντα τουλάχιστον δύο ιδεώδη. Το μη γνήσιο $I = D$ και το τετριμμένο $I = 0$. Κάθε άλλο ιδεώδες $I \neq D$ και $I \neq 0$ θα το αποκαλούμε **γνήσιο και μη τετριμμένο.**
- Αν τα I και J είναι ιδεώδη ενός δακτυλίου D, τότε είναι επίσης ιδεώδη του και τα $I \cap J$, $I + J$ και $I \cdot J$. Μάλιστα ισχύουν μεταξύ τους και οι σχέσεις: $I \subseteq I + J$, $J \subseteq I + J$ και $I \cdot J \subseteq I \cap J$.
- Τέλος αν ο $\varphi: D \to D'$ είναι ένας ομομορφισμός των δύο δακτυλίων, τότε ο πυρήνας του $\mathrm{Ker}(\varphi)$ αποτελεί ιδεώδες του D.

Αν και ο πρώτος που χρησιμοποίησε τον όρο δακτύλιος ήταν ο Hilbert το 1897 στο «Zahlbericht», ο όρος ιδεώδες προϋπήρχε. Ο Kummer το 1847 είχε εισαγάγει την έννοια του «ιδεώδους μιγαδικού αριθμού» με σκοπό να δείξει την μοναδικότητα παραγοντοποίησης σε κάποιους δακτυλίους αλγεβρικών ακεραίων. Από αυτό προέκυψε και η έννοια του «ιδεώδους αριθμού», που απέχει αρκετά από το νόημα του «αριθμού», το οποίο χρησιμοποίησε ο Dedekind με σκοπό να ορίσει τις έννοιες του πρώτου ιδεώδους και το γινόμενο ιδεωδών. Αποδεικνύοντας κατά αυτόν τον τρόπο ουσιαστικά και τον ορισμό που δώσαμε προηγουμένως.

Ορισμός 2.6: Θεωρούμε ένα ιδεώδες I ενός δακτυλίου D. Τα σύμπλοκα του I σχηματίζουν έναν δακτύλιο **D/I** (από θεώρημα 2.5) με πράξεις τις:

$$\text{Πρόσθεση: } (x + I) + (y + I) = (x + y) + I.$$

$$\text{Πολλαπλασιασμό: } (x + I)\cdot(y + I) = (xy) + I.$$

Ο δακτύλιος αυτός ονομάζεται **δακτύλιος πηλίκο του D προς I** (quotient ring) ή δακτύλιος πηλίκο του D modulo I.

Άμεσα συμπεράσματα που συνάγονται είναι ότι αν ο D έχει μοναδιαίο στοιχείο τότε και ο D/I θα έχει. Όπως επίσης αν ο D είναι αντιμεταθετικός το ίδιο θα συμβαίνει και για τον D/I. Στην περίπτωση τώρα του μη γνήσιου ιδεώδους $I = D$, ο δακτύλιος πηλίκο που προκύπτει είναι ο D/D και περιέχει ένα μόνο στοιχείο, το μηδενικό. Επίσης στην περίπτωση του τετριμμένου ιδεώδους $I = 0$, ο δακτύλιος πηλίκο είναι ο $D/\{0\}$ που είναι ισόμορφος με τον D. Δύο περιπτώσεις οι οποίες γενικά δεν παρουσιάζουν ιδιαίτερο

ενδιαφέρον. Αντίθετα όμως οι απεικονίσεις που θα οριστούν με τα επόμενα θεωρήματα είναι εξαιρετικά σημαντικές. Όπως θα δούμε αναλύουν έναν ομομορφισμό που συνδέει δύο δακτυλίους με την βοήθεια ενός πολύ σημαντικού δακτυλίου πηλίκου.

Θεώρημα 2.6: Για το ιδεώδες I του δακτυλίου D η απεικόνιση:

$$\psi: D \to D/I, \text{ ώστε } \psi(x) = x + I, \text{ με } x \in D,$$

είναι ένας ομομορφισμός δακτυλίων με $\text{Ker}(\psi) = I$.

Απόδειξη: Έστω τα στοιχεία x, y του D, τότε λόγω της απεικόνισης θα είναι:

$$\psi(x + y) = (x + y) + I = (x + I) + (y + I) = \psi(x) + \psi(y).$$

$$\text{Και } \psi(x \cdot y) = (x \cdot y) + I = (x + I) \cdot (y + I) = \psi(x) \cdot \psi(y).$$

Ο ψ είναι λοιπόν ομομορφισμός και μάλιστα αφού ισχύει ότι: $x + I = I$ αν και μόνο αν $x \in I$, τότε για τον πυρήνα του θα έχουμε:

$$\text{Ker}(\psi) = \{x \in D / \psi(x) = x + I\} = I. \qquad \blacklozenge$$

Το θεώρημα που ακολουθεί είναι το σημαντικότερο στην θεωρία των ομομορφισμών και αποτελεί και κριτήριο ελέγχου των ισομορφισμών.

Θεώρημα 2.7: (**Θεμελιώδες θεώρημα ομομορφισμών).** Θεωρούμε έναν ομομορφισμό δακτυλίων $\varphi: D \to D'$ με πυρήνα το $\text{Ker}(\varphi) = I$ και εικόνα του τον δακτύλιο $\varphi(D)$.

- Η απεικόνιση $\gamma: D/I \to \varphi(D)$ που ορίζεται από την σχέση $\gamma(x + I) = \varphi(x)$ είναι ισομορφισμός.
- Επίσης αν η $\psi: D \to D/I$, έτσι ώστε $\psi(x) = x + I$, είναι ομομορφισμός, τότε για κάθε $x \in D$ ισχύει ότι: $\varphi(x) = \gamma(\psi(x))$.

Απόδειξη: Ως γνωστών, αφού η $\varphi: D \to D'$ είναι ένας ομομορφισμός δακτυλίων, ο I θα είναι ιδεώδες του D και επομένως θα ορίζεται ο δακτύλιος πηλίκο D/I.

- Για $x, y \in I$, με $x + I = y + I$, από θεώρημα 2.2 $x - y \in I$. Δηλαδή είναι $\varphi(x - y) = \varphi(x) - \varphi(y) = 0$ ή $\varphi(x) = \varphi(y)$. Οπότε η γ είναι καλά ορισμένη.

  Έστω $x + I, y + I \in D/I$, τότε:

$$\gamma[(x + h) + (y + h)] = \gamma[(x + y) + h] = \varphi(x + y) =$$

$$= \varphi(x) + \varphi(y) = \gamma(x + h) + \gamma(y + h).$$

Όπως επίσης και

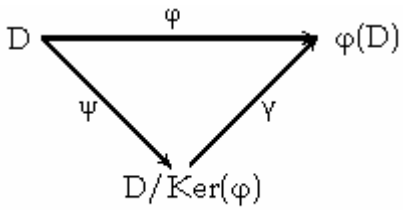
$\gamma[(x + h)\cdot(y + h)] = \gamma[(x\cdot y) + h] = \varphi(x\cdot y) = \varphi(x)\cdot\varphi(y) = \gamma(x + h)\cdot\gamma(y + h)$.

Επομένως η γ είναι ομομορφισμός δακτυλίων.

Αν τώρα $\gamma(x + I) = \gamma(y + I)$ τότε $\varphi(x) = \varphi(y)$ δηλαδή τα $(x + I), (y + I)$ είναι το ίδιο σύμπλοκο. Άρα η γ είναι «1-1». Έστω τέλος ότι $\omega \in \varphi(D)$, δηλαδή $\omega = \varphi(x)$, για κάποιο $x \in D$ και $\gamma(x + I) = \varphi(x) = \omega$. Η γ είναι και επί. Συνεπώς η απεικόνιση $\gamma: D/I \to \varphi(D)$ ώστε $\gamma(x + I) = \varphi(x)$ είναι ισομορφισμός δακτυλίων.

✦ Η απόδειξη του δεύτερου μέρους του θεωρήματος είναι άμεση συνέπεια των θεωρημάτων 2.6 και 2.7. ♦

Σύμφωνα λοιπόν με το θεώρημα που είδαμε, σε κάθε ομομορφισμό φ από ένα δακτύλιο D στον $\varphi(D)$ με πυρήνα τον $\mathrm{Ker}(\varphi)$ μπορούμε να ορίσουμε έναν δακτύλιο πηλίκο $D/\mathrm{Ker}(\varphi)$. Επίσης για κάθε δακτύλιο πηλίκο $D/\mathrm{Ker}(\varphi)$ έχουμε την δυνατότητα να ορίσουμε έναν νέο ομομορφισμό από τον D στον $D/\mathrm{Ker}(\varphi)$. Τέλος υπάρχει ένας ισομορφισμός που συνδέει τον $D/\mathrm{Ker}(\varphi)$ με τον $\varphi(D)$ ο οποίος ονομάζεται **κανονικός**. Οι δύο τελευταίες απεικονίσεις ορίζονται μοναδικά και είναι ιδιαίτερα βασικές. Διαγραμματικά μπορούμε να συνοψίσουμε όλες αυτές τις σχέσεις με το σχήμα 2.1.



Σχήμα 2.1

Μια άμεση συνέπεια των παραπάνω είναι το **τρίτο θεώρημα των ισομορφισμών** που αναφέρει ότι αν τα $I \subseteq J$ είναι ιδεώδη του D τότε το J/I είναι ιδεώδες του D/I και μάλιστα υπάρχει ισομορφισμός:

$$(D/I)/(J/I) \cong D/J.$$

Αυτό ισχύει γιατί και η $\varphi: D/I \to D/J$ με $\varphi(x + I) = x + J$ είναι επιμορφισμός με $\mathrm{Ker}(\varphi) = \{\alpha + I/\alpha \in J\} = J/I$.

Επιστρέφοντας στο **παράδειγμα** μας, έχουμε ήδη δει ότι για τον ομομορφισμό $f: \mathbb{Z} \to \mathbb{Z}_n$ ισχύει ότι $\mathrm{Ker}(f) = n\mathbb{Z} = \{kn/k \in \mathbb{Z}\}$, ο οποίος είναι

υποδακτύλιος του $\mathbb{Z}$. Το σύνολο των συμπλόκων του $n\mathbb{Z}$ είναι ένα σύνολο που θα περιέχει όλες τις κλάσεις υπολοίπων modulo n, δηλαδή το

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Επίσης γνωρίζουμε ότι ο $n\mathbb{Z}$ είναι αντιμεταθετικός δακτύλιος και προφανώς για κάθε $x, y \in \mathbb{Z}$ θα ισχύει ότι $x \cdot n\mathbb{Z} \subseteq n\mathbb{Z}$ και $n\mathbb{Z} \cdot y \subseteq n\mathbb{Z}$, δηλαδή ο $n\mathbb{Z}$ είναι ένα ιδεώδες του $\mathbb{Z}$. Συνεπώς ορίζεται ένας δακτύλιος πηλίκο από το σύνολο $\mathbb{Z}/n\mathbb{Z}$ επισυνάπτοντας τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, όπως τις έχουμε ήδη ορίσει.

Η απεικόνιση $q: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, με $q(m) = m + n\mathbb{Z}$ σύμφωνα με το θεώρημα 2.6 είναι ομομορφισμός δακτυλίων και είναι μοναδικά ορισμένη. Επίσης η απεικόνιση $g: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ με $g(m + \mathbb{Z}_n) = f(m) =$ το υπόλοιπο της διαίρεσης του m δια n (δηλαδή αντιστοιχεί σε κάθε σύμπλοκο του $n\mathbb{Z}$ το μικρότερο μη αρνητικό στοιχείο του), είναι ο κανονικός ισομορφισμός που έχουμε ήδη αναφέρει. Δηλαδή το θεώρημα 2.7 μας εξασφαλίζει ότι ο δακτύλιος $\mathbb{Z}/n\mathbb{Z}$ είναι ισόμορφος του δακτυλίου $\mathbb{Z}_n$. Παρατηρούμε λοιπόν ότι αυτό μας επιτρέπει να χρησιμοποιούμε τον δακτύλιο $\mathbb{Z}_n$ στην θέση του $\mathbb{Z}/n\mathbb{Z}$, δίνοντας μας έτσι την ευχέρεια να κινούμαστε μέσα σε έναν πιο χρηστικό δακτύλιο, με πεπερασμένο πλήθος στοιχείων.

2.3 Ιδιότητες Ιδεωδών

Η μελέτη των δακτυλίων πηλίκων παρουσιάζει πάντα ιδιαίτερο ενδιαφέρον, αφού συνήθως έχουν «καλύτερη» δομή από αυτή του αρχικού δακτυλίου. Πολλές φορές ο δακτύλιος πηλίκο έχει και επιπλέον ιδιότητες σε σχέση με τον δακτύλιο από τον οποίον έχει προέλθει. Αυτό όμως εξαρτάται σε μεγάλο βαθμό από την μορφή που έχει το ιδεώδες που χρησιμοποιούμε για την κατασκευή του. Ακολούθως θα εξετάσουμε κάποιες χαρακτηριστικές περιπτώσεις τέτοιων ιδεωδών αφού πρώτα τα ορίσουμε. Καθώς επίσης και των

αντίστοιχων δακτυλίων πηλίκων που παράγονται από αυτά, αποδεικνύοντας συγχρόνως τα θεωρήματα που τα συνδέουν.

Ορισμός 2.7: Ένα γνήσιο ιδεώδες I ενός δακτυλίου D ονομάζεται **πρώτο ιδεώδες** (prime ideal) αν για κάθε $\alpha, \beta \in D$ που ισχύει $\alpha \cdot \beta \in I$ τότε έχουμε $\alpha \in I$ ή $\beta \in I$.

Το θεώρημα που ακολουθεί εκτός από κριτήριο απόδειξης ενός ιδεώδους ότι είναι πρώτο αποτελεί και βασικό εργαλείο ελέγχου ώστε ένας δακτύλιος πηλίκο είναι ακέραια περιοχή.

Θεώρημα 2.8: Έστω D ένας αντιμεταθετικός δακτύλιος με μοναδιαίο και I ένα γνήσιο ιδεώδες του. Το I είναι πρώτο ιδεώδες του D αν και μόνο αν ο δακτύλιος πηλίκο D/I είναι ακέραια περιοχή.

Απόδειξη: Αν το I είναι ένα πρώτο ιδεώδες του D και $x, y \in D$ ώστε $(x + I)(y + I) = 0_{D/I}$ τότε $xy + I = I$, δηλαδή $xy \in I$ άρα $x \in I$ ή $y \in I$. Συνεπώς $x + I = 0_{D/I}$ ή $y + I = 0_{D/I}$.

Αντίστροφα όταν ο D/I είναι ακέραια περιοχή τότε $D/I \neq 0$ δηλαδή το $I \neq D$. Αν τα $x, y \in D$ με $xy \in I$ ώστε $xy + I = 0_{D/I}$ τότε έχουμε:

$$(x + I)(y + I) = 0_{D/I} \text{ δηλαδή } x + I = 0_{D/I} \text{ ή } y + I = 0_{D/I}.$$

Άρα $x \in I$ ή $y \in I$. ♦

Ορισμός 2.8: Ένα γνήσιο ιδεώδες I ενός δακτυλίου D ονομάζεται **μέγιστο** (maximal) αν δεν υπάρχει γνήσιο ιδεώδες που να το περιέχει και να είναι διαφορετικό του I. Δηλαδή το $I \neq D$ είναι μέγιστο, αν για το ιδεώδες J με $I \subseteq J$ τότε $J = I$ ή $J = D$.

Λήμμα 2.1: Αν το ιδεώδες I ενός δακτυλίου με μοναδιαίο D περιέχει αντιστρέψιμο στοιχείο, τότε $I = D$. Οπότε ένα σώμα δεν περιέχει γνήσια μη τετριμμένα ιδεώδη.

Απόδειξη: Έστω το αντιστρέψιμο στοιχείο του D $\alpha \in I$. Επειδή για κάθε $x \in D$ ισχύει $xI \subseteq I$ επιλέγουμε $x = \alpha^{-1} \in D$, οπότε και $1 = \alpha^{-1}\alpha \in I$. Όμως επειδή $dI \subseteq I$, για κάθε $d \in D$ έχουμε ότι $d1 = d \in I$ για κάθε $d \in D$. Συνεπώς $I = D$. ♦

Αφού κάθε μη μηδενικό στοιχείο ενός σώματος είναι αντιστρέψιμο τότε τα μοναδικά ιδεώδη που περιέχει θα είναι το μη γνήσιο και το τετριμμένο. Το

θεώρημα που ακολουθεί είναι αντίστοιχο του θεωρήματος 2.8 και είναι ένα από τα πιο σημαντικά θεωρήματα κυρίως στην θεωρία σωμάτων.

Θεώρημα 2.9: Έστω D ένας αντιμεταθετικός δακτύλιος με μοναδιαίο και I ένα γνήσιο ιδεώδες του. Το I είναι μέγιστο ιδεώδες του D αν και μόνο αν ο δακτύλιος πηλίκο D/I είναι σώμα.

Απόδειξη: Αν το I είναι ένα μέγιστο ιδεώδες του D και επειδή ο D/I είναι δακτύλιος πρέπει να δείξουμε την ύπαρξη αντίστροφου για το στοιχείο $(x + I) \in D/I$, υποθέτοντας ότι $x + I \neq 0_{D/I}$ άρα και $x \notin I$. Όμως επειδή το I είναι μέγιστο, τότε $I \subseteq Dx + I = D$. Συνεπώς $1 \in Dx + I$ και για κάποια στοιχεία $d \in D$ και $y \in I$ θα είναι: $1= dx + y$. Ισχύει λοιπόν ότι:

$$(d + I)(x + I) = dx + I = (1 – x) + I = 1 + I.$$

Άρα το αντίστροφο του $x + I$ υπάρχει και είναι το $d + I$.

Αντίστροφα αν το D/I είναι σώμα τότε $D/I \neq 0$ δηλαδή $I \neq D$. Έστω ένα ιδεώδες I' ώστε $I \subseteq I' \subseteq D$, θα δείξουμε ότι $I' = D$ οπότε το I θα είναι μέγιστο. Αν $I \neq I'$ τότε υπάρχει κάποιο $x' \in I'$ και $x' \notin I$ οπότε:

$$x' + I \neq 0_{D/I} \text{ και } (x' + I)(d + I) = 1 + I, \text{ με } d \in D.$$

Άρα $x'd – 1 \in I$ τότε $1 \in I'$ δηλαδή $I = D$, συνέπεια του Λήμματος 2.1. ♦

Από τα παραπάνω θεωρήματα μπορούμε να συμπεράνουμε ότι αν έχουμε ένα αντιμεταθετικό δακτύλιο D και ένα μέγιστο ιδεώδες του I, τότε ο δακτύλιος πηλίκο αφού είναι σώμα θα είναι και ακέραια περιοχή. Επομένως το I θα είναι και πρώτο ιδεώδες.

Συνοψίζοντας λοιπόν αυτά που έχουμε αποδείξει έως τώρα μπορούμε να έχουμε την ακόλουθη κωδικοποίηση συμπερασμάτων. Θεωρούμε έναν αντιμεταθετικό δακτύλιο D και τον ομομορφισμό $\varphi: D \to \varphi(D)$. Από το θεώρημα 2.7 γνωρίζουμε ότι $D/\text{Ker}(\varphi) \cong \varphi(D)$, οπότε θα ισχύει:

- Αν $\varphi(D)$ είναι σώμα τότε $\text{Ker}(\varphi)$ είναι μέγιστο ιδεώδες του D.
- Αν $\varphi(D)$ είναι ακέραια περιοχή τότε $\text{Ker}(\varphi)$ είναι πρώτο ιδεώδες του D.

Επανερχόμαστε τώρα στο **παράδειγμα** που έχουμε δώσει από την αρχή του κεφαλαίου, για να δούμε τι γίνεται όταν ο n είναι πρώτος ακέραιος. Θεωρούμε λοιπόν κάποιον πρώτο ακέραιο αριθμό p, τότε ο $\mathbb{Z}_p$ εκτός από

αντιμεταθετικός δακτύλιος με μοναδιαίο που προφανώς είναι, δεν μπορεί να έχει διαιρέτες του 0. Γιατί αν οι ακέραιοι $m, k \in \mathbb{Z}_p$ και $km = 0$ τότε αφού m πρώτος με τον p, τότε p/k δηλαδή $k = 0$. Αντίστοιχα αποδεικνύεται ότι $m = 0$. Συνεπώς ο $\mathbb{Z}_p$ είναι ακέραια περιοχή και αφού έχει πεπερασμένο πλήθος στοιχείων τότε θα είναι σώμα (αποτελεί ένα από τα πιο σημαντικά σώματα και ονομάζεται **πρώτο**).

Έχουμε όμως προηγουμένως αποδείξει ότι $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$, οπότε έπεται ότι και ο δακτύλιος πηλίκο $\mathbb{Z}/p\mathbb{Z}$ είναι σώμα. Επομένως από το θεώρημα 2.9 συμπεραίνουμε ότι το ιδεώδες $p\mathbb{Z}$ του αντιμεταθετικού δακτυλίου $\mathbb{Z}$ θα είναι μέγιστο.

Ορισμός 2.9: Έστω ο D είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $\alpha \in D$, τότε το ιδεώδες όλων των πολλαπλασίων του α δηλαδή το $\{x\alpha / x \in D\}$ είναι το **κύριο ιδεώδες που παράγεται από το α** (principal ideal is generated by α) και το συμβολίζομαι **<α>**. Ένα ιδεώδες I του D ονομάζεται κύριο αν $I = <\alpha>$ για κάποιο $\alpha \in D$.

Δηλαδή στο **παράδειγμα** μας το ιδεώδες $n\mathbb{Z}$, από τον τρόπο που έχει οριστεί, είναι κύριο ιδεώδες του $\mathbb{Z}$ το οποίο παράγεται από τον $n \in \mathbb{Z}$, οπότε συμβολίζεται και $\mathbf{n\mathbb{Z} = <n>}$.

Στην περίπτωση που ο D είναι ακέραια περιοχή και κάθε ιδεώδες του είναι κύριο τότε καλούμε τον D **περιοχή κύριων ιδεωδών.** Στην παράγραφο 1.3 με τον ορισμό 1.7 είχαμε δώσει την έννοια της Ευκλείδειας περιοχής με στόχο την μοναδικότητα ανάλυσης των ακεραίων Gauss. Με το επόμενο θεώρημα θα προσεγγίσουμε αυτή την έννοια από μια άλλη οδό.

Θεώρημα 2.10: Κάθε Ευκλείδεια περιοχή D είναι και περιοχή κυρίων ιδεωδών.

Απόδειξη: Θεωρούμε ότι η D έχει ως Ευκλείδεια συνάρτηση την $\varphi: D\backslash\{0\} \to \mathbb{N}^*$ και I ένα ιδεώδες της. Αν $I = \{0\}$ τότε $I = <0>$, δηλαδή κύριο. Αν $I \neq \{0\}$, τότε υπάρχει κάποιο μη μηδενικό $\beta \in I$, ώστε το $\varphi(\beta) < \varphi(x)$, για

κάθε $x \in I$. Έστω λοιπόν $\alpha \in I$ και επειδή ισχύει ο αλγόριθμος της διαίρεσης, θα υπάρχουν $\kappa, \upsilon \in D$ τέτοια ώστε:

$$\alpha = \beta\kappa + \upsilon, \text{ με } \upsilon = 0 \text{ είτε } \varphi(\upsilon) < \varphi(\beta).$$

Όμως $\upsilon = \alpha - \beta\kappa$ με $\alpha, \beta \in I$ συνεπώς και $\upsilon \in I$. Δηλαδή η σχέση $\varphi(\upsilon) < \varphi(\beta)$ αδύνατη. Επομένως $\upsilon = 0$ και $\alpha = \kappa\beta$ για κάθε $\alpha \in I$. Συνεπώς το $I = <\beta>$, είναι κύριο ιδεώδες. ♦

2.4 Η Διαίρεση στους Ακεραίους Gauss

Μετά την γοητευτική περιπλάνηση μας στα εύφορα πεδία της Άλγεβρας, θα σταματήσουμε για περαιτέρω ανάλυση στην ακέραια περιοχή του $\mathbb{Z}[i]$. Στο πρώτο κεφάλαιο στην προσπάθεια μας να διερευνήσουμε αυτούς τους αριθμούς και την παραγοντοποίησή τους αποδείξαμε κάποιες βασικές προτάσεις που αφορούν την διαιρετότητα μέσα στο σύνολο τους. Οι προτάσεις αυτές είναι χρήσιμες και απαραίτητες για την μελέτη της πράξης της διαίρεσης των ακεραίων Gauss, οπότε θα τις υπενθυμισθούν στα επόμενα βήματά μας.

Έστω λοιπόν οι μη μηδενικοί $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ και οι προερχόμενοι από αυτούς ακέραιοι Gauss $\alpha + \beta i$ και $\gamma + \delta i$. Η διαίρεση των δύο αυτών μιγαδικών αριθμών, όπως γνωρίζουμε θα είναι:

$$\frac{\alpha+\beta i}{\gamma+\delta i} = \frac{(\alpha+\beta i)(\gamma-\delta i)}{\gamma^2+\delta^2} = \frac{\alpha\gamma+\beta\delta}{\gamma^2+\delta^2} + \frac{\beta\gamma-\alpha\delta}{\gamma^2+\delta^2} i .$$

Το αποτέλεσμα της για να ανήκει στο $\mathbb{Z}[i]$ θα πρέπει προφανώς το πραγματικό και το φανταστικό του μέρος να είναι ακέραιοι. Κάτι τέτοιο δεν είναι πάντα εφικτό. Οπότε σαν πρώτο μας βήμα θα είναι να ελέγξουμε τις προϋποθέσεις που θα πρέπει να πληρούν δύο ακέραιοι Gauss ώστε να διαιρούνται μέσα στο $\mathbb{Z}[i]$.

Θεώρημα 2.11: Ένας ακέραιος Gauss $\alpha = x + yi$, με $x, y \in \mathbb{Z}$ διαιρείται από έναν πραγματικό μη μηδενικό ακέραιο β αν και μόνο αν τα πηλίκα των διαιρέσεων β/x και β/y ανήκουν στο $\mathbb{Z}$.

Απόδειξη: Από το ορισμό 1.2 για να ισχύει β/α στο $\mathbb{Z}[i]$ πρέπει και αρκεί $x + yi = \beta(\kappa + \lambda i)$, με $\kappa, \lambda \in \mathbb{Z}$. Επομένως ισχύει ότι $x = \beta\kappa$ και $y = \beta\lambda$ ή β/x και β/y ανήκουν στο $\mathbb{Z}$. ♦

Θεώρημα 2.12: Για δύο μη μηδενικούς ακέραιους Gauss α, β αν β/α τότε $N(\beta)/N(\alpha)$ ανήκει στο $\mathbb{Z}$.

Απόδειξη: Αφού υπάρχει κάποιος ακέραιος Gauss γ έτσι ώστε $\alpha = \beta\gamma$, τότε θα ισχύει και η αντίστοιχη ισότητα των στάθμεων τους, δηλαδή $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Επομένως $N(\beta)/N(\alpha)$ ανήκει στο $\mathbb{Z}$. ♦

Το θεώρημα αυτό μπορεί να μας δώσει ένα κριτήριο για το πότε ένας ακέραιος Gauss δεν διαιρεί κάποιον άλλον, μεταφέροντας το πρόβλημα σε ένα απλό πλέον θέμα διαιρετότητας πραγματικών ακεραίων. Επίσης φυσικά το αντίστροφο δεν ισχύει, γιατί αν πάμε στην διαίρεση που δείξαμε αρχικά και δεχθούμε ότι ισχύει $N(\gamma + \delta i)/N(\alpha + \beta i)$ οπότε και $(\gamma^2 + \delta^2)/(\alpha^2 + \beta^2)$ τότε δεν σημαίνει απαραίτητα ότι ισχύουν συγχρόνως $(\gamma^2 + \delta^2)/(\alpha\gamma + \beta\delta)$ και $(\gamma^2 + \delta^2)/(\beta\gamma - \alpha\delta)$. Επομένως στην περίπτωση που γνωρίζουμε ότι οι στάθμες δύο ακεραίων Gauss διαιρεί η μια την άλλη, η μόνη μέθοδος για να ελέγξουμε αν διαιρούνται και οι ίδιοι οι ακέραιοι Gauss δεν είναι άλλη παρά η εκτέλεση της διαίρεσης.

Γενικά λοιπόν μπορούμε να πούμε ότι η διαίρεση μεταξύ δύο στοιχείων του $\mathbb{Z}[i]$ θα γίνεται σύμφωνα με τον αλγόριθμο που αποδείξαμε στο θεώρημα 1.6 και αναφέρει ότι:

«Για δύο ακεραίους Gauss α, β, με $\beta \neq 0$ υπάρχουν $\kappa, \upsilon \in \mathbb{Z}[i]$,

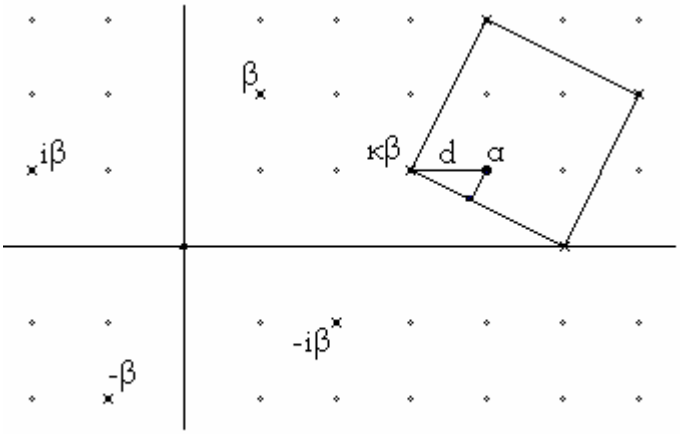
τέτοιοι ώστε $\alpha = \kappa\beta + \upsilon$ και $N(\upsilon) < N(\beta)$».

Ο μεν κ θα ονομάζεται πηλίκο και ο υ υπόλοιπο της διαίρεσης. Όπως ήδη έχουμε δει στην απόδειξη του συγκεκριμένου θεωρήματος η επιλογή του κ και επομένως και του υ μπορεί να μην είναι μονοσήμαντη. Αυτό βέβαια δεν σημαίνει ότι περιορίζεται η χρησιμότητά του αλγόριθμου, αρκεί βέβαια για οποιαδήποτε επιλογή και να κάνουμε να ισχύει ο περιορισμός που προϋποθέτετε για τη στάθμη του υπόλοιπου.

Εκτός από την αλγεβρική απόδειξη του αλγόριθμου που έχουμε αναφέρει, μια γραφική προσέγγιση της είναι αυτή που παρουσιάζεται παρακάτω. Στην παράγραφο 1.7 έχουμε ήδη δει ότι οι πολλαπλάσιοι ενός ακεραίου Gauss β, για τους οποίους προφανώς ισχύει ότι:

$$\beta\mathbb{Z}[i] = \{\beta\kappa / \kappa \in \mathbb{Z}[i]\} \subseteq \mathbb{Z}[i],$$

αποτελούν κορυφές τετραγώνων σε ένα διχτυωτό πλέγμα όπως του σχήματος 1.2. Μέσα από αυτό το υποσύνολο μπορούμε να επιλέξουμε τον ακέραιο Gauss $\kappa\beta$ που αποτελεί την πλησιέστερη κορυφή του τετράγωνου εντός ή πάνω στο οποίο ανήκει ο α. Το μήκος της πλευράς όλων των τετραγώνων θα είναι ίσο με $\sqrt{N(\beta)}$ και η απόσταση από τις εικόνες των α και $\kappa\beta$ θα είναι ίση με $d = |\alpha - \kappa\beta|$. Όπως φαίνεται και στο σχήμα 2.2 η d είναι η υποτείνουσα ενός ορθογωνίου τριγώνου με κάθετες πλευρές μικρότερες ή ίσες του $\frac{1}{2}\sqrt{N(\beta)}$. Όμως λόγω της τριγωνικής ανισότητας γνωρίζουμε ότι ισχύει $d < \sqrt{N(\beta)}$, οπότε επιλέγουμε ως υπόλοιπο το αριθμό $\upsilon = \alpha - \beta\kappa$, που προφανώς ανήκει στο $\mathbb{Z}[i]$. Επομένως η σχέση επαληθεύεται όπως ακριβώς απαιτείται, δηλαδή $\alpha = \beta\kappa + \upsilon$ με $N(\upsilon) < N(\beta)$.



Σχήμα 2.2

Επειδή όμως η επιλογή του υπολοίπου δεν είναι μονοσήμαντη μπορούμε για τη στάθμη του υπολοίπου να επιτύχουμε και ακόμη πιο περιοριστική ανισότητα. Αν εφαρμόσουμε το Πυθαγόρειο Θεώρημα στο ορθογώνιο τρίγωνο που αναφέραμε πιο πάνω βλέπουμε ότι:

$$N(\upsilon) = d^2 \le \left(\frac{\sqrt{N(\beta)}}{2}\right)^2 + \left(\frac{\sqrt{N(\beta)}}{2}\right)^2 = \frac{1}{2}N(\beta).$$

Δηλαδή η επιλογή του υπολοίπου υ ουσιαστικά δύναται να είναι τέτοια ώστε να έχουμε: $N(\upsilon) \le \frac{1}{2}N(\beta)$.

Ας δούμε και στην πράξη μια τέτοια διαίρεση. Θεωρούμε τους ακεραίους Gauss $\alpha = 41 + 24i$ και $\beta = 11 - 2i$, με $N(\beta) = 125$, τότε η διαίρεση τους δίνει:

$$\frac{\alpha}{\beta} = \frac{403}{125} + \frac{346}{125}i.$$

Αν εκτελέσουμε τις επιμέρους διαιρέσεις που προκύπτουν έχουμε 403:125 = 3,224… και 346:125 = 2,768…. Ο πλησιέστερος ακέραιος και για στους δύο είναι ο 3. Επομένως επιλέγουμε ως πηλίκο τον ακέραιο $\kappa = 3 + 3i$. Τότε το υπόλοιπο θα είναι $\upsilon = \alpha - \kappa\beta = (41 + 24i) - (11 - 2i)(3 + 3i) = 2 - 3i$, για το οποίο ισχύει ότι $N(\upsilon) = 13 < \frac{1}{2}N(\beta)$.

2.5 Ιδεώδη του $\mathbb{Z}[i]$.

Στην προηγούμενη παράγραφο αναφερθήκαμε στο διχτυωτό πλέγμα των τετραγώνων, που σχηματίζεται στο μιγαδικό επίπεδο, από τα πολλαπλάσια ενός ακεραίου Gauss. Οι κορυφές όλων αυτών των τετραγώνων, όπως είπαμε, δημιουργούν ένα σύνολο, το οποίο είναι υποσύνολο των ακεραίων Gauss και το συμβολίζουμε:

$$\alpha\mathbb{Z}[i] = \{\alpha\kappa / \kappa \in \mathbb{Z}[i]\},\ \text{για κάποιο } \alpha \in \mathbb{Z}[i].$$

Στην συνέχεια θα εστιάσουμε την προσοχή μας στη δομή των συνόλων που μόλις περιγράψαμε. Αρχικά αποδεικνύεται άμεσα ότι είναι υποδακτύλιοι του $\mathbb{Z}[i]$, με τις ίδιες πράξεις που έχουμε επισυνάψει στον δακτύλιο και μάλιστα επειδή επιπλέον ισχύει ότι:

$$\kappa(\alpha\mathbb{Z}[i]) = (\kappa\alpha)\,\mathbb{Z}[i] \subseteq \alpha\mathbb{Z}[i] \text{ και}$$

$$(\alpha\mathbb{Z}[i])\lambda = (\alpha\lambda)\,\mathbb{Z}[i] \subseteq \alpha\mathbb{Z}[i] \text{ για κάθε } \kappa, \lambda \in \mathbb{Z}[i].$$

Άρα αποτελούν ιδεώδη του $\mathbb{Z}[i]$.

Για την ακέραια περιοχή $\mathbb{Z}[i]$ έχουμε ήδη δείξει, στο θεώρημα 1.6, ότι είναι Ευκλείδεια Περιοχή με Ευκλείδεια συνάρτηση την $N: \mathbb{Z}[i]\backslash\{0\} \to \mathbb{N}^*$ όπου $N(\alpha)$ η στάθμη του $\alpha \in \mathbb{Z}[i]$. Επίσης στο θεώρημα 2.10 είδαμε πως κάθε Ευκλείδεια Περιοχή είναι και περιοχή κύριων ιδεωδών. Συνεπώς κάθε ιδεώδες του $\mathbb{Z}[i]$ είναι κύριο και θα παράγεται από κάποιο στοιχείο του. Για να προσεγγίσουμε το στοιχείο αυτό ας παρατηρήσουμε πρώτα ότι και στο σύνολο των πραγματικών ακεραίων όλα τα ιδεώδη είναι κύρια, αφού γνωρίζουμε ότι $n\mathbb{Z} = \langle n \rangle$, για κάποιο $n \in \mathbb{Z}$, το οποίο όμως θα πρέπει να έχει την μικρότερη απόλυτη τιμή μέσα στο σύνολο $n\mathbb{Z}$. Η λογική αίσθηση μας τώρα είναι ότι κάθε ιδεώδες $\alpha\mathbb{Z}[i]$, με $\alpha \in \mathbb{Z}[i]$, στο σύνολο των ακεραίων Gauss, θα παράγεται από κάποιο στοιχείο του, το οποίο θα πρέπει να έχει την ελάχιστη στάθμη. Στο σημείο αυτό είναι χρήσιμο να θυμηθούμε ότι αν δύο ακέραιοι Gauss α, β έχουν την ίδια στάθμη τότε αυτοί είναι ισοδύναμοι, δηλαδή $\alpha = \pm\beta$ ή $\alpha = \pm i\beta$.

Θεώρημα 2.13: Κάθε ιδεώδες του $\mathbb{Z}[i]$ είναι κύριο και προέρχεται από ένα εκ των στοιχείων του, αυτό με την μικρότερη στάθμη.

Απόδειξη: Ας πάρουμε λοιπόν ένα γνήσιο και μη τετριμμένο ιδεώδες I του $\mathbb{Z}[i]$. Το σύνολο $\{N(\alpha)/\alpha \in I\backslash 0\}$ είναι ένα μη κενό υποσύνολο του $\mathbb{N}^*$, οπότε θα έχει ελάχιστο στοιχείο, έστω το n. Αν θεωρήσουμε ως $\alpha \in I$ το ένα από τα τέσσερα στοιχεία για το οποίο ισχύει $N(\alpha) = n$ τότε:

$$\langle \alpha \rangle = \{\alpha\kappa/\kappa \in \mathbb{Z}[i]\} \subseteq I.$$

Επίσης για κάθε $z \in I$ από τον αλγόριθμο της διαίρεσης είναι:

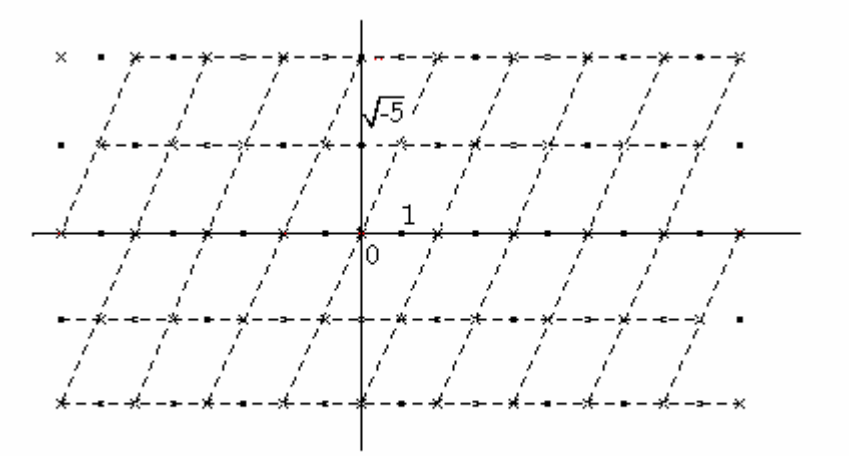
$$z = \lambda\alpha + \upsilon, \text{ με } \lambda, \upsilon \in \mathbb{Z}[i] \text{ και } N(\upsilon) < N(\alpha).$$

Αλλά το $N(\alpha) = n$, οπότε αφού το υ είναι ένα στοιχείο του I με στάθμη μικρότερη του n, τότε $N(\upsilon) = 0$, δηλαδή $\upsilon = 0$ και επομένως $z \in \langle \alpha \rangle$. ♦

Συμπεραίνουμε λοιπόν ότι για τους πραγματικούς ακεραίους α, β το ιδεώδες $(\alpha + \beta i)\mathbb{Z}[i]$ είναι κύριο και ισούται με $<\alpha + \beta i>$ αν και μόνο αν η $N(\alpha + \beta i)$ είναι η ελάχιστη στάθμη από όλες τις άλλες μέσα στο σύνολο αυτό. Επίσης ισχύει ότι τα ιδεώδη $<\alpha + \beta i>$, $<-\alpha - \beta i>$, $<-\beta + \alpha i>$ και $<\beta - \alpha i>$, του $\mathbb{Z}[i]$ ταυτίζονται.

Η σύνδεση που υπάρχει μεταξύ των ιδεωδών ενός δακτυλίου και της μοναδικότητας ανάλυσης των στοιχείων του σε πρώτους έχει γίνει φανερή πλέον. Θα επιχειρήσουμε τώρα μια γεωμετρική προσέγγιση, ώστε να γίνει πιο εμφανής η διαφορά που υπάρχει μεταξύ των δακτυλίων στους οποίους δεν ισχύει η μοναδικότητα από εκείνους στους οποίους ισχύει. Ένας δακτύλιος που γνωρίζουμε ότι δεν υφίσταται η συγκεκριμένη ιδιότητα είναι ο $\mathbb{Z}[\sqrt{-5}]$ σε αντίθεση βέβαια με τον $\mathbb{Z}[i]$ ή και με τον $\mathbb{Z}[\sqrt{-2}]$. Επειδή όμως όλα τα παραπάνω σύνολα, όπως και οι υποομάδες τους είναι αβελιανές ως προς την πρόσθεση, δημιουργούν διχτυωτά πλέγματα αντίστοιχα με εκείνο που έχουμε δει στο σχήμα 1.2.

Όλα τα ιδεώδη του $\mathbb{Z}[i]$ (όπως επίσης και του $\mathbb{Z}[\sqrt{-2}]$) είναι κύρια, ενώ αντίθετα δεν συμβαίνει το ίδιο και για τον $\mathbb{Z}[\sqrt{-5}]$. Δηλαδή υπάρχουν ιδεώδη που δεν έχουν την ίδια μορφή με τον αρχικό δακτύλιο. Αυτό ουσιαστικά συνιστά την αποτυχία της μοναδικότητας στην παραγοντοποίηση σε πρώτους.



Σχήμα 2.3

Η μορφή τέτοιων ιδεωδών εμφανίζεται στο σχήμα 2.3 όπου σημειώνονται τα αθροίσματα των πολλαπλασίων του 2 και του $1 + \sqrt{-5}$. Το διχτυωτό πλέγμα που προκύπτει δεν είναι τετραγωνικό, εκτιμώντας ότι το ίδιο θα συμβαίνει και για τον αρχικό δακτύλιο. Μέσω λοιπόν αυτής της εξήγησης έχουμε ενδείξεις της συναρπαστικής δομής που εμφανίζεται πίσω από την μοναδική ανάλυση των τετραγωνικών ακεραίων. Πάντως και στις δύο περιπτώσεις τα πάντα εξαρτώνται από την μορφή που έχει το πλέγμα και αυτή η μορφή είναι ακόμη πιο εντυπωσιακή στο μη-Ευκλείδειο χώρο. Αποτελούν δηλαδή οδούς που μας οδηγούν σε μη-Ευκλείδειες γεωμετρίες.

2.6 Δακτύλιοι Πηλίκα πάνω στο $\mathbb{Z}[i]$.

Για κάθε ιδεώδες $I = <\alpha + \beta i>$ με $\alpha, \beta \in \mathbb{Z}$ μπορούμε να ορίσουμε τα προσθετικά σύμπλοκά του $x + I$, με $x \in \mathbb{Z}[i]$ καθώς επίσης και το σύνολο των συμπλόκων $\mathbb{Z}[i]/I = \{x + I / x \in \mathbb{Z}[i]\}$. Σύμφωνα με το θεώρημα 2.5 το σύνολο αυτό αποτελεί έναν δακτύλιο με τις εξής πράξεις:

Πρόσθεση: $(x + I) + (y + I) = (x + y) + I$.

Πολλαπλασιασμό: $(x + I)\cdot(y + I) = (xy) + I$.

Οι δακτύλιοι αυτοί ως γνωστών είναι οι δακτύλιοι πηλίκα που ορίζονται πάνω στο σύνολο $\mathbb{Z}[i]$. Στην συνέχεια θα επιχειρήσουμε να συνδέσουμε, με την βοήθεια ομομορφισμών, αυτούς τους γενικούς δακτυλίους με πιο ειδικούς και συγκεκριμένους, όπως είναι οι δακτύλιοι $\mathbb{Z}_n$ ή $\mathbb{Z}_n[i]$. Οι τελευταίοι προέρχονται από το σύνολο

$$\mathbb{Z}_n[i] = \{\alpha + \beta i / \alpha, \beta \in \mathbb{Z}_n\}$$

και αποτελούν αντιμεταθετικούς δακτυλίους με πράξεις την πρόσθεση και τον πολλαπλασιασμό.

Αρχικά ας αναφέρουμε κάποιους ισομορφισμούς που ισχύουν για τους δακτυλίους πηλίκα στο $\mathbb{Z}[i]$ και οι οποίοι είναι προφανείς σύμφωνα με όσα έχουμε έως τώρα δει.

✶ $\mathbb{Z}[i]/\langle \alpha + \beta i\rangle \cong \mathbb{Z}[i]/\langle -\alpha - \beta i\rangle \cong \mathbb{Z}[i]/\langle -\beta + \alpha i\rangle \cong \mathbb{Z}[i]/\langle \beta - \alpha i\rangle$.

✶ $\mathbb{Z}[i]/\langle 0\rangle \cong \mathbb{Z}[i]$ και $\mathbb{Z}[i]/\langle 1\rangle \cong \{0\}$.

Στη συνέχεια θα δούμε ορισμένα θεωρήματα που σχετίζονται με τους ισομορφισμούς των δακτυλίων πηλίκων οι οποίοι σχηματίζονται από ιδεώδη που προέρχονται από φυσικούς ακέραιους. Σκοπός μας είναι να εξετάσουμε την δομή αυτών των δακτυλίων με όσο καλύτερο και ευκρινέστερο τρόπο γίνεται.

Θεώρημα 2.14: Για κάθε πραγματικό ακέραιο $n > 1$, ισχύει ότι:

$$\mathbb{Z}[i]/\langle n\rangle \cong \mathbb{Z}_n[i].$$

Απόδειξη: Θεωρούμε την απεικόνιση $\varphi: \mathbb{Z}[i] \to \mathbb{Z}_n[i]$ έτσι ώστε:

$$\varphi(x + yi) = [x]_n + [y]_n i, \text{ όπου } [x]_n, [y]_n,$$

αντιπροσωπεύουν τις κλάσεις ισοδυναμίας των ισοϋπόλοιπων modulo n, για τα x, y αντίστοιχα. Αρκεί τώρα να δείξουμε ότι η φ είναι ένας επιμορφισμός δακτυλίων. Επειδή:

$$\varphi(n) = [n]_n = [0]_n = 0 \text{ το } n \in \mathrm{Ker}(\varphi) \text{ δηλαδή } \langle n\rangle \subseteq \mathrm{Ker}(\varphi).$$

Αν τώρα έχουμε $\varphi(x + yi) = 0$ τότε $x \equiv 0(\mathrm{mod} n)$ και $y \equiv 0(\mathrm{mod} n)$. Οπότε υπάρχουν πραγματικοί ακέραιοι κ, λ ώστε $x = n\kappa$ και $y = n\lambda$. Έτσι έχουμε:

$$x + yi = n\kappa + n\lambda i = n(\kappa + \lambda i) \in \langle n\rangle.$$

Συνεπώς $\mathrm{Ker}(\varphi) = \langle n\rangle$, που μας δίνει ότι $\mathbb{Z}[i]/\langle n\rangle \cong \mathbb{Z}_n[i]$. ♦

Οι δακτύλιοι $\mathbb{Z}_n[i]$ έχουν μεν πεπερασμένο πλήθος στοιχείων, οπότε είναι ευκολότεροι στην μελέτη τους, αλλά θα ήταν σίγουρα καλύτερο να γνωρίζαμε αν έχουν και επιπλέον ιδιότητες, δηλαδή αν και πότε αποτελούν σώματα. Κάτι τέτοιο θα μας διευκόλυνε γιατί θα ίσχυε το ίδιο και για τους ισόμορφους τους δακτυλίους πηλίκο $\mathbb{Z}[i]/\langle n\rangle$. Οπότε θα μπορούσαμε να συμπεράνουμε, σύμφωνα με το θεώρημα 2.9, αν και πότε τα ιδεώδη $\langle n\rangle$ είναι μέγιστα. Ας δούμε πρώτα δύο παραδείγματα με δακτύλιους πηλίκα οι οποίοι προέρχονται από ιδεώδη που παράγονται από περιττούς πρώτους πραγματικούς ακέραιους.

Έστω το ιδεώδες $<3>$, τότε ισχύει ότι $\mathbb{Z}[i]/<3> \cong \mathbb{Z}_3[i]$. Όμως το τελευταίο έχει 9 στοιχεία. Αυτό συμβαίνει γιατί τα πραγματικά και τα φανταστικά μέρη των ακεραίων οι οποίοι ανήκουν στο $\mathbb{Z}_3[i]$ μπορούν να επιλεγούν από 3 δυνατές τιμές το κάθε ένα. Τόσες ακριβώς όσες είναι τα υπόλοιπα των διαιρέσεων ενός ακεραίου δια του 3. Οπότε το πλήθος των στοιχείων του συνόλου αυτού θα είναι $3 \cdot 3 = 9$. Επίσης επειδή μια ακέραια περιοχή με πεπερασμένο πλήθος στοιχείων είναι σώμα, τότε αρκεί να δείξουμε ότι ο $\mathbb{Z}[i]/<3>$ είναι ακέραια περιοχή ή λόγω του θεωρήματος 2.8 να δείξουμε ότι το ιδεώδες $<3>$ είναι πρώτο.

Δεχόμαστε λοιπόν ότι για τους ακεραίους $\alpha + \beta i$ και $\gamma + \delta i$ ισχύει:

$$(\alpha + \beta i)(\gamma + \delta i) \in <3> \text{ τότε } 3/(\alpha\gamma - \beta\delta) \text{ και } 3/(\alpha\delta + \beta\gamma),$$

$$\text{δηλαδή } 3/[(\alpha + \beta)\gamma + (\alpha - \beta)\delta].$$

Αν υποθέσουμε ότι $3 \nmid (\alpha + \beta i)$ τότε το 3 δεν θα διαιρεί τουλάχιστον έναν από τους πραγματικούς α, β. Χωρίς βλάβη της γενικότητας δεχόμαστε ότι $3/\alpha$ και $3 \nmid \beta$, τότε $3/\beta\delta$ και $3/\beta\gamma$ και επειδή ο 3 είναι πρώτος ακέραιος θα έχουμε $3/\gamma$ και $3/\delta$. Επίσης αν $3 \nmid \alpha$ και $3 \nmid \beta$, τότε θα διαιρεί έναν μόνο από τους $\alpha + \beta$, $\alpha - \beta$, έστω ότι $3/(\alpha + \beta)$ και $3 \nmid (\alpha - \beta)$, τότε $3/(\alpha - \beta)\delta$ δηλαδή $3/\delta$ και επομένως $3/\alpha\gamma$, οπότε $3/\gamma$. Συνεπώς το ιδεώδες $<3>$ είναι πρώτο στο $\mathbb{Z}[i]$. Αποδείχθηκε λοιπόν ότι ο $\mathbb{Z}[i]/<3>$ είναι ένα σώμα με 9 στοιχεία.

Γενίκευση όμως του παραπάνω δεν είναι εφικτή, αφού δεν μπορούμε να κάνουμε το ίδιο και για το ιδεώδες $<5>$. Αν εξετάσουμε τα στοιχεία:

$$2 + i \notin <5> \text{ και } 2 - i \notin <5>, \text{ έχουμε ότι:}$$

$$(2 + i)(2 - i) = 5 \in <5>.$$

Οπότε προφανώς το $\mathbb{Z}[i]/<5>$ δεν είναι σώμα και επομένως το $<5>$ δεν είναι μέγιστο ιδεώδες. Η διαφορά των δύο αυτών ιδεωδών μπορεί να βρεθεί αν θυμηθούμε την ταξινόμηση των πρώτων Gauss και δούμε ότι οι δύο παραπάνω ακέραιοι είναι μεν πρώτοι στο $\mathbb{Z}$, αλλά δεν συμβαίνει το ίδιο και για το $\mathbb{Z}[i]$.

Θεώρημα 2.15: Για κάθε πραγματικό ακέραιο $n > 1$, το $\mathbb{Z}_n[i]$ είναι σώμα αν και μόνο αν ο n είναι πρώτος της μορφής $4\kappa + 3$, με $\kappa \in \mathbb{Z}$.

Απόδειξη: Αρχικά δεχόμαστε ότι το $\mathbb{Z}_n[i]$ είναι σώμα. Όπως έχουμε αναφέρει και στο παράδειγμα της παραγράφου 2.3 αντίστοιχα για το $\mathbb{Z}_n$, ο πραγματικός ακέραιος n πρέπει να είναι πρώτος. Επιπλέον ο n δεν μπορεί να είναι ίσος με 2 γιατί $2 =(1 + i)(1 – i)$, οπότε θα είχαμε διαιρέτες του μηδενός. Επομένως ο n είναι περιττός πρώτος. Θεωρούμε τώρα τον ομομορφισμό δακτυλίων $\varphi: \mathbb{Z}_n[x] \to \mathbb{Z}_n[i]$ με $\varphi(x) = i$, επειδή ο n είναι πρώτος τότε ο πυρήνας του $\mathrm{Ker}(\varphi) = \langle x^2 + 1\rangle$. Σύμφωνα με το θεώρημα 2.7 έχουμε ότι $\mathbb{Z}_n[i] \cong \mathbb{Z}_n[x]/\langle x^2 + 1\rangle$ το οποίο θα είναι σώμα και επομένως ο n δεν θα διαιρεί το $(x^2 + 1)$. Αυτό όμως είναι αντίστοιχο με το ότι δεν υπάρχουν λύσεις της εξίσωσης $x^2 + 1 = \kappa n$, $\kappa \in \mathbb{Z}$. Όπως έχουμε αναφέρει στο θεώρημα 1.10 των δύο τετραγώνων του Fermat η εξίσωση αυτή έχει λύση μόνο αν ο n είναι πρώτος και έχει μορφή $4m + 1$, $m \in \mathbb{Z}$. Άρα καταλήγουμε στο ότι ο n είναι πραγματικός πρώτος έτσι ώστε $n = 4m + 3$, με $m \in \mathbb{Z}$.

Στην περίπτωση τώρα που ο n είναι πραγματικός πρώτος και της μορφής $n = 4m + 3$, με $m \in \mathbb{Z}$, εξετάζοντας τον ομομορφισμό φ συμπεραίνουμε ότι το $x^2 + 1$ δεν είναι αναλύσιμο και ο πυρήνας $\langle x^2 + 1\rangle$ θα είναι μέγιστο ιδεώδες. Επομένως το $\mathbb{Z}_n[i]$ αποτελεί σώμα. ♦

Στο σημείο αυτό θα επεκταθούμε σε δακτυλίους πηλίκα με πιο γενική μορφή, όπως οι $\mathbb{Z}[i]/\langle \alpha + \beta i\rangle$, με τον περιορισμό όμως οι ακέραιοι α, β να είναι σχετικά πρώτοι. Οι ισομορφισμοί που θα παρουσιαστούν είναι ιδιαίτερα ενδιαφέροντες και μας παρέχουν σημαντικές πληροφορίες για το πλήθος των στοιχείων τους καθώς και για την ανάλυσή τους σε απλούστερους.

Θεώρημα 2.16: Αν οι α, β είναι σχετικά πρώτοι πραγματικοί ακέραιοι, τότε ισχύει ότι:

$$\mathbb{Z}[i]/\langle \alpha + \beta i\rangle \cong \mathbb{Z}_{N(\alpha + \beta i)}.$$

Απόδειξη: Σύμφωνα με όσα αναφέραμε στο τέλος της παραγράφου 2.5 μπορούμε χωρίς βλάβη της γενικότητας του θεωρήματος να υποθέσουμε ότι οι α, β είναι θετικοί. Επίσης προφανώς ο β θα είναι και σχετικά πρώτος με τον $N(\alpha + \beta i) = \alpha^2 + \beta^2$, οπότε στον $\mathbb{Z}_{N(\alpha + \beta i)}$ θα ανήκει και ο αντίστροφος του δηλαδή ο β^{-1} (φυσικά εννοούμε το αντίστροφο στοιχείο των ισοϋπόλοιπων της κλάσης του β ως προς $\alpha^2 + \beta^2$). Επίσης ισχύει ότι:

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

Οπότε συμπεραίνουμε ότι ο $(\alpha^2 + \beta^2)/[(\alpha\beta^{-1})^2 + 1]$.

Ορίζουμε λοιπόν την απεικόνιση $\varphi: \mathbb{Z}[i] \to \mathbb{Z}_{N(\alpha + \beta i)}$ ώστε:

$$\varphi(x + yi) = [x - (\alpha\beta^{-1})y],$$

ισοϋπόλοιποι του $(\alpha^2 + \beta^2)$. Η φ είναι προφανώς επί, οπότε θα δείξουμε ότι διατηρεί τις πράξεις της πρόσθεσης και του πολλαπλασιασμού. Ας πάρουμε $\alpha = x + yi$ και $\beta = w + zi$, τότε:

- $\varphi(\alpha) + \varphi(\beta) = [x - (\alpha\beta^{-1})y] + [w - (\alpha\beta^{-1})z] \equiv (x + w) - (\alpha\beta^{-1})(y + z) = \varphi((x + w) + (y + z)i) = \varphi((x + yi) + (w + zi)) = \varphi(\alpha + \beta)$.
- $\varphi(\alpha)\cdot\varphi(\beta) = [x - (\alpha\beta^{-1})y]\cdot[w - (\alpha\beta^{-1})z] \equiv (xw) + (\alpha\beta^{-1})^2(yz) - \alpha\beta^{-1}(xz + yw) \equiv (xw - yz) - \alpha\beta^{-1}(xz + yw) = \varphi((xw - yz) + (xz + yw)i) = \varphi((x + yi)\cdot(w + zi)) = \varphi(\alpha\cdot\beta)$.

Στη συνέχεια επειδή $\varphi(\alpha + \beta i) = \alpha - (\alpha\beta^{-1})\beta = 0$, έχουμε ότι:

$$\langle\alpha + \beta i\rangle \subseteq \mathrm{Ker}(\varphi).$$

Από την άλλη όμως αν υποθέσουμε ότι το $\gamma + \delta i$ είναι κάποιο στοιχείο του πυρήνα $\mathrm{Ker}(\varphi)$ για το οποίο ισχύει $\gamma + \delta i = (\alpha + \beta i)(x + yi)$, με τους $x, y \in \mathbb{Z}$, τότε αφού είναι $0 = \varphi(\gamma + \delta i) = \gamma - (\alpha\beta^{-1})\delta = \beta\gamma - \alpha\delta$, συμπεραίνουμε ότι $(\alpha^2 + \beta^2)/(\beta\gamma - \alpha\delta)$, πράγμα που σημαίνει ότι ο y είναι ακέραιος. Επίσης αν πολλαπλασιάσουμε την ισότητα με $\alpha\beta$ γίνεται: $0 = \alpha\beta^2\gamma - \alpha^2\beta\delta$ που καταλήγει $0 = \alpha\gamma - (\alpha\beta^{-1})^2\beta\delta$. Όμως γνωρίζουμε ότι $(\alpha^2 + \beta^2)/[(\alpha\beta^{-1})^2 + 1]$, οπότε από τις δύο τελευταίες σχέσεις θα έχουμε $(\alpha^2 + \beta^2)/(\alpha\gamma + \beta\delta)$, δηλαδή ο x είναι επίσης ακέραιος. Συνεπώς $\mathrm{Ker}(\varphi) \subseteq \langle\alpha + \beta i\rangle$, βάση του οποίου έχουμε $\mathrm{Ker}(\varphi) = \langle\alpha + \beta i\rangle$. Άρα αποδείχθηκε ότι $\mathbb{Z}[i]/\langle\alpha + \beta i\rangle \cong \mathbb{Z}_{N(\alpha + \beta i)}$. ♦

Σύμφωνα λοιπόν με όσα ήδη δείξαμε, αρχικά από το θεώρημα 2.14, μπορούμε να συμπεράνουμε ότι ο δακτύλιος πηλίκο $\mathbb{Z}[i]/<n>$, με $n > 1$ πραγματικό ακέραιο, έχει το ίδιο πλήθος στοιχείων με τον δακτύλιο $\mathbb{Z}_n[i]$ δηλαδή n^2. Αυτό ισχύει, αφού για κάθε στοιχείο του $\mathbb{Z}_n[i]$ έχουμε n επιλογές για το πραγματικό και άλλες τόσες για το φανταστικό του μέρος, οπότε οι συνδυασμοί τους είναι $n \cdot n = n^2$. Επίσης από το θεώρημα 2.16 ο δακτύλιος πηλίκο $\mathbb{Z}[i]/<\alpha + \beta i>$ με μ.κ.δ$(\alpha, \beta) = 1$, θα έχει το ίδιο πλήθος στοιχείων με τον δακτύλιο $\mathbb{Z}_{N(\alpha + \beta i)}$, δηλαδή $N(\alpha + \beta i) = \alpha^2 + \beta^2$. Για παράδειγμα για τον αριθμό $2 + 5i$ ισχύει μ.κ.δ$(2, 5) = 1$, οπότε ο δακτύλιος πηλίκο $\mathbb{Z}[i]/<2 + 5i>$ είναι ισόμορφος με τον $\mathbb{Z}_{29}$ που έχει 29 στοιχεία.

Πριν περάσουμε στο επόμενο γενικό θεώρημα σχετικά με τα στοιχεία ενός παραγοντικού δακτυλίου πάνω στο $\mathbb{Z}[i]$, πρέπει να τονίσουμε μια άμεση συνέπεια από την διαίρεση μεταξύ των ακεραίων Gauss όπως την είδαμε στην παράγραφο 2.4. Ας υποθέσουμε ότι οι α, β είναι σχετικά πρώτοι πραγματικοί ακέραιοι, τότε ο ακέραιος Gauss $\gamma + \delta i$, θα ανήκει στο ιδεώδες $<\kappa\alpha + \kappa\beta i>$, για $\kappa \in \mathbb{Z}$ αν και μόνο αν ο $\kappa(\alpha^2 + \beta^2)$ διαιρεί το $(\alpha\gamma + \beta\delta)$ και το $(\alpha\delta - \beta\gamma)$. Ακόμη θα πρέπει να θυμίσουμε ότι στην παράγραφο 1.7 έχουμε αναφερθεί και ορίσει την έννοια των ισοϋπόλοιπων στο σύνολο $\mathbb{Z}[i]$.

Θεώρημα 2.17: Αν οι α, β, κ είναι θετικοί πραγματικοί ακέραιοι και οι α, β είναι σχετικά πρώτοι, τότε οι κλάσεις ισοϋπόλοιπων του $\mathbb{Z}[i]/<\alpha + \beta i>$ είναι $\{[x + yi]/0 \le x < \kappa(\alpha^2 + \beta^2)$ και $0 \le y < \kappa\}$.

Απόδειξη: Πριν ξεκινήσουμε την απόδειξη του θεωρήματος καλό είναι να διευκρινίσουμε ότι με την ορολογία κλάση $[x + yi]$ εννοούμε τον αριθμό $x + yi$ που αντιπροσωπεύει όλους τους ακεραίους Gauss οι οποίοι είναι ισοϋπόλοιποι κατά modulo $(\alpha\kappa + \beta\kappa i)$. Το πρώτο βήμα είναι να δείξουμε ότι οι κλάσεις αυτές είναι διακριτές. Αν θεωρήσουμε λοιπόν ότι υπάρχουν

$$[x_1 + y_1 i] = [x_2 + y_2 i] \text{ με } 0 \le x_1, x_2 < \kappa(\alpha^2 + \beta^2) \text{ και } 0 \le y_1, y_2 < \kappa,$$

τότε θα ισχύει ότι:

$$(x_2 - x_1) + (y_2 - y_1)i \in <\alpha\kappa + \beta\kappa i>.$$

Οπότε σύμφωνα με ότι προείπαμε έχουμε $\kappa(\alpha^2 + \beta^2)/[\alpha(x_2 - x_1) + \beta(y_2 - y_1)]$ και $\kappa(\alpha^2 + \beta^2)/[\alpha(y_2 - y_1) - \beta(x_2 - x_1)]$ ή επίσης:

$$\kappa(\alpha^2 + \beta^2)/\{\beta[\alpha(x_2 - x_1) + \beta(y_2 - y_1)] + \alpha[\alpha(y_2 - y_1) - \beta(x_2 - x_1)]\}.$$

Από το οποίο συμπεραίνουμε ότι ο $\kappa/(y_2 - y_1)$. Επειδή όμως και οι δύο είναι μη μηδενικοί και μικρότεροι του κ, τότε $y_1 = y_2$. Επίσης από τις σχέσεις:

$$\kappa(\alpha^2 + \beta^2)/\alpha(x_2 - x_1) \text{ και } \kappa(\alpha^2 + \beta^2)/\beta(x_2 - x_1)$$

και επειδή οι α, β είναι σχετικά πρώτοι θα ισχύει ότι $\kappa(\alpha^2 + \beta^2)/(x_2 - x_1)$ το οποίο όπως και πριν μας οδηγεί στο συμπέρασμα $x_1 = x_2$. Συνεπώς οι κλάσεις είναι διακριτές.

Το επόμενο βήμα είναι να δείξουμε ότι κάθε στοιχείο $x + yi$ αντιστοιχεί σε κάποια από τις κλάσεις ισοδυναμίας. Αφού οι ακέραιοι α, β είναι σχετικά πρώτοι, θα υπάρχουν ακέραιοι γ, δ ώστε: $\alpha\gamma + \beta\delta = 1$ ή $\alpha\kappa\gamma + \beta\kappa\delta = \kappa$. Παρατηρούμε ότι ισχύει:

$$\kappa i - (\delta + \gamma i)(\alpha\kappa + \beta\kappa i) =$$
$$\kappa i - (\alpha\kappa + \beta\kappa i)\gamma i - (\alpha\kappa + \beta\kappa i)\delta =$$
$$(\beta\kappa\gamma - \alpha\kappa\delta) + (\kappa - \alpha\kappa\gamma - \beta\kappa\delta)i =$$
$$(\beta\kappa\gamma - \alpha\kappa\delta) + (\kappa - \kappa)i = m \in \mathbb{Z}.$$

Δηλαδή ο μιγαδικός ακέραιος κi είναι ισοϋπόλοιπος ενός πραγματικού ακεραίου m ως προς modulo $(\alpha\kappa + \beta\kappa i)$ μέσα στο $\mathbb{Z}[i]$. Από αυτό μπορούμε να συμπεράνουμε ότι η $[x + yi]$ συμπίπτει με κάποια $[x' + y'i]$ για κάποιο y' που ικανοποιεί την συνθήκη $0 \le y' < \kappa$. Τέλος για τον πραγματικό αριθμό $\kappa(\alpha^2 + \beta^2)$ είναι φανερό ότι περιέχεται στο ιδεώδες $<\alpha\kappa + \beta\kappa i>$ και επομένως έχουμε ότι $[x + yi] = [x'' + y''i]$ με $0 \le x'' < \kappa(\alpha^2 + \beta^2)$ και $0 \le y'' < \kappa$. ♦

Είδαμε λοιπόν την ανάλυση της δομής ενός παραγοντικού δακτυλίου, ο οποίος προέρχεται από ένα πολλαπλάσιο ενός κύριου ιδεώδους. Στην συνέχεια θα επιχειρήσουμε να βρούμε κάποιες σχέσεις που συνδέουν το πλήθος των στοιχείων δύο κύριων ιδεωδών τα οποία παράγονται από στοιχεία του $\mathbb{Z}[i]$ που δεν είναι πρώτα μεταξύ τους.

Στην πρώτη περίπτωση θα ασχοληθούμε με τα ιδεώδη $<\alpha>$ και $<\beta>$ του $\mathbb{Z}[i]$ που παράγονται από δύο μη μηδενικούς ακεραίους Gauss α, β τέτοιοι ώστε ο β να διαιρεί τον α, προφανώς τότε ισχύει ότι $<\alpha> \subseteq <\beta>$. Σύμφωνα με το τρίτο θεώρημα των ισομορφισμών ο δακτύλιος $<\beta>/<\alpha>$ όπως επίσης και το $<\beta>$ θα είναι ιδεώδες του $\mathbb{Z}[i]/<\alpha>$ και μάλιστα υπάρχει ισομορφισμός:

$$(\mathbb{Z}[i]/<\alpha>)/(<\beta>/<\alpha>) \cong \mathbb{Z}[i]/<\beta>.$$

Όμως από το θεώρημα 2.6 γνωρίζουμε ότι $\mathbb{Z}[i]/<\alpha> \cong \mathbb{Z}_{N(\alpha)}$ που σημαίνει ότι ο δακτύλιος πηλίκο έχει $N(\alpha)$ πλήθος στοιχεία και $\mathbb{Z}[i]/<\beta> \cong \mathbb{Z}_{N(\beta)}$ δηλαδή ο $\mathbb{Z}[i]/<\beta>$ έχει $N(\beta)$ στοιχεία. Επομένως το ιδεώδες $<\beta>$ θα έχει $\frac{N(\alpha)}{N(\beta)}$ πλήθος στοιχείων.

Στην επόμενη περίπτωση ας επιλέξουμε ως β έναν ακέραιο Gauss ο οποίος δεν διαιρεί τον $\alpha \in \mathbb{Z}[i]$ και έστω ο $\mu.\kappa.\delta.(\alpha, \beta) = \delta \in \mathbb{Z}[i]$ (η ύπαρξη – εύρεσή του δ έχει αναλυθεί στο πόρισμα 1.2). Τότε το ιδεώδες $<\beta>$ παράγεται από τον δ και όπως είδαμε και παραπάνω θα έχουμε αφενός μεν ότι $<\beta> \subseteq \mathbb{Z}[i]/<\alpha>$ και αφετέρου ότι το πλήθος των στοιχείων του $<\beta>$ είναι ίσο με $\frac{N(\alpha)}{N(\delta)}$.

2.7 Η Δομή του Δακτυλίου $\mathbb{Z}[i]/<\alpha + \beta i>$.

Στην γενική περίπτωση, όταν δηλαδή έχουμε έναν τυχαίο ακέραιο Gauss $\alpha + \beta i$ και θέλουμε να αναλύσουμε την δομή του δακτυλίου πηλίκου του $\mathbb{Z}[i]/<\alpha + \beta i>$ θα πρέπει, όπως και προηγουμένως, να ελέγξουμε αν υπάρχουν ισομορφισμοί και τι είδους είναι αυτοί. Μπορούμε άραγε να έχουμε αντίστοιχους ισομορφισμούς όπως και στους πραγματικούς ακεραίους; Για τους τελευταίους γνωρίζουμε, ως άμεση συνέπεια του Κινέζικου θεωρήματος υπολοίπων, ότι για κάθε ακέραιο n ο οποίος είναι δυνατόν να αναλυθεί

σύμφωνα με την μορφή $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$, με p_i να είναι πρώτοι, υφίσταται ο ισομορφισμός: $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}$. Όπως βέβαια ήδη είναι γνωστό ο $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$ οπότε άμεσα καταλήγουμε στην σχέση:

$$\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}.$$

Στο σημείο αυτό, λόγω της αναφοράς μας στο **Κινέζικο Θεώρημα υπολοίπων** (Chinese remainder theorem) θα ήταν χρήσιμο να υπενθυμίσουμε την διατύπωση του. Δεδομένου λοιπόν ενός δακτυλίου D και των ιδεωδών του I και J ισχύουν οι εξής σχέσεις:

- Υπάρχει η απεικόνιση $\varphi: D/I \cap J \to D/I \times J$ ώστε $d + I \cap J \to (d + I, d + J)$ με $d \in D$ και είναι μονομορφισμός δακτυλίων.
- Αν επίσης ισχύει ότι $I + J = D$, τότε η απεικόνιση $\varphi: D/I \cap J \to D/I \times J$ είναι ισομορφισμός.
- Στην περίπτωση που $D = \mathbb{Z}$ και $I = \langle n \rangle$, $J = \langle m \rangle$ με n, m σχετικά πρώτους ακεραίους, τότε $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$.

Η τελευταία σχέση με επαγωγή μπορεί να γίνει ως εξής: Έστω $n_1, n_2, \ldots, n_k \in \mathbb{N}$ με μ.κ.δ.$(n_i, n_j) = 1$ για κάθε φυσικό αριθμό $i \neq j$. Αν $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ τότε $\mathbb{Z}_N \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$.

Ας ξεκινήσουμε λοιπόν με την ανάλυση ενός ακεραίου Gauss $\alpha + \beta i$ σε γινόμενο πρώτων παραγόντων. Σύμφωνα με την μοναδικότητα της ανάλυσης αυτής και από το θεώρημα 1.11 που ταξινομεί τους πρώτους Gauss θα έχουμε:

$$\alpha + \beta i = i^r \cdot \prod z_j^{\kappa_j} \cdot \prod z_j'^{\lambda_j} \cdot \prod p_j^{\mu_j} \cdot (1 + i)^\nu.$$

όπου οι $z = x + yi$, $z' = y + xi$ με $N(z) = N(z') = 4n + 1$, $n \in \mathbb{N}$, οι p_j πρώτοι πραγματικοί ακέραιοι της μορφής $4n + 3$, $n \in \mathbb{N}$ και οι $r, \kappa_j, \lambda_j, \mu_j, \nu$ μη αρνητικοί πραγματικοί ακέραιοι ώστε $\kappa_j \leq \lambda_j$. Συμβολίζουμε στην συνέχεια

ως $t = \prod N(z_j)^{\kappa_j}$, $t' = \prod N(z_j')^{\lambda_j}$ και $q = \prod p_j^{\mu_j}$, άρα παρατηρούμε ότι ισχύει $t, t', q \in \mathbb{N}$ και t/t'.

Βάση της προηγούμενης παραγοντοποίησης μπορούμε να περάσουμε στη ισότητα των στάθμεων τους. Οπότε λόγω της πολλαπλασιαστικής ιδιότητας της στάθμης θα είναι:

$$N(\alpha + \beta i) = \alpha^2 + \beta^2 = t \cdot t' \cdot q^2 \cdot 2^v.$$

Είμαστε λοιπόν έτοιμοι να αποδείξουμε το επόμενο κεντρικό θεώρημα σχετικά με τους δακτυλίους πηλίκο στον $\mathbb{Z}[i]$.

Θεώρημα 2.18: Διατηρώντας τους συμβολισμούς που χρησιμοποιήσαμε στην εισαγωγή του θεωρήματος, για τους πραγματικούς ακεραίους α, β που δεν είναι και οι δύο μηδέν, και θεωρώντας τον δακτύλιο $G_v = \mathbb{Z}[i]/\langle(1 + i)^v\rangle$ έχουμε τις εξής περιπτώσεις:

- $\mathbb{Z}[i]/\langle\alpha + \beta i\rangle \cong \mathbb{Z}_t \times \mathbb{Z}_{t'} \times \mathbb{Z}_q[i] \times \mathbb{Z}_{2^{v/2}}[i]$, όταν το v είναι άρτιος.
- $\mathbb{Z}[i]/\langle\alpha + \beta i\rangle \cong \mathbb{Z}_t \times \mathbb{Z}_{t'} \times \mathbb{Z}_q[i] \times G_v$, όταν το v είναι περιττός.

Απόδειξη: Λόγω της παραγοντοποίησης του μιγαδικού $\alpha + \beta i$ ισχύει:

$$\langle\alpha + \beta i\rangle = \langle \prod z_j^{\kappa_j} \cdot \prod z_j'^{\lambda_j} \cdot \prod p_j^{\mu_j} \cdot (1 + i)^v \rangle.$$

Από το θεώρημα 1.12 γνωρίζουμε ότι για δύο σχετικά πρώτους ακεραίους Gauss γ, δ μπορούμε να βρούμε $\omega, \varphi \in \mathbb{Z}[i]$ ώστε $\omega\gamma + \varphi\delta = 1$. Επομένως έχουμε ότι $\langle\gamma\rangle + \langle\delta\rangle = \mathbb{Z}[i]$. Επίσης είναι γνωστό ότι $\langle\gamma\rangle \cap \langle\delta\rangle = \langle\gamma\delta\rangle$. Εφαρμόζοντας τώρα την γενίκευση του Κινέζικου θεωρήματος υπολοίπων, που έχουμε προαναφέρει συμπεραίνουμε ότι:

$$\mathbb{Z}[i]/\langle\gamma\delta\rangle \cong \mathbb{Z}[i]/\langle\gamma\rangle \times \mathbb{Z}[i]/\langle\delta\rangle.$$

Συνεπώς από τις παραπάνω σχέσεις έχουμε:

$$\mathbb{Z}[i]/\langle\alpha + \beta i\rangle \cong \mathbb{Z}[i]/\langle \prod z_j^{\kappa_j} \rangle \times \mathbb{Z}[i]/\langle \prod z_j'^{\lambda_j} \rangle$$

$$\times \mathbb{Z}[i]/\langle \prod p_j^{\mu_j} \rangle \times \mathbb{Z}[i]/\langle (1 + i)^v \rangle.$$

Για να δείξουμε ότι η σχέση που μόλις αναφέραμε καταλήγει στο ζητούμενο αποτέλεσμα, ας συμβολίσουμε το $\prod z_j^{\kappa_j} = x + yi$. Επειδή όμως το $2 = i^3(1 + i)^2$ τότε το 2 δεν διαιρεί το $x + yi$. Επίσης κάθε πραγματικός πρώτος $p = 2n + 3$ είναι και πρώτος στο σύνολο $\mathbb{Z}[i]$ άρα και ο p δεν μπορεί να διαιρεί τον $x + yi$. Ακόμη για κάθε πραγματικό πρώτο $p' = 2n + 1$ γνωρίζουμε ότι ισχύει $p' = z_j \cdot z'_j$, για κάποιο $j \in \mathbb{N}$, οπότε ούτε ο p' θα διαιρεί τον $x + yi$. Επομένως μπορούμε να συμπεράνουμε ότι τα x, y είναι σχετικά πρώτοι πραγματικοί ακέραιοι. Σύμφωνα τώρα με το θεώρημα 2.16 έχουμε:

$$\mathbb{Z}[i]/<\prod z_j^{\kappa_j}> \cong \mathbb{Z}[i]/<x + yi> \cong \mathbb{Z}_{N(x + yi)} \cong \mathbb{Z}_t.$$

Με αντίστοιχο τρόπο καταλήγουμε ότι επίσης ισχύει:

$$\mathbb{Z}[i]/< \prod z'^{\lambda_j}_j > \cong \mathbb{Z}_{t'}.$$

Επίσης από το θεώρημα 2.14 έχουμε:

$$\mathbb{Z}[i]/< \prod p_j^{\mu_j} > \cong \mathbb{Z}_q[i].$$

Τέλος όσον αφορά τον δακτύλιο $G_v = \mathbb{Z}[i]/<(1 + i)^v>$ και ειδικά για το ιδεώδες του μπορούμε να δούμε ότι αν ο v είναι άρτιος γίνεται:

$$<(1 + i)^v> = <(2i)^{v/2}> = <2^{v/2}>.$$

Οπότε ο $G_v = \mathbb{Z}[i]/<(1 + i)^v> = \mathbb{Z}[i]/<2^{v/2}>$, το οποίο πάλι από το θεώρημα 2.14 δίνει:

$$G_v = \mathbb{Z}[i]/<2^{v/2}> \cong \mathbb{Z}_{2^{v/2}}[i].$$

Άρα αν το v είναι άρτιος ισχύει ότι:

$$\mathbb{Z}[i]/<\alpha + \beta i> \cong \mathbb{Z}_t \times \mathbb{Z}_{t'} \times \mathbb{Z}_q[i] \times \mathbb{Z}_{2^{v/2}}[i].$$

Στην περίπτωση τώρα που ο $v > 1$ είναι περιττός δεν μπορεί να υπάρξει αντίστοιχη απλή μορφή του G_v, δηλαδή έχουμε:

$$\mathbb{Z}[i]/<\alpha + \beta i> \cong \mathbb{Z}_t \times \mathbb{Z}_{t'} \times \mathbb{Z}_q[i] \times G_v. \qquad \blacklozenge$$

Στην συνέχεια ας δούμε ορισμένα παραδείγματα ισομορφισμών δακτυλίων πηλίκων. Σύμφωνα με την μοναδική παραγοντοποίηση σε πρώτους Gauss του ακεραίου $6 + 14i$ έχουμε:

$$6 + 14i = i^3(5 + 2i)(1 + i)^3,$$

οπότε από το θεώρημα 2.18 ισχύει ότι:

$$\mathbb{Z}[i]/\langle 6 + 14i\rangle \cong \mathbb{Z}_{29} \times G_3.$$

Κατά τον ίδιο τρόπο αν επιλέξουμε τον ακέραιο $3 + 9i$ η ανάλυση του σε πρώτους είναι:

$$3 + 9i = (2 + i)3(1 + i).$$

Εφαρμόζοντας τώρα το θεώρημα 2.18 έχουμε τους εξής ισομορφισμούς:

$$\mathbb{Z}[i]/\langle 3 + 9i\rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_3[i] \times \mathbb{Z}_2 \cong \mathbb{Z}_{10} \times \mathbb{Z}_3[i].$$

Στην περίπτωση επίσης του πραγματικού ακεραίου 156, από την παραγοντοποίηση του έχουμε: $156 = i(3 + 2i)(2 + 3i)3(1 + i)^4$. Οπότε για τον αντίστοιχο δακτύλιο πηλίκο του θα ισχύει:

$$\mathbb{Z}[i]/\langle 156\rangle \cong \mathbb{Z}_{13} \times \mathbb{Z}_{13} \times \mathbb{Z}_3[i] \times \mathbb{Z}_4[i].$$

Τέλος για τον πραγματικό πρώτο 11 γνωρίζουμε ότι:

$$\mathbb{Z}[i]/\langle 11\rangle \cong \mathbb{Z}_{11}[i],$$

που λόγω του θεωρήματος 2.15 αποτελεί σώμα. Όμως για τον επίσης πραγματικό πρώτο 13 επειδή ισχύει ότι:

$$13 = i^3(3 + 2i)(2 + 3i),$$

τότε από τον συνδυασμό των θεωρημάτων 2.16 και 2.18 θα είναι:

$$\mathbb{Z}[i]/\langle 13\rangle \cong \mathbb{Z}_{13}[i] \cong \mathbb{Z}_{13} \times \mathbb{Z}_{13},$$

ο οποίος προφανώς έχει διαιρέτες του μηδενός.

Φυσικά υπάρχουν και άλλοι δακτύλιοι με τις ανάλογες ιδιότητες. Οπότε η χρηστικότητα των θεωρημάτων που αποδείξαμε επεκτείνεται και πέραν της συγκεκριμένης ακέραιας περιοχής. Ένα παράδειγμα τέτοιου δακτυλίου είναι οι **ακέραιοι Eisenstein**. Το σύνολο τους συμβολίζεται με $\mathbb{Z}[\omega]$ και περιέχει τους μιγαδικούς της μορφής $z = \alpha + \beta\omega$, όπου οι α, β είναι πραγματικοί

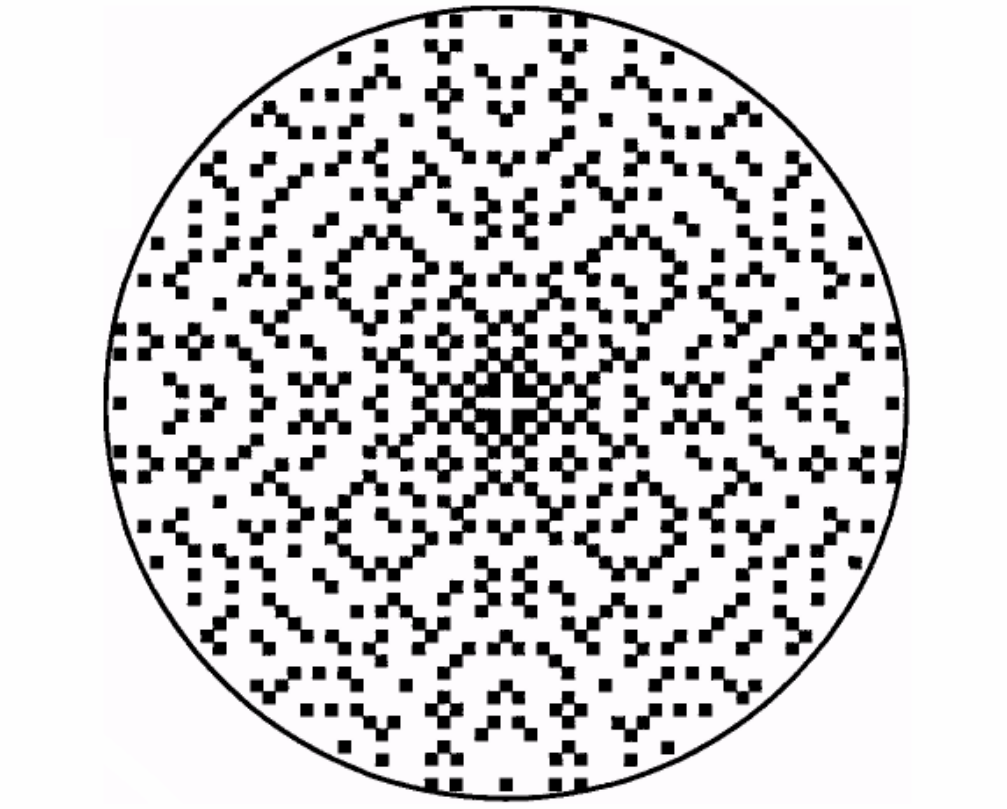
ακέραιοι, ενώ ο $\omega = \frac{1}{2}(-1 + i\sqrt{3}) = e^{2\pi i/3}$, δηλαδή είναι η μία από τις δύο μη πραγματικές κυβικές ρίζες της μονάδας. Οι εικόνες των αριθμών αυτών στο μιγαδικό επίπεδο δημιουργούν ένα δικτυωτό τριγωνικό πλέγμα, σε αντίθεση με το τετραγωνικό πλέγμα που όπως έχουμε δει δημιουργούν οι εικόνες των ακεραίων Gauss.

Ολοκληρώνοντας λοιπόν την παρουσίαση των επιμέρους δακτυλίων πάνω στο $\mathbb{Z}[i]$ καθώς και την ανάλυση της δομής τους πιστεύουμε να έχουμε επιτύχει τον στόχο μας. Ο οποίος δεν ήταν άλλος παρά μια προσιτή προσέγγιση του επιμερισμού αυτού του συνόλου, ώστε να γίνει περισσότερο κατανοητή η γενική του σύνθεση. Ενός συνόλου με ιδιότητες και χαρακτηριστικά αξιοσημείωτα, που όπως μας δόθηκε πολλές φορές η ευκαιρία να δούμε, αφενός μεν διευρύνει το σύνολο των πραγματικών ακεραίων, αφετέρου περιορίζει το αντίστοιχο των μιγαδικών. Διατηρώντας όμως σε κάθε περίπτωση μια λεπτή ισορροπία, μεταξύ αυτών των δύο συνόλων, είτε επεκτείνοντας τα διακριτικά γνωρίσματα του ενός, είτε περιοριορίζοντας τα αντίστοιχα του δευτέρου.

Πίνακας πρώτων ακεραίων Gauss με στάθμη μικρότερη του 1000.

Στάθμη	Ακέραιος	Στάθμη	Ακέραιος	Στάθμη	Ακέραιος
2	1+i	149	7+10i 10+7i	361	19
5	1+2i 2+i	157	6+11i 11+6i	373	7+18i 18+7i
9	3	173	2+13i 13+2i	389	10+17i 17+10i
13	2+3i 3+2i	181	9+10i 10+9i	397	6+19i 19+6i
17	1+4i 4+i	193	7+12i 12+7i	401	1+20i 20+i
29	2+5i 5+2i	197	1+14i 14+i	409	3+20i 20+3i
37	1+6i 6+i	229	2+15i 15+2i	421	14+15i 15+14i
41	4+5i 5+4i	233	8+13i 13+8i	433	12+17i 17+12i
49	7	241	4+15i 15+4i	449	7+20i 20+7i
53	2+7i 7+2i	257	1+16i 16+i	457	4+21i 21+4i
61	5+6i 6+5i	269	10+13i 13+10i	461	10+19i 19+10i
73	3+8i 8+3i	277	9+14i 14+9i	593	8+23i 23+8i
89	5+8i 8+5i	281	5+16i 16+5i	601	5+24i 24+5i
97	4+9i 9+4i	293	2+17i 17+2i	613	17+18i 18+17i
101	1+10i 10+i	313	12+13i 13+12i	617	16+19i 19+16i
109	3+10i 10+3i	317	11+14i 14+11i	641	4+25i 25+4i
113	7+8i 8+7i	337	9+16i 16+9i	653	13+22i 22+13i
121	11	349	5+18i 18+5i	661	6+25i 25+6i
137	4+11i 11+4i	353	8+17i 17+8i	673	12+23i 23+12i

Στάθμη	Ακέραιος	Στάθμη	Ακέραιος	Στάθμη	Ακέραιος
677	1+26i 26+i	797	11+26i 26+11i	929	20+23i 23+20i
701	5+26i 26+5i	809	5+28i 28+5i	937	19+24i 24+19i
709	15+22i 22+15i	821	14+25i 25+14i	941	10+29i 29+10i
733	2+27i 27+2i	829	10+27i 27+10i	953	13+28i 28+13i
757	9+26i 26+9i	853	18+23i 23+18i	961	31
761	19+20i 20+19i	857	4+29i 29+4i	977	4+31i 31+4i
769	12+25i 25+12i	877	6+29i 29+6i	997	6+31i 31+6i
773	17+22i 22+17i	881	16+25i 25+16i		



Γραφική απεικόνιση των πρώτων Gauss με στάθμη μικρότερη του 1000

Πίνακας παραγοντοποίησης σε πρώτους των ακεραίων Gauss που έχουν στάθμη μικρότερη ίση του 200.

Στάθμη	Ακέραιος	Παράγοντες	Στάθμη	Ακέραιος	Παράγοντες
4	2	$-i(1+i)^2$	64	8	$i(1+i)^6$
8	2+2i	$-i(1+i)^3$	65	1+8i 4+7i 7+4i 8+i	$i(2+i)(3-2i)$ $(2+i)(3+2i)$ $i(2-i)(3-2i)$ $(2-i)(3+2i)$
10	1+3i 3+i	$(1+i)(2+i)$ $(1+i)(2-i)$	68	2+8i 8+2i	$(1+i)^2(4-i)$ $-i(1+i)^2(4+i)$
16	4	$-(1+i)^4$	72	6+6i	$-i(1+i)^3 3$
18	3+3i	$(1+i)\cdot 3$	74	5+7i 7+5i	$(1+i)(6+i)$ $(1+i)(6-i)$
20	2+4i 4+2i	$(1+i)^2(2-i)$ $-i\cdot(1+i)^2(2+i)$	80	4+8i 8+4i	$-i(1+i)^4(2-i)$ $-(1+i)^4(2+i)$
25	3+4i 4+3i 5	$(2+i)^2$ $i(2-i)^2$ $(2+i)(2-i)$	81	9	3^2
26	1+5i 5+i	$(1+i)(3+2i)$ $(1+i)(3-2i)$	82	1+9i 9+i	$(1+i)(5+4i)$ $(1+i)(5-4i)$
32	4+4i	$-(1+i)^5$	85	2+9i 6+7i 7+6i 9+2i	$i(2-i)(4+i)$ $i(2-i)(4-i)$ $(2+i)(4+i)$ $(2+i)(4-i)$
34	3+5i 5+3i	$(1+i)(4+i)$ $(1+i)(4-i)$	90	3+9i 9+3i	$(1+i)(2+i)3$ $(1+i)(2-i)3$
36	6	$-i(1+i)^2 3$	98	7+7i	$(1+i)7$
40	2+6i 6+2i	$-i(1+i)^3(2+i)$ $-i(1+i)^3(2-i)$	100	6+8i 8+6i 10	$-i(1+i)^2(2+i)^2$ $(1+i)^2(2-i)^2$ $-i(1+i)^2(2+i)(2-i)$
45	3+6i 6+3i	$i(2-i)\cdot 3$ $(2+i)\cdot 3$	104	2+10i 10+2i	$-i(1+i)^3(3+2i)$ $-i(1+i)^3(3-2i)$
50	1+7i 5+5i 7+i	$i(1+i)(2-i)^2$ $(1+i)(2+i)(2-i)$ $-i(1+i)(2+i)^2$	106	5+9i 9+5i	$(1+i)(7+2i)$ $(1+i)(7-2i)$
52	4+6i 6+4i	$(1+i)^2(3-2i)$ $-i(1+i)^2(3+2i)$	116	4+10i 10+4i	$(1+i)^2(5-2i)$ $-i(1+i)^2(5+2i)$
58	3+7i 7+3i	$(1+i)(5+2i)$ $(1+i)(5-2i)$	117	6+9i 9+6i	$i3(3-2i)$ $3(3+2i)$

Στάθμη	Ακέραιος	Παράγοντες
122	1+11i 11+i	(1+i)(6+5i) (1+i)(6-5i)
125	2+11i 5+10i 10+5i 11+2i	$(2+i)^3$ $i(2+i)(2-i)^2$ $(2+i)^2(2-i)$ $i(2-i)^3$
128	8+8i	$i(1+i)^7$
130	3+11i 7+9i 9+7i 11+3i	i(1+i)(2-i)(3-2i) (1+i)(2-i)(3+2i) (1+i)(2+i)(3-2i) -i(1+i)(2+i)(3+2i)
136	6+10i 10+6i	$-i(1+i)^3(4+i)$ $-i(1+i)^3(4-i)$
144	12	$-(1+i)^43$
145	1+12i 8+9i 9+8i 12+i	i(2-i)(5+2i) (2+i)(5+2i) i(2-i)(5-2i) (2+i)(5-2i)
146	5+11i 11+5i	(1+i)(8+3i) (1+i)(8-3i)
148	2+12i 12+2i	$(1+i)^2(6-i)$ $-i(1+i)^2(6+i)$
153	3+12i 12+3i	i3(4-i) 3(4+i)
160	4+12i 12+4i	$-(1+i)^5(2+i)$ $-(1+i)^5(2-i)$
162	9+9i	$(1+i)3^2$
164	8+10i 10+8i	$(1+i)^2(5-4i)$ $-i(1+i)^2(5+4i)$
169	5+12i 12+5i 13	$(3+2i)^2$ $i(3-2i)^2$ (3+2i)(3-2i)
170	1+13i 7+11i 11+7i 13+i	(1+i)(2+i)(4+i) (1+i)(2+i)(4-i) (1+i)(2-i)(4+i) (1+i)(2-i)(4-i)
178	3+13i 13+3i	(1+i)(8+5i) (1+i)(8-5i)
180	6+12i 12+6i	$(1+i)^2(2-i)3$ $-i(1+i)^2(2+i)3$
185	4+13i 8+11i 11+8i 13+4i	i(2-i)(6+i) i(2-i)(6-i) (2+i)(6+i) (2+i)(6-i)
194	5+13i 13+5i	(1+i)(9+4i) (1+i)(9-4i)
196	14	$-i(1+i)^27$
200	2+14i 10+10i 14+2i	$(1+i)^3(2-i)^2$ $-i(1+i)^3(2+i)(2-i)$ $-(1+i)^3(2+i)^2$

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Ξενόγλωσση Βιβλιογραφία

- **Ash Avner, Cross Robert** (2006) Fearless Symmetry. Exposing the Hidden Patterns of Numbers. *Princeton University Press*.
- **Bourbaki Nicolas** (1970) Elements of Mathematics Algebra I. *Springer – Verlag*.
- **Cohen Henri** (1993) A Course in Computational Algebraic Number Theory. *Springer – Verlag, Berlin*.
- **Connell H. Edwin** (2004) Elements of Abstract and Linear Algebra. *Orange Grove Text Plus*.
- **Conway H. John** (1996) The Book of Numbers. *Springer – Verlag. New York Inc*.
- **Cox David, Little John, O' Shea Donal** (1997) Ideals, Varieties and Algorithms. An Introduction to Commutative Algebra. *Springer – Verlag. New York Inc*.
- **Davenport Harold** (1999) The Higher Arithmetic. An Introduction to the Theory of Numbers. Seventh Edition. *Cambridge University Press*.
- **Gauss Carl Friedrich** (1973) Theoria residuorum biquadraticorum. Commentatio secunda. Comm. Soc. Reg. Sci. Gottingen 7 (1832) reprintedin Werke George Olms. *Verlag. Hildesheim*.
- **Guy K. Richard** (2004) Unsolved Problems in Number Theory. *Springer – Verlag Inc*.
- **Goldman R. Jay** (2004) The Queen of Mathematics: A Historically Motivated Guide to Number Theory. *A. K. Peters Natick Massachusetts*.
- **Hahn Liang – Shin** (1994) Complex Numbers and Geometry. *The Mathematical Association of America*.
- **Harold M. Edwards** (2000) Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory. *Springer – Verlag Inc*.
- **Hungerford W. Thomas** (1996) Abstract Algebra. An Introduction. Second edition. *Saunders College Publishing*.

- **Hungerford W. Thomas** (2000) Algebra. *Springer – Verlag. New York Inc.*
- **Ireland Kenneth Rosen Michael** (1990) A Classical Introduction to Modern Number Theory. Second Edition. *Springer – Verlag. New York Inc.*
- **Katz J. Victor** (1998) A History of Mathematics: An Introduction. *New York. Addison – Wesley, Longman.*
- **Klee Victor Wagon Stan** (1991) Old and New Unsolved Problems in Plane Geometry and Number Theory. *The Mathematical Association of America.*
- **Lam Yuen Tsit** (2001) A First Course in Noncommutative Rings. Second Edition. *Springer – Verlag. New York Inc.*
- **Martinez Carmen, Beivide Ramon** (2007) Codes and Graphs Over Complex Integer Rings. *University of Cantabria. Dpt. Mathematics, Statistics. Doctoral Thesis.*
- **Molin A. Richard** (1996) Quadratics. *CRC Press Boca Raton.*
- **Murty M. Ram, Esmond Jody** (2004) Problems in Algebraic Number Theory. Second Edition. *Springer – Verlag. New York Inc.*
- **Niven Ivan, Zuckerman S. Herbert, Montgomery L. Hugh.** (1991) An Introduction to the Theory of Numbers. *John Wiley & sons, Inc. New York.*
- **Pollard Harry, Diamond G. Harold** (1975) The Theory of Algebraic Numbers. *The Mathematical Association of America. New York Wiley.*
- **Shanks Daniel** (2001) Solved and Unsolved Problems in Number Theory. *American Mathematical Society. Chelsea Publishing.*
- **Stillwell John** (1998) Numbers and Geometry. *Springer – Verlag. New York Inc.*

Άρθρα

- **Calcut S. Jack** (2009) Gaussian Integers and Arctangent Identities for π. *The Mathematical Association of American Monthly Vol. 116 (p. 515 – 530).*
- **Cross T. James** (1983) The Euler's ϕ-function in the Gaussian Integers. *The American Mathematical Monthly. Vol. 90 No. 8 (p. 518 – 528).*

- **Denf Jan, Lipshitz Leonard** (1978) Diophantine Sets Over Some Rings of Algebraic Integers. *Journal of London Mathematical Society. Vol. 18 (p. 385 – 391).*
- **Dresden Greg, Dymacek M. Wayne** (2005) Finding Factors of Factor Rings Over the Gaussian Integers. *The Mathematical Association of America Monthly. Vol. 112 (p. 602 – 611).*
- **Eldridge E. Klauss** (1966) On Ring Structures Determined by Groups. *Proc. American Mathematical Society. Vol. 23 (p. 472 – 477).*
- **Gethner Ellen, Wagon Stan, Wick Brian** (1998) A Stroll Thought the Gaussian Primes. *The American Mathematical Monthly. Vol. 105 No. 4 (p. 327 – 337).*
- **Goldfeld Dorian** (1985) Gauss's Class Number Problem for Imaginary Quadratic Fields. *Bulletin of the American Mathematical Society. Vol. 13 (p. 23 – 37).*
- **Haraty A. Ramzi, El-Kassar N. A.** (2006) A Comparative Study of El Gamal Based Digital Signature Algorithms. *Journal of Computational Methods in Sciences add Engineering. Vol. 6 (p. 147 – 156).*
- **Holben A. C. Jordan H. James** (1968) The Twin Prime Problem and Goldbah's Conjecture in the Gaussian Integers. *The Fibonacci Quarterly No 5 (p. 81 – 85).*
- **Huber Klaus** (1994) Codes Over Gaussian Integers. *IEEE Transactions Information Theory. Vol. 40 (p. 207 – 216).*
- **Jordan H. James, Potratz J. C.** (1965) Complete Residue Systems in the Gaussian Integers. *Mathematics Magazine. Vol. 338 No 1 (p. 1 – 12).*
- **Smith L. Judy, Gallian A. Joseph** (1985) Factoring Finite Factor Rings. Mathematics. *Magazine Mathematical of Association of America. Vol. 58 No 2 (p. 93 – 95).*
- **Stoutemyer R. David** (2009) Unit Normalization of Multinomials Over Gaussian Integers. *ACM Communication in Computer Algebra. Vol. 43 No 3 (p. 73 – 76).*

Ελληνόγλωσση Βιβλιογραφία

- **Βάρσος Δημήτριος, Δεριζιώτης Δημήτριος, Μαλιάκας Μιχαήλ, Παπασταυρίδης Σταύρος, Ράπτης Ευάγγελος, Ταλέλλη Ολυμπία** (2003) Εισαγωγή στη Γραμμική Άλγεβρα. Τόμος Α. *Εκδ. Σοφία*.
- **Βάρσος Δημήτριος, Δεριζιώτης Δημήτριος, Μαλιάκας Μιχαήλ, Ταλέλλη Ολυμπία** (2005) Εισαγωγή στη Γραμμική Άλγεβρα. Τόμος Β. Νέα Έκδοση. *Εκδ. Σοφία*.
- **Βάρσος Δημήτριος, Δεριζιώτης Δημήτριος, Μαλιάκας Μιχαήλ, Ταλέλλη Ολυμπία** (2005) Μια Εισαγωγή στην Άλγεβρα. Νέα Έκδοση. *Εκδ. Σοφία*.
- **Δρόσος Α. Κώστας** (2005) Εισαγωγή στην Μαθηματική Σκέψη. Τόμος 2. Θεμελιώδεις Έννοιες και Θεμέλια των Μαθηματικών. *Εκδόσεις Πανεπιστημίου Πατρών*.
- **Πάμφιλος Πάρις** (2002) Εισαγωγή στην θεωρία ομάδων. *Πανεπιστημιακές Εκδόσεις Κρήτης*.
- **Bell T. Eric** (2006) Οι Μαθηματικοί. Τόμοι Ι και ΙΙ. *Πανεπιστημιακές Εκδόσεις Κρήτης*.
- **Davis M. Donald** (2007) Η Φύση και η Δύναμη των Μαθηματικών. *Πανεπιστημιακές Εκδόσεις Κρήτης*.
- **Fraleigh B. John** (2003) Εισαγωγή στην Άλγεβρα. Τέταρτη Έκδοση. *Πανεπιστημιακές Εκδόσεις Κρήτης*.
- **Hurwitz Adolph, Κριτικός Νικόλαος** (1981) Μαθήματα Αριθμοθεωρίας. *Γ. Α. Πνευματικού*.
- **Morris O. Alun** (1980) Μια Εισαγωγή στη Γραμμική Άλγεβρα. *Γ. Α. Πνευματικού*.
- **Singh Simon** (1998) Το Τελευταίο Θεώρημα του Fermat. *Π. Τραυλός*.
- **Tent B. Margaret** (2007) Ο Πρίγκιπας των Μαθηματικών. *Π. Τραυλός*.
- **Van Der Waerden L. Bartel** (2003) Η Αφύπνιση της Επιστήμης. Δεύτερη Έκδοση. *Πανεπιστημιακές Εκδόσεις Κρήτης*.