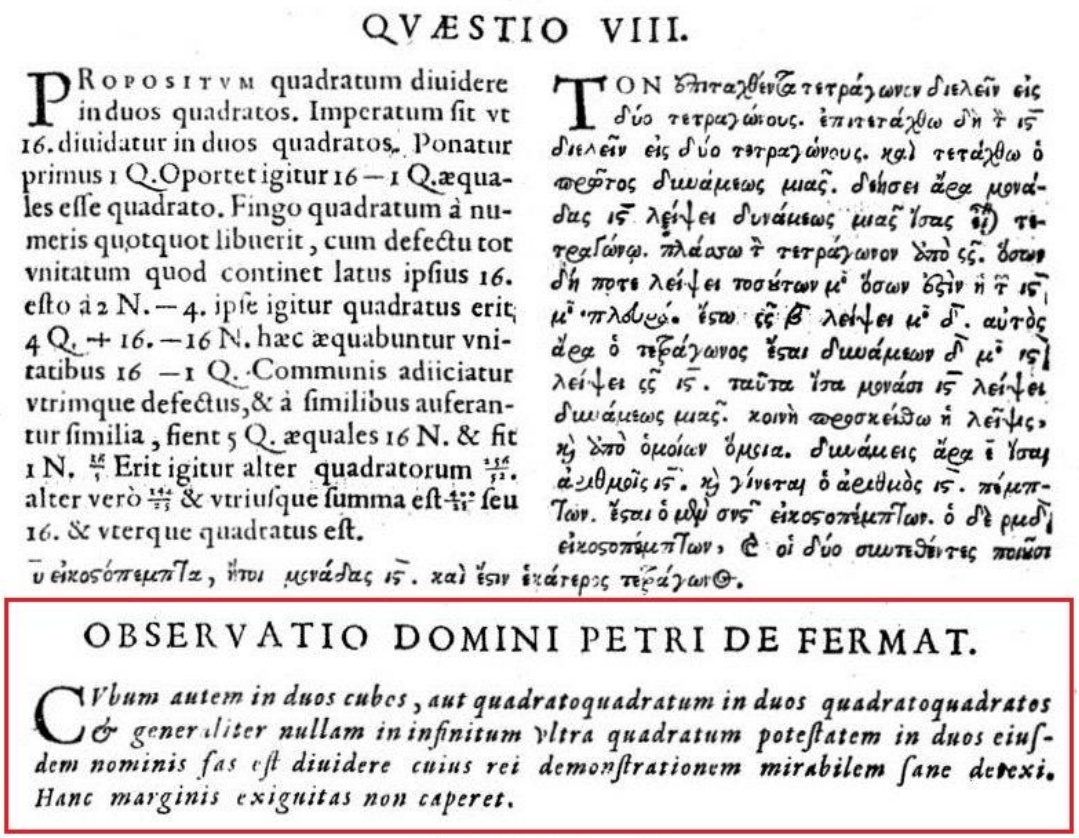

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 — 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. — 4. ipse igitur quadratus erit 4 Q. + 16. — 16 N. hæc æquabuntur vnitatibus 16 — 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

Τὸν δοθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δή τὸ ις διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις λεῖψει δυνάμεως μιᾶς ἴσας ϛα τετραγώνῳ. πλάσω τὸ τετράγωνον ἀπὸ ης. ὅσων δή ποτε λείψει τοσούτων μ̄ ὅσων ὄξις ἡ τοῦ ις μ̄ πλευρά. ἔσω ης β λείψει μ̄ δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσαι δυνάμεων δ μ̄ ις λείψει ης ις. ταῦτα ἴσα μονάσι ις λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ις. καὶ γίνεται ὁ ἀριθμὸς ις. πέμπτων. ἔσαι ὁ μὲν εἷς εἰκοσιπέμπτων. ὁ δὲ ρμδ εἰκοσιπέμπτων, ἃ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοσιπέμπτα, ἴσοι μονάδας ις. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Εύρεση Πυθαγορείων τριάδων με χρήση ακεραίων του Gauss

Στην παράγραφο αυτή θα λύσουμε το πρόβλημα της εύρεσης των Πυθαγορείων τριάδων με χρήση των ακεραίων του Gauss, δηλαδή των αριθμών του συνόλου $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}] = \{a + bi \; με \; a, b \in \mathbb{Z}\}$. Σε ένα άλλο άρθρο θα δούμε αναλυτικά τις ιδιότητες αυτού του αριθμητικού δακτυλίου. Εδώ θα θεωρήσουμε γνωστά κάποια βασικά αποτελέσματα για το $\mathbb{Z}[i]$.

Οι «ακέραιοι» του $\mathbb{Z}[i]$ έχουν τη μορφή $\alpha+\beta i$ με $\alpha,\beta \in \mathbb{Z}$. Νόρμα του αριθμού $\alpha+\beta i$ ονομάζουμε τον αριθμό $N(\alpha+\beta i)=\alpha^2+\beta^2$. Η νόρμα έχει την πολλαπλασιαστική ιδιότητα: $N(Z_1Z_2)=N(Z_1)N(Z_2)$ για κάθε $Z_1, Z_2 \in \mathbb{Z}[i]$. Είναι φανερό ότι η νόρμα ενός στοιχείου του $\mathbb{Z}[i]$ είναι πάντοτε ένας συνηθισμένος ακέραιος του $\mathbb{Z}$.

Τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}[i]$ τα ονομάζουμε και μονάδες του δακτυλίου. Πολύ εύκολα προκύπτει ότι το στοιχείο $\alpha+\beta i$ είναι μονάδα του $\mathbb{Z}[i]$ αν και μόνο αν $N(\alpha+\beta i)=1$. Έτσι προκύπτει ότι οι μονάδες του $\mathbb{Z}[i]$ είναι τα στοιχεία του συνόλου $\{-1,+1,i,-i\}$. Η διαιρετότητα στο δακτύλιο Gauss ορίζεται όπως και στους συνήθεις ακεραίους. Δηλαδή $z/w \Leftrightarrow w=z\,t$ για κάποιο $t \in \mathbb{Z}[i]$. Αν δυο αριθμοί z, w του $\mathbb{Z}[i]$ αλληλοδιαιρούνται τότε υπάρχει μονάδα u ώστε $w=zu$.
Αν z/w τότε λόγω της πολλαπλασιαστικής ιδιότητας της νόρμας θα είναι $N(z)/N(w)$.

Ένας αριθμός $\rho \in \mathbb{Z}[i]$ καλείται πρώτος, όταν ο ρ δεν είναι μονάδα και από την ανάλυση $\rho=\alpha\beta$ με $\alpha,\beta \in \mathbb{Z}[i]$, προκύπτει ότι είτε ο α είτε ο β είναι μονάδα. Αν για τον πρώτο αριθμό ρ ισχύει ρ/zw τότε ρ/z ή ρ/w.

Ο δακτύλιος $\mathbb{Z}[i]$ είναι δακτύλιος με μονοσήμαντη ανάλυση. Αυτό σημαίνει ότι κάθε μη μηδενικό στοιχείο που δεν είναι μονάδα γράφεται ως γινόμενο πρώτων αριθμών του δακτυλίου, και αυτή η ανάλυση σε γινόμενο πρώτων είναι μοναδική με την εξής έννοια.

Αν $\alpha=\alpha_1\alpha_2 \ldots\alpha_\kappa$ και $\alpha=\beta_1\beta_2 \ldots\beta_\lambda$ είναι δυο αναλύσεις του α σε γινόμενο πρώτων αριθμών τότε $\kappa=\lambda$ και για κάθε j, υπάρχει μονάδα u_j , έτσι ώστε $\alpha_j = u_j \beta_j$.

Το πρόβλημα:

Να λυθεί η Διοφαντική εξίσωση $\chi^2+\psi^2=\omega^2$ με $\chi\wedge\psi=1$ και $\chi,\psi,\omega>0$.

Όπως ήδη έχουμε δεί μπορούμε να υποθέσουμε ότι χ άρτιος, ψ περιττός, ω περιττός. Έχουμε λοιπόν $(\chi+\psi i)(\chi-\psi i)=\omega^2$ (1). Θα δείξουμε ότι οι $\chi+\psi i$, $\chi-\psi i$ είναι πρώτοι μεταξύ τους. Πράγματι αν ο πρώτος ρ διαιρεί τους $\chi+\psi i$, $\chi-\psi i$ τότε $\rho/2\chi$ και $\rho/2\psi i$. Από την σχέση $\rho/2\chi$ έχουμε $\rho/2$ ή ρ/χ. Αν ρ/χ τότε αφού επίσης $\rho/\chi+\psi i$ θα είχαμε $\rho/\psi i$ και αφού i είναι μονάδα θα έπρεπε ρ/ψ άτοπο αφού $\chi\wedge\psi=1$. Μένει λοιπόν η περίπτωση $\rho/2$. Τότε $N(\rho)/N(2)$ άρα $N(\rho)/4$ οπότε $N(\rho)=2$ ή 4. (Δεν μπορεί να είναι $N(\rho)=1$ γιατί ο ρ είναι πρώτος). Τώρα όμως αφού ρ/ω θα είναι $N(\rho)/N(\omega)$ δηλαδή $N(\rho)/\omega^2$. Αυτό σημαίνει ότι ο ω θα έπρεπε να είναι άρτιος αριθμός, πράγμα άτοπο. Έτσι δείξαμε ότι οι $\chi+\psi i$, $\chi-\psi i$ είναι πρώτοι μεταξύ τους.

Από την (1) προκύπτει πως πρέπει να υπάρχουν ακέραιοι $\alpha,\beta \in \mathbb{Z}$ έτσι ώστε να ισχύει $\chi+\psi i=u(\alpha+\beta i)^2$, όπου u μονάδα του $\mathbb{Z}[i]$.

- Αν $u=1$ βρίσκουμε $\chi=\alpha^2-\beta^2$, $\psi=2\alpha\beta$ αδύνατη αφού ο ψ υποτέθηκε περιττός.
- Αν $u=-1$ τότε $\chi+\psi i=-1(\alpha+\beta i)^2=(\beta-\alpha i)^2$. Άρα $\chi=\beta^2-\alpha^2$, $\psi=-2\alpha\beta$ αδύνατη.
- Αν $u=i$ τότε $\chi+\psi i=i(\alpha+\beta i)^2=-2\alpha\beta+i(\alpha^2-\beta^2)$, έτσι $\chi=-2\alpha\beta$, $\psi=\alpha^2-\beta^2$ (2).
- Αν $u=-i$ τότε $\chi+\psi i=-i(\alpha+\beta i)^2$ κι έτσι $\chi=2\alpha\beta$, $\psi=\beta^2-\alpha^2$ (3).

Από τις παραπάνω σχέσεις (2),(3) προκύπτει πως γενικά υπάρχουν ακέραιοι $\kappa,\lambda \in \mathbb{Z}$ έτσι ώστε να είναι $\chi=2\kappa\lambda$, $\psi=\kappa^2-\lambda^2$. Φυσικά τότε $\omega=\kappa^2+\lambda^2$. Προφανώς πρέπει $\kappa\wedge\lambda=1$ και οι κ,λ ανισότιμοι mod2, δηλαδή ο ένας άρτιος και ο άλλος περιττός.

Καταλήγουμε επομένως στο εξής συμπέρασμα:

Οι λύσεις της εξίσωσης $\chi^2+\psi^2=\omega^2$ με $\chi,\psi,\omega>0$ και $\chi\wedge\psi=1$ δίνονται από τις σχέσεις $\chi=2\kappa\lambda$, $\psi=\kappa^2-\lambda^2$, $\omega=\kappa^2+\lambda^2$ όπου $\kappa\wedge\lambda=1$, $\kappa>\lambda$, κ,λ ανισότιμοι mod2.