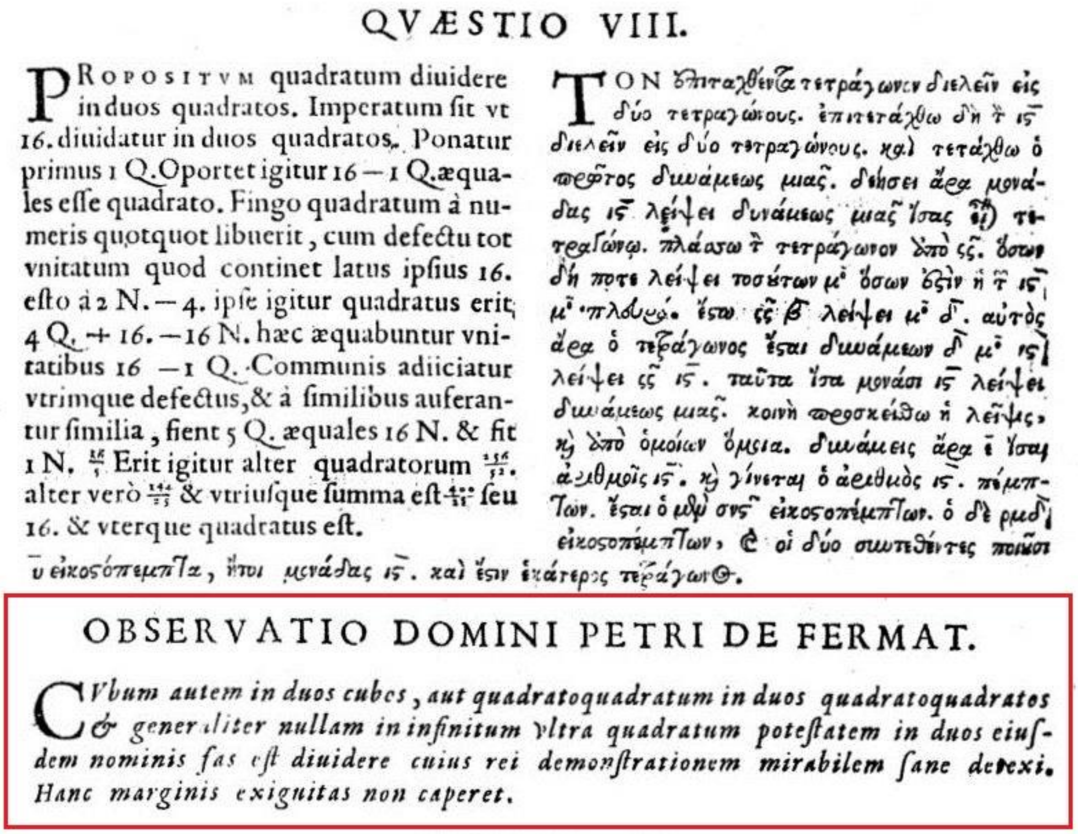

QVÆSTIO VIII.

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. 16/5 Erit igitur alter quadratorum 256/25. alter verò 144/25 & vtriusque summa est 400/25 seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ιϛ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ιϛ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ϛϛ. ὅσων δή ποτε λείψει τοσούτων μο ὅσων ἐστὶν ἡ τῶν ιϛ μο πλευρά. ἔστω ϛϛ β λείψει μο δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μο ιϛ λείψει ϛϛ ιϛ. ταῦτα ἴσα μονάσι ιϛ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ιϛ. καὶ γίνεται ὁ ἀριθμὸς ιϛ πέμπτων. ἔσται ὁ μὲν σνϛ εἰκοστοπέμπτων. ὁ δὲ ρμδ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοστόπεμπτα, ἤτοι μονάδας ιϛ. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

*Cubum 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.*

*Είναι αδύνατον μια κυβική δύναμη να γραφεί ως άθροισμα δυο 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 ίδιων δυνάμεων. Έχω μια πραγματικά υπέροχη απόδειξη της πρότασης, που όμως δε χωρά σ' ένα τόσο στενό περιθώριο.*

Pierre de Fermat 1601-1665

## Το θεώρημα του Fermat για N=3 και N=4

Όπως είδαμε σε προηγούμενο άρθρο, το δύσκολο σημείο για την απόδειξη του θεωρήματος Fermat για τον εκθέτη 3, ήταν η απόδειξη του παρακάτω λήμματος:

***Λήμμα 1 (Euler): Αν για τους ακέραιους αριθμούς α,β με α^β=1,α≠βmod2, ισχύει $\alpha^2+3\beta^2=\sigma^3$ τότε υπάρχουν ακέραιοι t,w με t^w=1,t≠w mod2, ώστε: $\alpha=t(t^2-9w^2)$, $\beta=3w(t^2-w^2)$, $\sigma=t^2+3w^2$.***

Για την απόδειξη του λήμματος στα πλαίσια της Αλγεβρικής Θεωρίας Αριθμών, θα δουλέψουμε στο δακτύλιο $\mathbb{Z}[\zeta_3]$ όπου $\zeta_3$ είναι η κυβική ρίζα της μονάδας $\zeta_3=\frac{-1+\sqrt{-3}}{2}$ $=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$.

Είναι $\mathbb{Z}[\zeta_3]=\{\ \alpha+\beta\zeta_3\ /\ \alpha,\beta\in\mathbb{Z}\ \}$. Πολύ εύκολα φαίνεται ότι $\mathbb{Z}[\sqrt{-3}]\subset\mathbb{Z}[\zeta_3]$. Ισχύει βέβαια ότι $\zeta_3^3=1$, $\zeta_3^2+\zeta_3+1=0$, $\overline{\zeta_3}=\zeta_3^2$. Αν $w=\alpha+\beta\zeta_3$ είναι αριθμός του δακτυλίου $\mathbb{Z}[\zeta_3]$ ορίζουμε ως νόρμα του αριθμού τον αριθμό $N(w)=w\overline{w}=\alpha^2-\alpha\beta+\beta^2$. Προφανώς $N(w)\in\mathbb{Z}$ και ισχύει η πολλαπλασιαστική ιδιότητα: $N(zw)=N(z)N(w)$.

Τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}[\zeta_3]$ καλούνται και μονάδες. Έτσι αν u είναι μια μονάδα θα πρέπει να υπάρχει κάποιο άλλο στοιχείο του $\mathbb{Z}[\zeta_3]$ ώστε $uu'=1$. Παίρνοντας νόρμες προκύπτει $N(u)N(u')=N(1)=1$. Άρα θα πρέπει $N(u)=1 \Leftrightarrow \alpha^2-\alpha\beta+\beta^2=1 \Leftrightarrow (\alpha-\frac{\beta}{2})^2+\frac{3\beta^2}{4}=1$. Αφού λοιπόν θα πρέπει $\frac{3\beta^2}{4}\leq 1$ θα είναι β=0 ή β=1 ή β=-1 και αντιστοίχως οι τιμές του α θα είναι α=±1, α=0 ή α=1, α=0 ή α=-1. Έτσι τελικά προκύπτει ότι το σύνολο των μονάδων του δακτυλίου $\mathbb{Z}[\zeta_3]$ είναι το σύνολο $U=\{\pm1,\pm\zeta_3,\pm\zeta_3^2\}$. Στα παρακάτω για τυπογραφικούς λόγους θα συμβολίζουμε την τρίτη ρίζα της μονάδας $\zeta_3$, απλά ως ζ. Έτσι θα είναι $\zeta=\frac{-1+\sqrt{-3}}{2}$, οπότε $\sqrt{-3}=2\zeta+1$.

Από τη σχέση $\alpha^2+3\beta^2=\sigma^3$ έχουμε $(\alpha+\beta+2\beta\zeta)(\alpha-\beta-2\zeta\beta)=\sigma^3$ (1). Αν ο πρώτος αριθμός π διαιρούσε και τους δυο παράγοντες στο αριστερό μέλος της (1) τότε θα είχαμε π/2α και π/2β+4βζ ⇔ π/2β(1+2ζ) ⇔ π/2β ή π/1+2ζ.

- Αν π/2α και π/2β τότε αφού α^β=1 θα είναι π/2, άρα N(π)/N(2)=4. Έτσι είτε N(π)=1 άτοπο αφού ένας πρώτος δεν μπορεί να είναι μονάδα, είτε N(π)=2, είτε N(π)=4. Όμως δεδομένου ότι $\pi/\sigma^3$ θα είχαμε $N(\pi)/N(\sigma^3)=\sigma^6$ δηλαδή ο αριθμός $\sigma^6$ άρα και ο σ, θα ήταν άρτιος το οποίο είναι άτοπο.
- Αν π/1+2ζ τότε N(π)/N(1+2ζ). $N(1+2\zeta)=(1+2\zeta)(1+2\bar{\zeta})=1+2(\zeta+\bar{\zeta})+4\zeta\bar{\zeta}=1-2+4=3$. Έτσι θα είχαμε N(π)=3. Επειδή $N(\pi)/\sigma^3 \Rightarrow 3/\sigma^3 \Rightarrow 3/\sigma$. Άρα $3/\alpha^2 \Rightarrow 3/\alpha \Rightarrow 9/\alpha^2$ και αφού $9/\sigma^3$ θα είχαμε τελικά $9/3\beta^2$ δηλαδή 3/β, άτοπο.

Από τα παραπάνω προκύπτει ότι (α+β+2βζ)^(α-β-2βζ)=1 οπότε καθένας από τους παράγοντες του $\sigma^3$ στην ισότητα (1) θα πρέπει να είναι τέλειος κύβος. Έτσι θα υπάρχει μονάδα u ∈ U έτσι ώστε $\alpha+\beta+2\beta\zeta=u(\chi+\psi\zeta)^3$ με $\chi,\psi\in\mathbb{Z}$. (2)
Θα είναι λοιπόν $\alpha+\beta+2\beta\zeta=u\{\chi^3+\psi^3-3\chi\psi^2+(3\chi^2\psi-3\chi\psi^2)\zeta\}$ (3).

- **Αν u=1**, τότε $\alpha+\beta=\chi^3+\psi^3-3\chi\psi^2$ (4) και $2\beta=3\chi^2\psi-3\chi\psi^2$ (5). Αφού α^β=1 και α≢βmod2 θα πρέπει α+β περιττός και χ^ψ=1. Λύνοντας το σύστημα των

(4),(5) βρίσκουμε $\alpha = (\chi+\psi)^3 - \frac{9\chi\psi(\chi+\psi)}{2}$, $\beta = \frac{3\chi\psi(\chi-\psi)}{2}$ (7). Οι αριθμοί χ,ψ δεν μπορεί να είναι και οι δυο άρτιοι αφού α^β=1.

- Διακρίνουμε τις περιπτώσεις:

  i) **Οι χ,ψ είναι περιττοί**. Θέτουμε $\begin{cases}\chi = -t+w \\ \psi = -t-w\end{cases}$ (8). Είναι πολύ απλό να διαπιστώσουμε ότι το σύστημα (8) με αγνώστους t,w έχει πάντα λύση στους ακέραιους αριθμούς. Αντικαθιστώντας στην (7) βρίσκουμε τελικά $\alpha=t(t^2-9w^2)$ και $\beta=3w(t^2-w^2)$. (9)

  ii) **Αν ο χ είναι άρτιος και ο ψ περιττός** θέτουμε $\begin{cases}\chi = -2w \\ \psi = -w+t\end{cases}$ (10), οπότε αντικαθιστώντας στις (7) βρίσκουμε $\alpha=t(t^2-w^2)$ και $\beta=w(t^2-9w^2)$ (11).

  iii) **Αν ο ψ είναι άρτιος και ο χ περιττός** θέτουμε $\begin{cases}\chi = w+t \\ \psi = 2w\end{cases}$ (12) και από τις (7) και πάλι βρίσκουμε $\alpha=t(t^2-w^2)$ και $\beta=w(t^2-9w^2)$ (13).

  Σε κάθε περίπτωση λοιπόν υπάρχουν ακέραιοι t,w ώστε $\alpha=t(t^2-w^2)$ και $\beta=w(t^2-9w^2)$ . Από την εξίσωση $\alpha^2+3\beta^2=\sigma^3$ προκύπτει τότε $\sigma=t^2+3w^2$.
- Αν **u=-1**, ομοίως βρίσκουμε $-\alpha=t(t^2-9w^2)$ και $-\beta=3w(t^2-w^2)$ οπότε θέτοντας T=-t, W=-w και πάλι θα είναι $\alpha=T(T^2-9W^2)$, $\beta=3W(T^2-W^2)$, $\sigma=T^2+3W^2$.
- Αν **u=ζ**. Τότε $\alpha+\beta+2\beta\zeta=\zeta(\chi^3+\psi^3-3\chi\psi^2)+3\chi\psi(\chi-\psi)\zeta^2=$
  $=-3\chi\psi(\chi-\psi)+\zeta[\chi^3+\psi^3-3\chi\psi^2-3\chi\psi(\chi-\psi)]$ κι επομένως θα έχουμε $\alpha+\beta=-3\chi\psi(\chi-\psi)$, δηλαδή ένας περιττός αριθμός ισούται με έναν άρτιο, άτοπο.
- Αν **u=-ζ**, παρομοίως καταλήγουμε σε άτοπο.
- Αν **u=ζ²**, τότε $\alpha+\beta+2\beta\zeta=\chi^3+\psi^3-3\chi\psi^2(-\zeta-1)+3\chi\psi(\chi-\psi)=$
  $= \chi^3+\psi^3-3\chi\psi^2+3\chi\psi(\chi-\psi)+(-\chi^3-\psi^3+3\chi\psi^2)\zeta$
  οπότε $\begin{cases}\alpha+\beta = \chi^3+\psi^3-3\chi\psi^2+3\chi\psi(\chi-\psi) \\ 2\beta = -\chi^3-\psi^3+3\chi\psi^2\end{cases}$ (14). Αν τώρα οι ακέραιοι χ,ψ ήταν ταυτόχρονα άρτιοι, από την (14) θα προέκυπτε ότι 2/α και 2/β, άτοπο. Έτσι από την δεύτερη ισότητα των (14) προκύπτει το άτοπο: άρτιος=περιττός.
- Αν $u=-\zeta^2$, ομοίως καταλήγουμε σε άτοπο.

Από όλα τα προηγούμενα προκύπτει τελικά ότι αν $\boldsymbol{\alpha^2+3\beta^2=\sigma^3}$, α^β=1, σ περιττός, τότε υπάρχουν ακέραιοι t,w έτσι ώστε $\boldsymbol{\alpha=t(t^2-9w^2)}$, $\boldsymbol{\beta=3w(t^2-w^2)}$, $\boldsymbol{\sigma=t^2+3w^2}$. Επιπλέον για τους t,w έχουμε t^w= , t μη διαρετός με το 3 και $t \neq w \bmod 2$.

Σε **επόμενο άρθρο** θα δώσουμε και άλλη μια λύση του θεωρήματος Fermat για τις περιπτώσεις N=3 και N=4 στα πλαίσια της αλγεβρικής θεωρίας αριθμών. Μάλιστα για την περίπτωση N=3 δεν θα επικαλεστούμε το λήμμα του Euler.