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 δὴ τὸ ις̄ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις̄ λεῖψει δυνάμεως μιᾶς ἴσας ☐ τετραγώνῳ. πλάσω τὸ τετράγωνον ἀπὸ ϛ̄. ὅσων δή ποτε λείψει τοσούτων μ̄ ὅσων ἔχει ἡ τοῦ ις̄ μ̄ πλευρά. ἔστω ϛ̄ β̄ λείψει μ̄ δ̄. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ̄ μ̄ ις̄ λείψει ϛ̄ ις̄. ταῦτα ἴσα μονάσι ις̄ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὁμοῖα. δυνάμεις ἄρα ε̄ ἴσαι ἀριθμοῖς ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄. πέμπτων. ἔσαι ὁ μὲ σὸς εἰκοσιπέμπτων. ὁ δὲ ρμδ̄ εἰκοσιπέμπτων, ☾ οἱ δύο συντεθέντες ποιοῦσι τὸν εἰκοσιπέμπτα, ἴσους μονάδας ις̄. 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.

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

Μέρος Ι: Μια κλασική στοιχειώδης προσέγγιση

Μια βασική πρόταση

Αν για τους ακέραιους α,β,γ ισχύει $\alpha^2=\beta\gamma$, όπου οι αριθμοί β,γ είναι πρώτοι μεταξύ τους, τότε καθένας από τους β και γ είναι ίσος με το τετράγωνο ενός ακεραίου.

<u>απόδειξη 1η</u>

Αν $\alpha=\prod p_i^{a_i}, \beta=\prod p_j^{\beta_j}, \gamma=\prod p_\kappa^{\gamma_\kappa}$ είναι η ανάλυση των α,β,γ σε γινόμενο πρώτων παραγόντων, όπου α_i, β_j , γ_k σχεδόν όλοι μηδέν, θα ισχύει $\prod p_i^{2a_i}=\prod p_j^{\beta_j}\prod p_\kappa^{\gamma_\kappa}$ και δεδομένου ότι οι β και γ δεν έχουν κοινούς πρώτους παράγοντες, θα πρέπει κάθε ένας από τους εκθέτες β_j και γ_k να είναι άρτιος αριθμός. Αυτό όμως σημαίνει ότι καθένας από τους αριθμούς β και γ θα είναι τετράγωνο ενός ακεραίου.

<u>απόδειξη 2η</u>

Έχουμε $\alpha^2=\beta\gamma$ και $\beta\wedge\gamma=1$. Είναι $\beta=\beta\cdot1=\beta\cdot(\beta\wedge\gamma)=\beta^2\wedge\beta\gamma=\beta^2\wedge\alpha^2=(\beta\wedge\gamma)^2$. Ομοίως $\gamma=(\gamma\wedge\alpha)^2$.[1]

Παρατήρηση

Η πρόταση γενικεύεται για οποιαδήποτε δύναμη και οποιοδήποτε γινόμενο παραγόντων πρώτων ανα δύο μεταξύ τους αριθμών. Δηλαδή αν $\alpha_1\alpha_2\ldots\alpha_\kappa=\alpha^\nu$ και οι αριθμοί $\alpha_1, \alpha_2,\ldots,\alpha_\kappa$ είναι ανά δυο πρώτοι μεταξύ τους, τότε καθένας από τους $\alpha_1, \alpha_2,\ldots,\alpha_\kappa$ είναι ν^η δύναμη κάποιου ακεραίου.

[1] Ο συμβολισμός α∧β δηλώνει τον Μέγιστο Κοινό Διαιρέτη των ακεραίων α,β. Δηλ. α∧β=(α,β).

Πυθαγόρειες τριάδες

Να λυθεί η διαφαντική εξίσωση: $\chi^2+\psi^2=\omega^2$.

Λύση

Κατ' αρχή παρατηρούμε πως αν $\chi\wedge\psi=\delta>1$ τότε δ^2/ω^2 οπότε δ/ω. Αν λοιπόν θέσουμε $\chi=\delta\chi'$, $\psi=\delta\psi'$και $\omega=\delta\omega'$τότε η δοθείσα εξίσωση μπορεί να γραφεί $\chi'^2+\psi'^2=\omega'^2$ με $\chi'\wedge\psi'=1$. Φυσικά τότε θα είναι και $\chi'\wedge\omega'=\psi'\wedge\omega'=1$. Έτσι δε βλάπτει τη γενικότητα να αναζητήσουμε λύσεις με την πρόσθετη υπόθεση $\chi\wedge\psi=1$.

Επειδή το τετράγωνο ενός ακεραίου είναι πάντα ισότιμο είτε με 0 είτε με 1 mod4, έπεται ότι οι ακέραιοι χ,ψ δεν μπορεί να είναι και οι δυο άρτιοι ή και οι δυο περιττοί. Υποθέτουμε λοιπόν ότι ο χ είναι άρτιος και ο ψ περιττός. Τότε ο ω θα είναι περιττός.

Έχουμε τώρα $\chi^2+\psi^2=\omega^2 \Leftrightarrow \chi^2=\omega^2-\psi^2 \Leftrightarrow \chi^2=(\omega-\psi)(\omega+\psi)$ **(1)**

Οι αριθμοί ω-ψ και ω+ψ είναι άρτιοι, συνεπώς $4/\chi^2 \Leftrightarrow 2/\chi$. Έτσι η (1) μπορεί να γραφεί ως $(\frac{\chi}{2})^2=\frac{\omega-\psi}{2}\frac{\omega+\psi}{2}$ **(2).**

Οι αριθμοί $\frac{\omega-\psi}{2},\frac{\omega+\psi}{2}$ είναι πρώτοι μεταξύ τους διότι αν ρ είναι ο ΜΚΔ τους τότε $\rho/\frac{\omega-\psi}{2}$ και $\rho/\frac{\omega+\psi}{2}$ οπότε ρ/ω και ρ/ψ επομένως $\rho/\omega\wedge\psi$ δηλαδή ρ/1 άρα ρ=1.

Η σχέση (2) σύμφωνα με την βασική πρόταση που αποδείξαμε προηγουμένως μας δίνει ότι:

$\frac{\omega-\psi}{2}=\alpha^2$ και $\frac{\omega+\psi}{2}=\beta^2$ με $\alpha\wedge\beta=1$.

Θα είναι λοιπόν $\omega=\beta^2+\alpha^2$, $\psi=\beta^2-\alpha^2$ και $\chi=2\alpha\beta$ και καταλήγουμε στο συμπέρασμα ότι οι λύσεις που αναζητούμε έχουν τη μορφή:

$\chi=2\alpha\beta$, $\psi=\beta^2-\alpha^2$, $\omega=\beta^2+\alpha^2$ με $\alpha\wedge\beta=1$, και από τους α, β ο ένας είναι άρτιος και ο άλλος περιττός.

Η γενική λύση της $\chi^2+\psi^2=\omega^2$ δίχως την απαίτηση $\chi\wedge\psi=1$ θα είναι **$\chi=2\kappa\alpha\beta$, $\psi=\kappa(\beta^2-\alpha^2)$, $\omega=\kappa(\beta^2+\alpha^2)$ όπου κ τυχαίος ακέραιος, $\alpha\wedge\beta=1$, και από τους α, β ο ένας είναι άρτιος και ο άλλος περιττός.**

Θεώρημα Fermat για Ν=4

Η διοφαντική εξίσωση $\chi^4+\psi^4=\omega^4$ δεν έχει μη τετριμμένες λύσεις.

απόδειξη

Η απόδειξη θα γίνει με **απαγωγή σε άτοπο** και με χρήση της μεθόδου της **ατέρμονης καθόδου**. Δηλαδή υποθέτοντας ότι η εξίσωση έχει τουλάχιστον μια μη τετριμμένη λύση (χ,ψ,ω) με χψω≠0, θα καταφέρουμε να κατασκευάσουμε άλλη μια λύση της (Χ,Ψ,Ω) με ΧΨΩ≠0 για την οποία |Ω|<|ω|. Αυτό όμως οδηγεί σε άτοπο, γιατί αν επαναλαμβάναμε την ίδια διαδικασία για τη λύση (Χ,Ψ,Ω) θα οδηγούμασταν σε άλλη μια λύση της οποίας η τρίτη συνιστώσα θα ήταν κατ' απόλυτη τιμή μικρότερη της |Ω| και εξακολουθώντας με τον ίδιο τρόπο θα προέκυπτε μια άπειρη γνησίως φθίνουσα ακολουθία φυσικών αριθμών, πράγμα το οποίο είναι αδύνατο.

Η διαδικασία διευκολύνεται πολύ αν αντί της αρχικής εξίσωσης, θεωρήσουμε την εξίσωση $\chi^4+\psi^4=\omega^2$ (2). Προφανώς αν η (2) δεν έχει μη τετριμμένες λύσεις, τότε ούτε και η αρχική θα έχει μη τετριμμένες λύσεις. Ξεκινάμε λοιπόν υποθέτοντας πως η (2) έχει τη λύση (χ,ψ,ω) με χψω≠0 και μάλιστα χ>0, ψ>0, ω>0.

Μπορούμε **να υποθέσουμε ότι χ^ψ=1**. (Αν χ^ψ=δ, τότε δ/χ, δ/ψ, δ^4/ω^2 άρα και δ^2/ω^2 δηλ. δ/ω. Για κάποιους ακεραίους $\chi_1,\psi_1,\omega_1,\omega_2$ θα είχαμε επομένως $\delta^4(\chi_1{}^4+\psi_1{}^4)=\delta^2\omega_1{}^2$, άρα $\delta^2/\omega_1{}^2$ κι έτσι $\chi_1{}^4+\psi_1{}^4=\omega_2{}^2$ με $\chi_1\wedge\psi_1=1$). Επίσης τα χ,ψ δεν μπορεί να είναι αμφότεροι περιττοί γιατί τότε το άθροισμα $\chi^4+\psi^4$ θα ήταν ισοδύναμο με 2mod4 πράγμα αδύνατο αφού υποθέτουμε πως $\chi^4+\psi^4=\omega^2$. Μπορούμε να υποθέσουμε επομένως ότι ο **χ είναι άρτιος και ο ψ περιττός**. Φυσικά ο ω θα είναι περιττός.

Από την εύρεση των Πυθαγορείων τριάδων που κάναμε στην προηγούμενη παράγραφο θα έχουμε τότε ότι υπάρχουν ακέραιοι α,β με α^β=1, α>β>0 ο ένας άρτιος και ο άλλος περιττός, έτσι ώστε

$$\begin{cases} \chi^2 = 2\alpha\beta \\ \psi^2 = \alpha^2 - \beta^2 \\ \omega = \alpha^2 + \beta^2 \end{cases} \qquad (3)$$

Ο **β επιπλέον πρέπει να είναι άρτιος** γιατί διαφορετικά ο α θα ήταν άρτιος και $\psi^2=\alpha^2-\beta^2 \equiv -1 \bmod 4$, που είναι αδύνατο.

Από την δεύτερη εξίσωση παραπάνω έχουμε $\beta^2+\psi^2=\alpha^2$ δηλαδή οι αριθμοί (β,ψ,α) αποτελούν Πυθαγόρεια τριάδα με β^ψ=1, β άρτιος, ψ περιττός.

Θα υπάρχουν επομένως ακέραιοι γ,δ με γ>δ>0, γ^δ=1, ανισότιμοι mod2, έτσι ώστε να ισχύει $\begin{cases} \beta = 2\gamma\delta \\ \psi = \gamma^2 - \delta^2 \\ \alpha = \gamma^2 + \delta^2 \end{cases}$ (4)

Αφού $\chi^2=2\alpha\beta$ θα έχουμε $\chi^2=4\gamma\delta(\gamma^2+\delta^2) \Leftrightarrow (\chi/2)^2=\gamma\delta(\gamma^2+\delta^2)$ (5).

Εύκολα φαίνεται ότι $\gamma\delta\wedge(\gamma^2+\delta^2)=1$, οπότε σύμφωνα με τη αρχική βασική μας πρόταση θα πρέπει να υπάρχουν ακέραιοι Χ,Ψ,Ω έτσι ώστε $\gamma=X^2$, $\delta=\Psi^2$, $\gamma^2+\delta^2=\Omega^2$. Δηλαδή θα είναι $X^4+\Psi^4=\Omega^2$, οπότε η τριάδα (Χ,Ψ,Ω) αποτελεί μια λύση της (2) για την οποία έχουμε ΧΨΩ≠0, Χ^Ψ=1, και $\omega=\alpha^2+\beta^2= (\gamma^2+\delta^2)^2+4\gamma^2\delta^2=\Omega^4>\Omega$ αφού Ω>1.

Υποθέτοντας λοιπόν την ύπαρξη μιας λύσης (χ,ψ,ω) της (2) με ω>0, καταφέραμε να κατασκευάσουμε άλλη μια λύση της (Χ,Ψ,Ω) με 0< Ω<ω. Αυτό όμως όπως έχουμε ήδη επισημάνει είναι άτοπο και η απόδειξη έχει ολοκληρωθεί.

Θεώρημα Fermat για N=3

Η διοφαντική εξίσωση $\chi^3+\psi^3=\omega^3$ δεν έχει μη τετριμμένες λύσεις.

απόδειξη

Τετριμμένες είναι οι λύσεις για τις οποίες χψω=0. Έτσι για παράδειγμα η τριάδα (κ,-κ,0) αποτελεί τετριμμένη λύση για κάθε ακέραιο κ. Θεωρούμε λοιπόν ότι χψω≠0. Επίσης αν χ^ψ=δ, τότε χ=δχ_1, ψ=δψ_2 και επειδή δ^3/ω^3 θα είναι δ/ω δηλαδή ω=δω_1 για κάποιους ακέραιους χ_1,ψ_1,ω_1. Αφού $\chi_1^3+\psi_1^3=\omega_1^3$ και $\chi_1\wedge\psi_1=1$, μπορούμε να υποθέσουμε ότι χ^ψ=1. Τότε φυσικά και ψ^ω=χ^ω=χ^ψ^ω=1. Δίχως βλάβη της γενικότητας μπορούμε επίσης να υποθέσουμε ότι οι αριθμοί χ,ψ είναι περιττοί, ενώ ο ω είναι άρτιος.

Θα ξεκινήσουμε λοιπόν με την υπόθεση ότι υπάρχει λύση (χ,ψ,ω) της $\chi^3+\psi^3=\omega^3$ (1) με χψω≠0, χ^ψ=1, χ,ψ≡1mod2, ω≡0mod2. Μπορούμε να υποθέσουμε επιπλέον ότι έχουμε επιλέξει την τριάδα (χ,ψ,ω) με τέτοιο τρόπο ώστε |ω| να είναι το ελάχιστο δυνατό.

Θα δείξουμε τότε, ότι με τις παραπάνω προϋποθέσεις, μπορούμε να βρούμε άλλη μια λύση (μ,ν,λ) της αρχικής εξίσωσης για την οποία ισχύουν επίσης οι παραπάνω προϋποθέσεις, όμως |λ|<|ω|. Αυτή είναι η περίφημη μέθοδος της **ατέρμονης καθόδου**, η οποία μας οδηγεί σε άτοπο δεδομένου ότι |ω| υποτέθηκε το ελάχιστο δυνατό.(Πράγμα εφικτό αφού |ω| είναι φυσικός αριθμός.)

Θέτουμε χ+ψ=2α και χ-ψ=2β. Τότε χ=α+β και ψ=α-β, με αβ≠0, α^β=1, α≠βmod2, οπότε αντικαθιστώντας στην (1) βρίσκουμε $(\alpha+\beta)^3+(\alpha-\beta)^3=\omega^3$ <=>

$$\mathbf{2\alpha(\alpha^2+3\beta^2)=\omega^3\ (2).}$$

Ο αριθμός $\alpha^2+3\beta^2$ είναι περιττός άρα αν $2\alpha\wedge(\alpha^2+3\beta^2)=\delta$ τότε δ/α και $\delta/3\beta^2$ και επειδή δ^β=1 θα είναι δ/3. Άρα δ=1 ή δ=3.
Διακρίνουμε επομένως δυο περιπτώσεις:

Πρώτη περίπτωση : $2\alpha\wedge(\alpha^2+3\beta^2)=1$
Τότε από την (2) προκύπτει ότι $2\alpha=\rho^3$ (3.1) και $\alpha^2+3\beta^2=\sigma^3$ (3.2).
Ισχύει όμως το εξής

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

Στην περίπτωσή μας λοιπόν θα έχουμε $\alpha=u(u^2-9v^2)$, $\beta=3v(u^2-v^2)$, $\sigma=u^2+3v^2$ (3.3). Από την (3.1-3.3) προκύπτει $2u(u-3v)(u+3v)=\rho^3$ (3.4). Είναι $2u\wedge(u-3v)\wedge(u+3v)=1$ γιατί οι αριθμοί u-3v,u+3v είναι περιττοί και αν ένας πρώτος p/2u, p/u-3v, p/u+3v τότε p/6v και p≠2,3 άρα θα είχαμε p/u, p/v που είναι άτοπο.

Από την (3.4) προκύπτει ότι: $2u=l^3$, $u-3v=m^3$, $u+3v=n^3$ δηλαδή $m^3+n^3=l^3$. Παρατηρούμε τώρα ότι $|\omega|^3=|2\alpha(\alpha^2+3\beta^2)|^3=|2u(u^2-9v^2)(\alpha^2+3\beta^2)|^3=|l|^3|u^2-9v^2)||\alpha^2+3\beta^2|$ επειδή $u^2-9v^2\neq 0$ και $\alpha^2+3\beta^2>1$ προκύπτει ότι $|\omega|>|l|$ το οποίο είναι άτοπο.

Δεύτερη περίπτωση: $2\alpha\wedge(\alpha^2+3\beta^2)=3$

Τότε 3/α και αν γράψουμε α=3γ θα είναι $2\gamma\wedge(\alpha^2+3\beta^2)/3=1\Leftrightarrow 2\gamma\wedge(3\gamma^2+\beta^2)=1$ και επειδή το 3 δεν μπορεί να διαιρεί το β, θα είναι επίσης $18\gamma\wedge(\beta^2+3\gamma^2)=1$. Έτσι $2\alpha(\alpha^2+3\beta^2)=\omega^3\Leftrightarrow 18\gamma(\beta^2+3\gamma^2)=\omega^3$. Θα έχουμε επομένως $18\gamma=\rho^3$ (4.1) και $\beta^2+3\gamma^2=\sigma^3$ (4.2) με $\beta\wedge\gamma=1$. Από το λήμμα 1 συνεπώς προκύπτει ότι υπάρχουν ακέραιοι u,v τέτοιοι ώστε $u\wedge v=1$, $u\neq v \bmod 2$, $\beta=u(u^2-9v^2)$ (4.3), $\gamma=3v(u^2-v^2)$ (4.4).

Από την (4.4) και (4.1) προκύπτει $54v(u-v)(u+v)=\rho^3$. Επειδή $3/\rho^3$ επίσης θα είναι $3/\rho$ κι έτσι η τελευταία ισότητα γράφεται ως $2v(u-v)(u+v)=(\rho/3)^3$.
Όμως $2v\wedge(u-v)\wedge(u+v)=1$ επομένως $2v=l^3$, $v-u=m^3$, $u+v=n^3$
οπότε προκύπτει $m^3+n^3=l^3$.
Παρατηρούμε τώρα ότι $|\omega|^3==|2\alpha(\alpha^2+3\beta^2)|^3=|6\gamma(\alpha^2+3\beta^2)|^3=|18v(u^2-v^2)(\alpha^2+3\beta^2)|^3=|9l^3(u^2-v^2)(\alpha^2+3\beta^2)|^3$. Επειδή $u^2-v^2\neq 0$ και $\alpha^2+3\beta^2>1$ θα είναι $|\omega|>|l|$, άτοπο.
Επομένως δεν υπάρχουν μη τετριμμένες λύσεις της διοφαντικής εξίσωσης $\chi^3+\psi^3=\omega^3$.

Για να ολοκληρωθεί πλήρως η παραπάνω απόδειξη, οφείλουμε να αποδείξουμε τον ισχυρισμό του λήμματος 1. Αυτό δεν είναι και τόσο εύκολο να γίνει όπως θα δούμε στη συνέχεια. Η μορφή της απόδειξης που δόθηκε παραπάνω, ουσιαστικά οφείλεται στον Euler και χρονολογείται από το 1770. Μια κριτική σπουδή της απόδειξης του Euler αποκαλύπτει κάποια σημαντικά κενά που αφορούν τις ιδιότητες διαιρετότητας αριθμών της μορφής $\alpha^2+3\beta^2$. Έτσι ο Euler δεν αποκατέστησε πλήρως την ισχύ του λήμματος 1. Κάτι τέτοιο επιχειρήθηκε από τον Legendre (1808,1830) δίχως και πάλι την αποκατάσταση όλων των λεπτομερειών.

πρόταση 1

Ο πρώτος p γράφεται στη μορφή $\alpha^2+3\beta^2$ αν και μόνο αν p=3 ή $p\equiv 1 \bmod 3$.

<u>απόδειξη</u>

Έστω ότι $p=\alpha^2+3\beta^2$. Τότε $p\equiv\alpha^2 \bmod 3\equiv 1 \bmod 3$ αν $\alpha\neq 0$, ενώ p=3 αν α=0.
Αντίστροφα, αν p=3 τότε $3=0^2+3\cdot 1^2$. Έστω λοιπόν $p\neq 3$ και $p\equiv 1 \bmod 3$. Από τον νόμο της τετραγωνικής αντιστροφής έχουμε $\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right)=\left(\frac{p}{3}\right)$ και αφού $p\equiv 1 \bmod 3$ θα είναι τελικά $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)=1$ οπότε το -3 είναι τετραγωνικό υπόλοιπο mod3, δηλαδή υπάρχει t, $0<t\leq p-1$, ώστε $t^2\equiv -3 mod p$. (1)

Θεωρούμε τους αριθμούς $m+nt$ με $0\leq m,n\leq[\sqrt{p}]$. Αφού το πλήθος των ζευγών (m,n) είναι $([\sqrt{p}]+1)^2>\sqrt{p}^2=p$, ακόμη και στην περίπτωση όπου όλοι οι παραπάνω αριθμοί είναι διαφορετικοί μεταξύ τους, θα υπάρχουν ακέραιοι m_1,m_2,n_1,n_2 τέτοιοι ώστε

$m_1+n_1t\equiv m_2+n_2t$ modp $\Leftrightarrow$ $m_1-m_2\equiv(n_2-n_1)t$ modp (2). Είναι $m_1\neq m_2$, $n_1\neq n_2$ (διαφορετικά ο p θα έπρεπε να διαιρεί έναν ακέραιο μικρότερό του).
Αν λοιπόν θέσουμε $\alpha=m_1-m_2$ και $\beta=n_2-n_1$ θα είναι $\alpha,\beta\neq0$ και $\alpha\equiv\beta t$ modp.
Θα έχουμε λοιπόν $\alpha^2\equiv\beta^2t^2$modp. (3).
Από τις (1),(3) προκύπτει $\alpha^2+3\beta^2\equiv0$ modp, δηλαδή υπάρχει ακέραιος κ, ώστε $\alpha^2+3\beta^2=\kappa p$. Όμως $|\alpha|,|\beta|\leq\lceil\sqrt{p}\rceil<\sqrt{p}$, επομένως $\alpha^2+3\beta^2<4p$.
Συνεπώς θα είναι κ=1 ή κ=2 ή κ=3.
Αν κ=1, τότε $\alpha^2+3\beta^2=p$
Αν κ=2, τότε $\alpha^2+3\beta^2=2p$. Οι α,β πρέπει να είναι ισότιμοι mod2. Όμως τότε $\alpha^2+3\beta^2\equiv0$ mod4, πράγμα που σημαίνει ότι ο p θα είναι άρτιος, άτοπο.
Αν κ=3, τότε $\alpha^2+3\beta^2=3p$, άρα $3/\alpha^2$, οπότε $3/\alpha$. Αν $\alpha=3\alpha'$ με αντικατάσταση στη σχέση $\alpha^2+3\beta^2=3p$, θα έχουμε $9\alpha^2+3\beta^2=3p \Leftrightarrow \beta^2+3\alpha'^2=p$.
Από τα παραπάνω γίνεται φανερό πως ο p έχει τη μορφή $\chi^2+3\psi^2$. ο.ε.δ.

πρόταση 2

Αν ο πρώτος p διαιρεί έναν περιττό αριθμό της μορφής u^2+3v^2, $u\wedge v=1$, τότε ο p καθώς και το πηλίκο της διαίρεσης των u^2+3v^2 και p, έχουν την ίδια μορφή και υπάρχουν ακέραιοι α,β,κ,λ ώστε να ισχύει
$$u+\sqrt{-3}v=(\alpha\pm\sqrt{-3}\beta)(\kappa+\sqrt{-3}\lambda)$$
όπου $\alpha^2+3\beta^2=p$ και $\alpha,\beta\geq0$, $\alpha\wedge\beta=1$.

απόδειξη

Αν p=3, τότε $3=0+3\cdot1^2$.
Αν p≠3 τότε επειδή p δεν διαιρεί τον v (αφού $u\wedge v=1$), θα υπάρχει v΄ τέτοιος ώστε $vv'\equiv1$modp. Αν $m=u^2+3v^2$, τότε $mv'=(uv')^2+3vv'$, συνεπώς $(uv')^2\equiv-3$modp. Δηλαδή το -3 είναι τετραγωνικό υπόλοιπο modp. Από το νόμο της τετραγωνικής αντιστροφής $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)=1$. Έτσι προκύπτει ότι p≡1mod3, και σύμφωνα με την πρόταση 1 θα είναι $p=\alpha^2+3\beta^2$, για κάποιους ακέραιους α,β με $\alpha\wedge\beta=1$.
Αφού p/u^2+3v^2 θα είναι $u^2+3v^2=(\alpha^2+3\beta^2)\tau$. Έτσι $\tau=\frac{u^2+3v^2}{\alpha^2+3\beta^2}=\frac{(u^2+3v^2)(\alpha^2+3\beta^2)}{(\alpha^2+3\beta^2)^2}=\frac{(\alpha u\pm3\beta v)^2+3(\alpha v\mp\beta u)^2}{(\alpha^2+3\beta^2)^2}$ (2.1)
Παρατηρούμε τώρα ότι : $(\alpha u+3\beta v)(\alpha u-3\beta v)=\alpha^2u^2-9\beta^2v^2=\alpha^2u^2+3\alpha^2v^2-3\alpha^2v^2-9\beta^2v^2=\alpha^2(u^2+3v^2)-3v^2(\alpha^2+3\beta^2)=\alpha^2p\tau-3v^2p$. Έτσι $p/(\alpha u+3\beta v)(\alpha u-3\beta v)$ πράγμα που σημαίνει ότι $p/\alpha u+3\beta v$ ή $p/\alpha u-3\beta v$. Σε κάθε περίπτωση από την (2.1) προκύπτει ότι επίσης ο πρώτος p θα διαιρεί τον $\alpha v-u\beta$ ή τον $\alpha v+u\beta$ αντιστοίχως.
Οι αριθμοί επομένως $\gamma=\frac{\alpha u\pm3\beta v}{\alpha^2+3\beta^2}$ και $\delta=\frac{\beta u\mp\alpha v}{\alpha^2+3\beta^2}$ είναι ακέραιοι και θα έχουμε $\tau=\gamma^2+3\delta^2$.
Είναι $(\alpha\pm\sqrt{-3}\beta)(\gamma\mp\sqrt{-3}\delta)=(\alpha\gamma+3\beta\delta)\pm3(\beta\gamma-\alpha\delta)\sqrt{-3}$. Επίσης παρατηρούμε ότι:
$$\alpha\gamma+3\beta\delta=\frac{\alpha^2u\pm3v\alpha\beta+3\beta^2u\mp3\alpha\beta v}{p}=u$$
$$\beta\gamma-\alpha\delta=\frac{\beta\alpha u\pm3\beta^2v-\alpha\beta u\pm\alpha^2v}{p}=\pm v$$

Έτσι $(\alpha \pm \sqrt{-3}\beta)(\gamma \mp \sqrt{-3}\delta) = u + v\sqrt{-3}$.
Αναλυτικότερα αν p/ αu+3βv τότε $(\alpha + \sqrt{-3}\beta)(\gamma - \sqrt{-3}\delta) = u + v\sqrt{-3}$.
αν p/ αu-3βv τότε $(\alpha - \sqrt{-3}\beta)(\gamma + \sqrt{-3}\delta) = u + v\sqrt{-3}$.
Από τις τελευταίες ισότητες προκύπτει το ζητούμενο.

πρόταση 3

Αν p=3, ή p≡1mod3, η αναπαράσταση $p=\alpha^2+3\beta^2$ με α,β≥0 είναι μοναδική.

απόδειξη

Αν υποθέσουμε ότι υπάρχουν δυο αναπαραστάσεις διαφορετικές, τότε θα υπάρχουν ακέραιοι α,β,χ,ψ≥0 ώστε $\alpha^2+3\beta^2=\chi^2+3\psi^2$. Αφού $\alpha^2+3\beta^2$/ $\chi^2+3\psi^2$ σύμφωνα με την προηγούμενη πρόταση $\chi + \psi\sqrt{-3} = (\alpha \pm \beta\sqrt{-3})(\kappa + \lambda\sqrt{-3})$. Παίρνοντας συζυγείς και πολλαπλασιάζοντας τις αντίστοιχες σχέσεις λαμβάνουμε $\chi^2+3\psi^2=(\alpha^2+3\beta^2)(\kappa^2+3\lambda^2)$ οπότε $\kappa^2+3\lambda^2=1$, δηλαδή κ=±1,λ=0. Έτσι η μόνη αποδεκτή λύση είναι να έχουμε χ=α και ψ=β.

πρόταση 4

Αν ο περιττός αριθμός $m=u^2+3v^2$ με u∧v=1 είναι δύναμη ενός πρώτου p, δηλαδή $u^2+3v^2=p^e$ με e≥1, τότε υπάρχουν ακέραιοι α,β≥0 με α∧β=1, ώστε

$$u + \sqrt{-3}v = \pm(\alpha \pm \sqrt{-3}\beta)^e$$

απόδειξη

Αν p=3 τότε e≤1, διότι διαφορετικά 9/ u^2+3v^2, 9/u^2, άρα 3/v άτοπο. Θα είναι συνεπώς $3=0^2+3\cdot1^2$ και $0 + \sqrt{-3}\cdot 1 = 0 + \sqrt{-3}\cdot 1$ και η πρόταση αληθεύει στην περίπτωση αυτή.
Αν p≠3 τότε θα είναι $p=\alpha^2+3\beta^2$ για κάποιους ακέραιους α,β>0. Είναι p>α έτσι αν ένας πρώτος π διαιρούσε τους α,β θα ήταν π/p και π<p άτοπο. Άρα α∧β=1.
Αν e=1 η πρόταση 4 είναι φανερή λόγω της πρότασης 3.
Αν e>1 αφού p/m από την πρόταση (2) θα υπάρχουν κ,λ ακέραιοι ώστε
$u + \sqrt{-3}v = (\alpha \pm \sqrt{-3}\beta)(\kappa + \sqrt{-3}\lambda)$, και $\kappa^2+3\lambda^2=p^{e-1}$. Αν e-1=1 λόγω της (3) θα πρέπει κ=±α,λ=±β. Αν ο ένας παράγοντας του παραπάνω γινομένου είναι ο $\alpha + \sqrt{-3}\beta$ τότε ο άλλος παράγοντας δεν μπορεί να είναι ο $\alpha - \sqrt{-3}\beta$ γιατί τότε το γινόμενό τους $\alpha^2+3\beta^2=p$ θα διαιρούσε τα u,v άτοπο. Έτσι οι μόνες δυνατότητες που απομένουν είναι να έχουμε $u + \sqrt{-3}v = \pm(\alpha \pm \sqrt{-3}\beta)^2$. Αν e-1>1 συνεχίζουμε με τον ίδιο τρόπο. Αφού p/ $\kappa^2+3\lambda^2=p^{e-1}$ μπορούμε να γράψουμε
$u + \sqrt{-3}v = (\alpha \pm \sqrt{-3}\beta)(\alpha \pm \sqrt{-3}\beta)(\kappa_1 + \sqrt{-3}\lambda_1)$, με ${\kappa_1}^2 + 3{\lambda_2}^2 = p^{e-2}$. Για το λόγο που αναφέραμε ήδη, στο παραπάνω γινόμενο δεν μπορεί να εμφανίζονται ταυτόχρονα οι παράγοντες $\alpha + \sqrt{-3}\beta$, $\alpha - \sqrt{-3}\beta$ έτσι θα έχουμε

$u+\sqrt{-3}v=(\alpha\pm\sqrt{-3}\beta)^2(\kappa_1+\sqrt{-3}\lambda_1)$, με ${\kappa_1}^2+3{\lambda_2}^2=p^{e-2}$. Συνεχίζοντας ομοίως θα έχουμε:
$u+\sqrt{-3}v=(\alpha\pm\sqrt{-3}\beta)^{e-1}(\kappa_{e-2}+\sqrt{-3}\lambda_{e-2})$, με ${\kappa_{e-2}}^2+3{\lambda_{e-2}}^2=p$. Πάλι λόγω της πρότασης (3) θα είναι $\kappa_{e-2}=\pm\alpha$, $\lambda_{e-2}=\pm\beta$ και λόγω των παραπάνω επισημάνσεων θα πρέπει $(\kappa_{e-2}+\sqrt{-3}\lambda_{e-2})=\pm(\alpha\pm\sqrt{-3}\beta)$ κι έτσι τελικά προκύπτει ότι $u+\sqrt{-3}v=\pm(\alpha\pm\sqrt{-3}\beta)^e$ ο.ε.δ.

πρόταση 5

Αν ο περιττός αριθμός $m=u^2+3v^2$ με $u\wedge v=1$ είναι αναλύεται σε γινόμενο πρώτων παραγόντων ως $m=\prod_{i=1}^{n}p_i^{e_i}$, με $e_i\geq 1$, τότε
υπάρχουν ακέραιοι $\alpha_i,\beta_i\geq 0$ με $\alpha_i\wedge\beta_i=1$, ώστε

$$u+\sqrt{-3}v=\pm\prod_{i=1}^{n}(\alpha_i\pm\sqrt{-3}\beta_i)^{e_i}$$

<u>απόδειξη</u>

Αφού $m=\prod_{i=1}^{n}p_i^{e_i}=\prod_{i=1}^{n}({\alpha_i}^2+3{\beta_i}^2)^{e_i}$ εφαρμόζοντας τη διαδικασία που περιγράψαμε στην πρόταση (4) διαδοχικά μέχρι να εξαντληθούν όλοι οι πρώτοι παράγοντες του m, προκύπτει το ζητούμενο.

πρόταση 6

Αν $u^2+3v^2=s^3$, όπου s περιττός, $u\wedge v=1$, τότε υπάρχουν διαφορετικής ισοτιμίας mod2 ακέραιοι t,w με $t\wedge w=1$ και $3\wedge t=1$, ώστε $u=t(t^2-9w^2)$, $v=3w(t^2-w^2)$, $s=t^2+3w^2$.

<u>απόδειξη</u>

Έστω $s^3=\prod p_i^{e_i}$, τότε $e_i=3e_i'$. Αν $p_i={\alpha_i}^2+3{\beta_i}^2$, i=1,2,…,n, θα έχουμε

$$u+\sqrt{-3}v=\pm\prod_{i=1}^{n}(\alpha_i\pm\sqrt{-3}\beta_i)^{e_i}=\pm\prod_{i=1}^{n}(\alpha_i\pm\sqrt{-3}\beta_i)^{3e'_i}$$

Θεωρούμε τον αριθμό που ορίζεται από την ισότητα

$$t+\sqrt{-3}w=\pm\prod_{i=1}^{n}(\alpha_i\pm\sqrt{-3}\beta_i)^{e'_i}$$

Ισχύει η ισότητα $u+\sqrt{-3}v=(t+\sqrt{-3}w)^3$ (6.1)
Αναπτύσοντας την ταυτότητα και εξισώνοντας πραγματικά με φανταστικά μέρη προκύπτουν οι τύποι $u=t(t^2-9w^2)$, $v=3w(t^2-w^2)$ (6.2).
Από την (6.1) $u-\sqrt{-3}v=(t-\sqrt{-3}w)^3$ (6.3). Με πολλαπλασιασμό κατά μέλη των 6.1,6.3 έχουμε $u^2+3v^2=(t^2+3w^2)^3\Leftrightarrow s^3=(t^2+3w^2)^3\Leftrightarrow s=t^2+3w^2$.
Θα είναι $t\wedge w=1$ αφού $u\wedge v=1$. Επίσης αν $3/t$ τότε $3/u\Rightarrow 3/s^3\Rightarrow 3^2/s^3\Rightarrow 3/v$, άτοπο. Επομένως το 3 δεν διαιρεί τον t, δηλαδή $3\wedge t=1$. Επειδή ο s είναι περιττός οι t,w οφείλουν να έχουν διαφορετική ισοτιμία mod2. ο.ε.δ.

Κάποιες παρατηρήσεις

Στην προηγούμενη παράγραφο αποδείξαμε το λήμμα 1 με έναν ομολογουμένως περιπετειώδη τρόπο. Ωστόσο κάποιος θα έμπαινε στον πειρασμό να σκεφτεί ως εξής: $u^2+3v^2=s^3 \Leftrightarrow (u+\sqrt{-3}v)(u-\sqrt{-3}v)=s^3$. Εδώ έχουμε ένα γινόμενο δυο αριθμών να είναι ίσο με έναν τέλειο κύβο. Αν οι αριθμοί που εμπλέκονται στην παραπάνω εξίσωση θεωρηθούν ως κάποιο ιδιαίτερο είδος «ακεραίων» και αυτού του είδους οι ακεραίοι έχουν παρόμοιες ιδιότητες με τους συνηθισμένους ακεραίους, τότε κατ' αναλογία με τη βασική πρόταση με την οποία ξεκινήσαμε στο άρθρο αυτό, θα έπρεπε αν ο μέγιστος κοινός διαιρέτης των $(u+\sqrt{-3}v)$, $(u-\sqrt{-3}v)$ είναι 1, καθένας εξ' αυτών να είναι τέλειος κύβος. Δηλαδή θα υπήρχαν ακέραιοι t,w ώστε $(u+\sqrt{-3}v)=(t+\sqrt{-3}w)^3 \Leftrightarrow (u+\sqrt{-3}v)=t^3-9tw^2+\sqrt{-3}(3t^2w-3w^3)$ κι έτσι $u=t(t^2-9w^2)$, $v=3w(t^2-w^2)$ βρήκαμε δηλαδή τους τύπους που με τόσο κόπο αποκαταστήσαμε προηγουμένως την εγκυρότητά τους. Καλό; Σίγουρα πολύ καλό για να είναι αληθινό!

Με τον παραπάνω τρόπο σκέψης γιατί να μην επιχειρήσουμε να αναζητήσουμε τις λύσεις της Πυθαγόρειας διοφαντικής εξίσωσης $\chi^2+\psi^2=\omega^2$; Για να δούμε λοιπόν. Παραγοντοποιώντας το πρώτο μέλος έχουμε $(\chi+\psi i)(\chi-\psi i)=\omega^2$. Αν οι ιδιαιτέρου είδους ακέραιοι που θα θεωρήσουμε είναι της μορφής $\alpha+\beta i$, με α,β συνηθισμένους ακέραιους και αν υποθέσουμε και πάλι ότι καθένας από τους παράγοντες του γινομένου είναι τέλειο τετράγωνο, τότε θα υπάρχουν ακέραιοι α,β ώστε $\chi+\psi i=(\alpha+\beta i)^2$ άρα $\chi+\psi i=\alpha^2-\beta^2+2\alpha\beta i$. Έτσι $\chi=\alpha^2-\beta^2$, $\psi=2\alpha\beta$ και συνεπώς $\omega=\alpha^2+\beta^2$. Ξαναβρίσκουμε τους γνωστούς τύπους για τις πυθαγόρειες τριάδες!

Ωραία όλα αυτά, αλλά πόσο σωστά είναι; Δεδομένων των σωστών αποτελεσμάτων, κάτι σωστό θα πρέπει να έχουν οι παραπάνω συλλογισμοί, αν και ενδεχομένως ερμηνευμένοι με διαφορετικό τρόπο. Στα μέσα του δεκάτου εννάτου αιώνα, ο Γερμανός μαθηματικός Έρνστ Κούμερ (Ernst Kummer 1810-1893), κατάφερε να κάνει συλλογισμούς σαν τους παραπάνω, τμήμα μιας μαθηματικής θεωρίας που επέκτεινε τις ιδιότητες των γνωστών μας ακεραίων, σε άλλου είδους αριθμητικά αντικείμενα, ο Κούμερ ονόμασε αυτά τα αντικείμενα «ιδεώδεις αριθμούς». Η θεωρία του που λίγο αργότερα επεκτάθηκε από τους μαθηματικούς Dedekind και Kronecker είναι γνωστή σήμερα ως **αλγεβρική θεωρία αριθμών.**

Σε επόμενο άρθρο[2], θα δούμε πώς μέσα στα πλαίσια της αλγεβρικής θεωρίας αριθμών οι παραπάνω «χαλαρές» αποδείξεις μπορούν να γίνουν τελείως αυστηρές. Οι δακτύλιοι μέσα στους οποίους ανήκουν οι «ιδεώδεις» ακέραιοι αριθμοί που θα χρησιμοποιήσουμε είναι τα εξής σύνολα:

$\mathbb{Z}[i]=\mathbb{Z}[\sqrt{-1}]=\{a+bi \ με \ a,b\in\mathbb{Z}\}$. (Ακέραιοι του Gauss.)

$\mathbb{Z}[\zeta_3]=\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]=\{\alpha+\beta\,\zeta_3 \ \ με \ a,b\in\mathbb{Z}\}$. Το ζ_3 είναι μια κυβική μιγαδική ρίζα της μονάδας. Προσέξτε ότι στην τελευταία περίπτωση δεν θα χρησιμοποιήσουμε ως ακεραίους μόνο τους αριθμούς της μορφής $\alpha+\beta\sqrt{-3}$ με $\alpha,\beta\in\mathbb{Z}$, αλλά ένα ευρύτερο σύνολο από το σύνολο αυτών των αριθμών.

Τέλος πρώτου μέρους.

[2] Στο δεύτερο μέρος αυτού του άρθρου θα αποδείξουμε το θεώρημα Fermat για N=3 και N=4 στα πλαίσια της αλγεβρικής θεωρίας αριθμών.

Βιβλιογραφία

1. Fermat Last Theorem - Paulo Ribenboim

2. Number Theory 1, Fermat's Dream – Kazuya Kato, Nobushige Kurokawa, Takeshi Saito

3. An introduction to theory of numbers – Ivan Niven, Herbert Zuckerman, Hungh Montgomery

4. Θεωρία Αριθμών – Δημήτριος Πουλάκης

5. Αριθμοθεωρητικός Λογισμός – Κασαπίδης Γεώργιος