ΓΥΜΝΑΣΜΑΤΑ ΑΡΙΘΜΟΘΕΩΡΙΑΣ
Κασαπίδης Γεώργιος – Μαθηματικός
geokasap@sch.gr

Κάθε πρώτος της μορφής 4κ+1 γράφεται ως άθροισμα δυο τετραγώνων.

Έστω p πρώτος $p\equiv 1\,mod4$ $q=\frac{p-1}{2}$ **και** $\alpha=q!$ **. Δείξτε ότι**

α. $\alpha^2\equiv -1\,modp$

β. Υπάρχουν ακέραιοι x,y με $0<x\,,\,y<\sqrt{p}$

τέτοιοι ώστε $\alpha^2x^2-y^2\equiv 0\,modp$

γ. $\mathbf{p=x^2+y^2}$

Απόδειξη

α. (πρώτος τρόπος)

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

Θεωρούμε την ισοδυναμία

$$(x-1^2)(x-2^2)...(x-(\frac{p-1}{2})^2)-(x^{\frac{p-1}{2}}-1)\equiv 0\,modp \quad (1)$$

Η ισοδυναμία $x^{\frac{p-1}{2}}-1\equiv 0\,modp$ έχει το πολύ $\frac{p-1}{2}$ λύσεις.

Θα δείξουμε οτι έχει ακριβώς $\frac{p-1}{2}$ λύσεις.

Έστω $1\leqslant k\leqslant p-1.$ Τότε (k,p)=1 και απο το θεώρημα Fermat-Euler θα έχουμε $k^{p-1}\equiv 1\,modp$ και άρα $(k^2)^{\frac{p-1}{2}}\equiv 1\,modp$ δηλαδή οι αριθμοί k^2 με $1\leqslant k\leqslant p-1$ είναι λύσεις της $x^{\frac{p-1}{2}}-1\equiv 0\,modp$

Αν k_1^2,k_2^2 είναι δυο τέτοιες λύσεις τότε

$k_1^2-k_2^2\equiv 0\,modp\Leftrightarrow(k_1-k_2)(k_1+k_2)\equiv 0\,modp$

και επειδή $|k_1-k_2|<p$ προκύπτει p/k_1+k_2 .

Εκλέγοντας όμως $1 \leqslant k \leqslant \frac{p-1}{2}$ τότε προφανώς όλες οι λύσεις k^2 *είναι* διαφορετικές μεταξύ τους και $\frac{p-1}{2}$ σε πλήθος.

Δείξαμε δηλαδή ότι οι λύσεις της ισοδυναμίας $x^{\frac{p-1}{2}} \equiv 1\, modp$ είναι οι $1^2, 2^{2,}, \ldots, (\frac{p-1}{2})^2$. Τότε η (1) έχει βαθμό μικρότερο του $\frac{p-1}{2}$ και έχει $\frac{p-1}{2}$ διαφορετικές λύσεις. Συνεπώς όλοι οι συντελεστές του πολυωνύμου $(x-1^2)(x-2^2)\ldots(x-(\frac{p-1}{2})^2)-(x^{\frac{p-1}{2}}-1)$ θα είναι μηδενικοί στο δακτύλιο $\mathbb{Z}_p$, δηλαδή θα διαιρούνται με τον p.

Ειδικότερα για το σταθερό όρο θα έχουμε $1+(-1)^q(q!)^2 \equiv 0\, modp$ οπότε

$$(-1)^q(q!)^2 \equiv -1\, modp \Leftrightarrow (q!)^2 \equiv -(-1)^q\, modp$$
$$\Leftrightarrow (q!)^2+(-1)^q \equiv 0\, modp \ .$$

Δεδομένου τώρα ότι $p \equiv 1\, mod4$ ο q είναι άρτιος κι έτσι προκύπτει τελικά ότι $\alpha^2 \equiv -1\, modp.$

α. (δεύτερος τρόπος)

$A=(p-1)!=1\cdot 2\cdot \ldots \frac{p-1}{2}\cdot(\frac{p-1}{2}+1)\cdot\ldots(p-1)$ ή A=B Γ

όπου

$B=1\cdot 2\cdot \ldots \frac{p-1}{2}$ και $\Gamma=(\frac{p-1}{2}+1)\cdot\ldots(p-1)$. Παρατηρούμε τώρα ότι κάθε παράγοντας του γινομένου Β μπορεί να γραφεί ως $\beta_m = \frac{p-1}{2}-m+1$ με

$1 \leqslant m \leqslant \frac{p-1}{2}$, ενώ κάθε παράγοντας του γινομένου Γ μπορεί να γραφεί στη μορφή $\gamma_m = \frac{p-1}{2} + m$ με $1 \leqslant m \leqslant \frac{p-1}{2}$. Ισχύει $\beta_m + \gamma_m = p$ κι έτσι $\gamma_m \equiv -\beta_m \, mod p$.

Άρα

$$\prod_{m=1}^{\frac{p-1}{2}} \gamma_m \equiv \prod_{m=1}^{\frac{p-1}{2}} -\beta_m \, mod p \quad => \quad \Gamma \equiv (-1)^{\frac{p-1}{2}} B \, mod p \quad => \quad \Gamma \equiv B \, mod p$$

Συνεπώς $A \equiv B^2 \, mod p$ δηλαδή $(p-1)! \equiv \alpha^2 \, mod p$. (1)

Θα αποδείξουμε τώρα ότι $(p-1)! \equiv -1 \, mod \, p \quad (\Theta. Wilson)$ (2)

Αν p=2 ή p=3 η πρόταση είναι προφανής. Έστω λοιπόν p>3.

Θεωρούμε την ισοδυναμία $\lambda\chi \equiv 1 \, mod p$ (*) με $\lambda \in \Lambda = \{1,2,\ldots,p-1\}$

Επειδή (λ,p)=1 η (*) έχει πάντοτε λύση. Άρα υπάρχει για κάθε $\lambda \in \Lambda$ ένας μοναδικός ακέραιος λ' που ανήκει στο σύνολο Λ έτσι ώστε λλ'≡1 modp.

Αν λ=λ' τότε $p/\lambda^2-1=(\lambda-1)(\lambda+1)$, άρα p/λ-1 ή p/λ+1 οπότε λ=1 ή λ=p-1. Αν εξαιρέσουμε από το σύνολο Λ τα στοιχεία του 1 και p-1, απομένουν p-3 στοιχεία τα οποία μπορούμε να τα ομαδοποιήσουμε σε $\frac{p-3}{2}$ ζεύγη στοιχείων λ,λ' για τα οποία λλ'≡1 modp. Θα ισχύει επομένως $2 \cdot 3 \cdot \ldots (p-2) \equiv 1 \, mod p$ <=> (p-1)! ≡ (p-1) modp ≡-1 modp και το θεώρημα έχει αποδειχθεί. Από τις σχέσεις (1) και (2) προκύπτει $\alpha^2 \equiv -1$ modp.

β. Θεωρούμε το σύνολο των ζευγών (χ',ψ') με χ',ψ ' να ανήκουν στο σύνολο $\{0,1,2,\ldots,[\sqrt{p}]\}$.

Το πλήθος αυτών των ζευγών είναι $([\sqrt{p}]+1)^2 > (\sqrt{p})^2 = p$.

Σχηματίζουμε τώρα τους ακεραίους της μορφής αχ'-ψ' και τους ανάγουμε modp. Δεδομένου ότι τα ζεύγη (χ',ψ') είναι περισσότερα από p, θα υπάρχουν σίγουρα δυο τουλάχιστον ζεύγη (χ',ψ') και χ'',ψ'') έτσι ώστε να ισχύει αχ'-ψ' ≡ αχ''-ψ'' modp <=> α(χ'-χ'') ≡ ψ'-ψ'' modp.

Θέτοντας χ=|χ'-χ''| και ψ=|ψ'-ψ''| (3) θα έχουμε αχ ≡ ± ψ modp (4)

οπότε $\alpha^2\chi^2 \equiv \psi^2 \bmod p \iff \alpha^2\chi^2 - \psi^2 \equiv 0 \bmod p$ (5)

Οι ακέραιοι χ,ψ είναι μη μηδενικοί γιατί διαφορετικά από τις σχέσεις (3) και (4) θα είχαμε (χ',ψ')=(χ'',ψ'').

γ. Από τις (4) και (5) αφού $\alpha^2 \equiv -1 \bmod p$ προκύπτει ότι $p/\chi^2+\psi^2$.
Επειδή $0<\chi,\psi< \sqrt{p}$ θα είναι $\chi^2+\psi^2<2p$ οπότε θα πρέπει $\chi^2+\psi^2=p$.

Παρατηρήσεις

1. Σύμφωνα με τα παραπάνω αποτελέσματα **κάθε πρώτος της μορφής 4κ+1 μπορεί να παρασταθεί σαν άθροισμα δυο τετραγώνων.** Η πρόταση αυτή αποδίδεται στο Fermat. Η βασική ιδέα της απόδειξης που δώσαμε οφείλεται στο Νορβηγό αριθμοθεωρίστα Axel Thue και κάνει χρήση της αρχής του **Dirichlet**, που συχνά αναφέρεται και ως αρχή του **περιστερώνα:** Αν έχουμε ν φωλιές και ν+1 περιστέρια, μια τουλάχιστον φωλιά θα έχει τουλάχιστον 2 περιστέρια.

2. Επειδή το τετράγωνο ενός ακεραίου είναι ισοδύναμο με 0 ή 1 mod4, το άθροισμα δυο τετραγώνων θα είναι ισοδύναμο με 0 ή 1 ή 2 mod4. Συνεπώς **ένας πρώτος της μορφής 4κ+3 δεν μπορεί να παρασταθεί ως άθροισμα δυο τετραγώνων.**

3. Με βάση το γεγονός ότι $\alpha^2+1 \equiv 0 \bmod p$ μπορούμε να δώσουμε και μια **διαφορετική απόδειξη** του γεγονότος ότι κάθε πρώτος της μορφής 4κ+1 μπορεί να γραφεί ως άθροισμα δυο τετραγώνων. Για την απόδειξη θα χρησιμοποιήσουμε το δακτύλιο ακεραίων του Gauss $\mathbb{Z}[i]$. Αφού $p/\alpha^2+1=(\alpha+i)(\alpha+i)$ αν υποθέσουμε ότι ο p είναι πρώτος στο $\mathbb{Z}[i]$ τότε θα πρέπει $p/\alpha+i$ ή $p/\alpha-i$. Αν ισχύει η πρώτη σχέση τότε $\alpha+i = p(x+iy)$ για κάποιους ακέραιους x,y. Έτσι $py=1$ σχέση αδύνατη. Ομοίως καταλήγουμε σε άτοπο από τη σχέση $p/\alpha-i$. Συνεπώς ο p δεν μπορεί να είναι πρώτος στο δακτύλιο $\mathbb{Z}[i]$. Αυτό με τη σειρά του σημαίνει ότι υπάρχουν ακέραιοι α,β του δακτυλίου, τέτοια ώστε $p=\alpha\beta$ και οι α,β να μην είναι μονάδες. Λαμβάνοντας νόρμες στα δυο μέλη της τελευταίας σχέσης βρίσκουμε $p^2=N(\alpha)N(\beta)$. Υπάρχουν τώρα οι εξής δυνατότητες: $p^2=N(\alpha)$ και $N(\beta)=1$ ή $p^2=N(\beta)$ και $N(\alpha)=1$ ή $p=N(\alpha)=N(\beta)$. Στην πρώτη περίπτωση ο β πρέπει να είναι μονάδα του δακτυλίου πράγμα αδύνατο, ενώ

στη δεύτερη ο α θα είναι μονάδα επίσης αδύνατο. Έτσι απομένει μόνο η τρίτη δυνατότητα p=N(α). Αν α= x+yi τότε $p=x^2+y^2$ με x,y ακεραίους.

Μια τρίτη απόδειξη (Roger Heath-Brown)

Θεωρούμε το σύνολο:

$T=\{ (x,y,z)\in\mathbb{Z}^3 : 4xy+z^2=p,\ x>0,\ y>0\}$.

Το σύνολο αυτό είναι μη κενό όταν p=4κ+1, αφού η τριάδα (κ,1,1) ανήκει στο T.

Επίσης αφού χ>0 θα είναι $4y\leqslant p$ δηλαδή $y\leqslant\frac{p}{4}$ και ομοίως $x\leqslant\frac{p}{4}$. Υπάρχει συνεπώς πεπερασμένο πλήθος ζευγών x,y που επαληθεύουν την $4xy+z^2=p$ και για καθένα απ' αυτά υπάρχουν το πολύ δυο αντίστοιχες τιμές του z. Είναι προφανώς $z\neq 0$ γιατί ο p είναι πρώτος αριθμός.

Έτσι το T είναι μη κενό και πεπερασμένο σύνολο.

Ορίζουμε την απεικόνιση f:T→ T, f(x,y,z) = (y,x,-z).

Η f έχει την ιδιότητα $f^2=I$, είναι αντιστρέψιμη και δεν έχει σταθερά σημεία αφού τότε θα έπρεπε z=0, x=y κι έτσι $p=(2x)^2$ αδύνατο όταν p πρώτος και x>0.

Έστω $A=\{ (x,y,z)\in T : z>0 \}$ και $B=\{ (x,y,z)\in T : x-y+z>0 \}$.

Είναι f(A)=T-A. Επίσης επειδή $x-y+z\neq 0$ (διαφορετικά $p=4xy+(x-y)^2=(x+y)^2$ αδύνατο αφού p πρώτος) προκύπτει ότι f(B)=T-B.

Αφού η f είναι "ένα προς ένα" θα ισχύει:

$f(A-B)=f(A\cap B')=f(A)\cap f(B')=A'\cap B=B-A$.

Τώρα είναι εύκολο να δούμε ότι μπορούμε να ορίσουμε μια 1-1 και επί απεικόνιση Φ από το σύνολο A στο σύνολο B ως εξής: Αν $x\in A-B$ τότε Φ(x)=f(x) ενώ αν $x\in A\cap B$ τότε Φ(x)=x. Από τα προηγούμενα καταλήγουμε στο συμπέρασμα ότι τα σύνολα A και B έχουν τον ίδιο πληθάριθμο.

Ορίζουμε τώρα την απεικόνιση g : B→B με g(x,y,z)=(x-y+z,y,2y-z). Κατ' αρχήν θα δείξουμε ότι η g είναι καλά ορισμένη συνάρτηση. Αν λοιπόν (x,y,z) ανήκει στο B τότε $4xy+z^2=p$ με x,y>0 και x-y+z>0. Παρατηρούμε ότι (x-y+z)-y+(2y-z)=x>0.

Επίσης $4(x-y+z)y+(2y-z)^2 = 4xy+z^2 = p$, δηλαδή g(x,y,z) ανήκει στο B.

Η g είναι συνάρτηση 1-1 και μάλιστα $g^2(x,y,z)=(x,y,z)$. Αν g(x,y,z)=(x,y,z) τότε προκύπτει ότι y=z και αφού $4xy+z^2=p$ θα είναι y(4x+y)=p οπότε y=1=z και 4x+1=p

δηλαδή $x=\frac{p-1}{4}$. Έτσι η τριάδα $\left(\frac{p-1}{4},1,1\right)$ είναι το μοναδικό σταθερό σημείο της g. Αυτό μας οδηγεί στο συμπέρασμα ότι ο πληθάριθμος του συνόλου B είναι περιττός αριθμός.
Τέλος ορίζουμε τη συνάρτηση h: A→A με h(x,y,z)=(y,x,z). Η h είναι προφανώς συνάρτηση 1-1 και μάλιστα $h^2(x,y,z)=(x,y,z)$. Επειδή το A έχει τον ίδιο πληθάριθμο με το B, το πλήθος των στοιχείων του είναι περιττός αριθμός. Δεδομένου πως η h είναι 1-1 και επί πάνω σ' ένα σύνολο περιττού πληθάριθμου, αυτή οφείλει να έχει περιττού πλήθους σταθερά σημεία. Αν (x,y,z) είναι ένα σταθερό σημείο της h, θα πρέπει x=y. Όμως $4xy+z^2=p$ άρα $(2x)^2+z^2=p$ δηλαδή ο πρώτος αριθμός p, γράφεται σαν άθροισμα δυο τετραγώνων.

Παρατηρήσεις

1. Σύμφωνα με την τελευταία απόδειξη, το πλήθος των αναπαραστάσεων του p της μορφής $p=(2x)^2+z^2$ είναι περιττό. Στην πραγματικότητα μια τέτοια αναπαράσταση είναι μοναδική. Να σημειώσουμε ότι όλες οι προηγούμενες αποδείξεις μας πιστοποιούν την ύπαρξη ακεραίων χ,ψ, για τους οποίους $p=x^2+y^2$ όμως καμιά τους δεν είναι υπολογιστικά αποτελεσματική.
2. Μετά τα παραπάνω εύκολα πλέον μπορούμε να δώσουμε ένα κριτήριο για το πότε ένας φυσικός αριθμός μπορεί να παρασταθεί σαν άθροισμα δυο τετραγώνων. Ισχύει το εξής: **Ένας φυσικός αριθμός n αναπαρίσταται σαν άθροισμα δυο τετραγώνων αν και μόνο αν κάθε πρώτος παράγοντάς του της μορφής 4κ+3 εμφανίζεται με άρτια δύναμη στην ανάλυση του n σε γινόμενο πρώτων.**

Βιβλιογραφία

1. I NIVEN & H.S. ZUCKERMAN: An Introtuction to the Theory of Numbers. Fifth edition , Wiley, New York 1972

2. Martin Aigner, Gunter M. Ziegler: Proofs from THE BOOK Fourth Edition - Springer