Εκθέτης
Φύλλα Μαθηματικής Παιδείας
Φυλλο 8, 21 Δεκεμβριου 2010

Διανέμεται και αναπαράγεται ελεύθερα.
Δικτυακός Τόπος
www.nsmavrogiannis.gr/ekthetis.htm
Στοιχειοθετείται με το LaTeX 2ε
Επιμέλεια:
Ν.Σ. Μαυρογιάννης, Δρ Μαθηματικών
Πειραματικό Λύκειο
Ευαγγελικής Σχολής Σμύρνης
mavrogiannis@gmail.com

Ποιοι φυσικοί αριθμοί γράφονται ως άθροισμα δυο, το πολύ, τετραγώνων ακεραίων αριθμών.

Στράτος Μάκρας, Δρ Μαθηματικών
Ευρωπαϊκό Σχολείο Βρυξελλες ΙΙΙ

Περίληψη

Το κείμενο αυτό προέρχεται από μαθήματα που έδωσα για τους μαθητές και τις μαθήτριες των προχωρημένων Μαθηματικών του Ευρωπαϊκού σχολείο Βρυξελλών ΙΙΙ και πραγματεύεται τον χαρακτηρισμό των φυσικών αριθμών που μπορούν να γραφούν ως άθροισμα τετραγώνων δύο άλλων φυσικών.

Το πρόβλημα που θα μας απασχολήσει εδώ είναι το εξής:

Προβλημα Για ποιους φυσικούς αριθμούς n υπάρχουν ακέραιοι x και y τέτοιοι ώστε $x^2+y^2=n$;

Το πρόβλημα είναι παλιό. Από τον Διόφαντο, ίσως και πριν, μέχρι τον Fermat και τον Euler ο οποίος τελικά και δημοσίευσε την πρώτη πλήρη απόδειξη. Θα αρχίσουμε με δυο παρατηρήσεις

Παρατηρηση 1 Αν οι αριθμοί x και y είναι και οι δυο άρτιοι ή και οι δυο περιττοί, τότε και ο αριθμός n θα είναι άρτιος. Αν οι αριθμοί x και y είναι διαφορετικής αρτιότητας $x=2k$ και $y=2m+1$ τότε έχουμε, $x^2+y^2=4k^2+4m^2+4m+1=4\left(k^2+m^2+m\right)+1=1(\mathrm{mod}\,4)$. Έτσι δεν είναι δυνατόν ο n να είναι περιττός της μορφής $4k+3$.

Έχουμε λοιπόν το εξής πρώτο συμπέρασμα:

(Π1) Οι ακέραιοι της μορφής $4k+3$ δεν γράφονται ως άθροισμα δυο τετραγώνων .

Παρατηρηση 2 Από την γνωστή ταυτότητα

$$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$$

έπεται ότι, αν δυο αριθμοί γράφονται ως άθροισμα δυο τετραγώνων τότε και το γινόμενό τους γράφεται επίσης ως άθροισμα δυο τετραγώνων. Με άλλα λόγια: Αν ονομάσουμε S το σύνολο των ακεραίων που γράφονται ως άθροισμα δυο τετραγώνων, τότε το S είναι κλειστό ως προς τον πολλαπλασιασμό.

Αυτή η παρατήρηση μας επιτρέπει να εστιάσουμε την προσοχή μας στους πρώτους αριθμούς που γράφονται ως άθροισμα δυο τετραγώνων, μια και κάθε άλλος ακέραιος γράφεται ως γινόμενο πρώτων.

Θα εξετάσουμε λοιπόν τους πρώτους της μορφής $4k+1$ και θα προσπαθήσουμε να δούμε ποιοι από αυτούς γράφονται ως άθροισμα δυο τετραγώνων .

Για να μην έχετε αγωνία, σας λέω ότι όλοι οι πρώτοι της μορφής $4k+1$ γράφονται ως άθροισμα δυο τετραγώνων.

Έστω λοιπόν ένας πρώτος αριθμός p της μορφής $4k+1$. Ζητάμε να αποδείξουμε ότι υπάρχουν φυσικοί αριθμοί x και y τέτοιο ώστε να ισχύει $x^2+y^2=p$.

Ας εργασθούμε στο $(\mathbb{Z}_p,+,.)$ των ακεραίων modulo p το οποίο, όπως γνωρίζουμε, είναι σώμα. Έχουμε λοιπόν:
$x^2+y^2=p \Leftrightarrow$
$x^2+y^2=0(\mathrm{mod}p) \Leftrightarrow$
$(xy^{-1})^2+1=0(\mathrm{mod}p)$,
ή αν θέσουμε, $xy^{-1}=w$, $w^2+1=0(\mathrm{mod}p)$ ή τέλος $w^2=-1(\mathrm{mod}p)$.
Ένα πρώτο θέμα είναι το εξής:

Ερωτημα Υπάρχει στοιχείο $w\in\mathbb{Z}_p$ τέτοιο ώστε $w^2=-1(\mathrm{mod}p)$;

Και πάλι η απάντηση είναι «ναι» και θα το αποδείξουμε αμέσως τώρα χρησιμοποιώντας, μεταξύ άλλων, και το θεώρημα του Wilson:
Ο p είναι της μορφής $4k+1$, άρα $p-1=4k$ και $\frac{p-1}{2}=2k$: Από το θεώρημα του Wilson έχουμε $(p-1)!=-1(\mathrm{mod}p)$ και, επειδή οι αριθμοί $1,2,...,p-1$, είναι ανά δυο αντίθετοι, μπορούμε να γράψουμε:

$$1.2...\frac{p-1}{2}.\frac{p+1}{2}...(p-1)=(-1)^{2m}(1.2...\frac{p-1}{2})^2=(1.2...\frac{p-1}{2})^2$$

άρα

$$(1.2...\frac{p-1}{2})^2=-1(\mathrm{mod}p)$$

Έχουμε, ήδη, προχωρήσει αρκετά. Είδαμε ότι υπάρχει ένας τουλάχιστον $w\in\mathbb{Z}_p$ τέτοιος ώστε $w^2+1=0(\mathrm{mod}p)$. Μια και το $(\mathbb{Z}_p,+,.)$ είναι σώμα, το w θα γράφεται στην μορφή xy^{-1} οπότε η προηγούμενη σχέση θα γράφεται

$$(xy^{-1})^2+1=0(\mathrm{mod}p)$$

ή

$$x^2+y^2=0(\mathrm{mod}p)$$

ή τέλος

$$x^2+y^2=np \text{ με } n\in\mathbb{N}$$

Από τα διάφορα x, y που ικανοποιούν την τελευταία αυτή σχέση υπάρχουν δυο ¨αρκετά μικρά' ώστε η σχέση αυτή να ισχύει με $n = 1$. Η απάντηση είναι και πάλι «ναι» (σήμερα είναι η τυχερή μας ημέρα) αλλά έχετε λίγη υπομονή γιατί η απόδειξη δεν είναι πολύ εύκολη. Χρειάζονται δυο λήμματα: ένα του Γερμανού Johann Peter Gustav Lejeune Dirichlet (1805-1859) και ένα του Νορβηγού Axel Thue (1863-1922) (πολύ ωραία και τα δυο)

Johann Peter Gustav Lejeune Dirichlet (1805-1859)

Λήμμα 1 *(Dirichlet). Για κάθε $\xi \in R$ και κάθε $H > 1$ υπάρχουν $a \in N$ και $b \in N$ τέτοιοι ώστε να ισχύουν: $b < H$ και $|b\xi - a| \leq \frac{1}{H}$ (ή $\left|\xi - \frac{a}{b}\right| \leq \frac{1}{bH}$)*

Θα το αποδείξουμε λίγο πιο κάτω αλλά πρώτα θα δούμε πως το χρησιμοποίησε ο Axel Thue για να αποδείξει το δικό του λήμμα, το οποίο οδηγεί αμέσως και στην απόδειξη της πρότασης που μας ενδιαφέρει εδώ.

Axel Thue (1863-1922)

Λήμμα 2 *(Thue)(μια διατύπωση) Έστω p ένας φυσικός αριθμός για τον οποίο υπάρχει x τέτοιο ώστε*

$$x^2 = -1(\mathrm{mod} p)$$

Θα υπάρχουν τότε ακέραιοι u και v τέτοιοι ώστε $u^2 + v^2 = p$

Αποδειξη του Λημματος του Thue Θα εφαρμόσουμε το Λήμμα του Dirichlet με $H = \sqrt{p}$ και $\xi = \frac{x}{p}$. Θα υπάρχουν $a \in \mathbb{Z}$ και $b \in N$ τέτοιοι ώστε να ισχύουν: $b < \sqrt{p}$ και $\left|b\frac{x}{p} - a\right| \leq \frac{1}{\sqrt{p}}$ ή $|bx - ap| \leq \frac{p}{\sqrt{p}}$ ή τέλος $|bx - ap| < \sqrt{p}$ Θέτουμε τώρα $u = |bx - ap|$, $v = b$ και έχουμε

$$u^2 + v^2 = |bx - ap|^2 + b^2 =$$

$$b^2x^2 + a^2p^2 - 2bxap + b^2 =$$

$$b^2(x^2 + 1)(\mathrm{mod} p) = 0(\mathrm{mod} p)$$

(θυμηθείτε ότι $x^2 = -1(\mathrm{mod} p)$). Επίσης $u < \sqrt{p}$ και $v = b < \sqrt{p}$ άρα $u^2 + v^2 < p + p = 2p$. Με λίγα λόγια ο $u^2 + v^2$ είναι πολλαπλάσιο του p και μικρότερος του $2p$ άρα τελικά $u^2 + v^2 = p$; Έτσι λοιπόν, κάθε πρώτος αριθμός p της μορφής $4k+1$, γράφεται ως άθροισμα δυο τετράγωνων. Εύκολα τώρα καταλήγουμε στο εξής συμπέρασμα:

- Οι μοναδικοί φυσικοί ακέραιοι που δεν γράφονται ως άθροισμα δυο τετράγωνων είναι αυτοί των οποίων η ανάλυση τους σε γινόμενο πρώτων παραγόντων περιέχει έναν τουλάχιστον παράγοντα της μορφής $4k+3$ σε περιττό εκθέτη.

Θα αποδείξουμε αμέσως και Λήμμα του Dirichlet ώστε να μην μείνει κανένα σκοτεινό σημείο. Αποδειξη του Λημματος του Dirichlet Θέτουμε

$$N = [H] + 1$$

($[H]$ το ακέραιο μέρος του H) και θεωρούμε τους N σε πλήθος ακέραιους :

$$0\xi,\ 1\xi,\ 2\xi, ..., (N-1)\,\xi$$

καθώς και τους $N + 1$ σε πλήθος αριθμούς:

$$A_0 = 0\xi - [0\xi]$$

$$A_1 = 1\xi - [1\xi]$$

$$A_2 = 2\xi - [2\xi]$$

$$...$$

$$A_{N-1} = (N-1)\,\xi - [(N-1)\,\xi]$$

και

$$1$$

Οι αριθμοί αυτοί ανήκουν, όλοι, στο διάστημα $[0, 1]$, άρα, αν χωρίσουμε το $[0, 1]$ σε N υποδιαστήματα μήκους $1/N$ δυο τουλάχιστον από αυτούς θα ανήκουν στο ίδιο υποδιάστημα Αν οι δυο αυτοί αριθμοί είναι οι $\lambda\xi - [\lambda\xi]$ και $\kappa\xi - [\kappa\xi]$ με $\lambda < \kappa < N - 1$ θα έχουμε θέτοντας $b = \kappa - \lambda$ και $a = [\kappa\xi] - [\lambda\xi]$

$$0 < b < N - 1 = [H] + 1 - 1 = [H] \leq H$$

και

$$|\kappa\xi - [\kappa\xi] - (\lambda\xi - [\lambda\xi])| \leq \frac{1}{N}$$

ή $|\kappa\xi - [\kappa\xi] - (\lambda\xi - [\lambda\xi])| \leq \frac{1}{N}$ ή τέλος $|b\xi - a| \leq \frac{1}{N} < \frac{1}{H}$
Σημειωση: Το λήμμα του Dirichlet είναι πολύ γενικό και θα το χρησιμοποιήσουμε και αλλού!