Κυπριακή Μαθηματική Εταιρεία
Στασίνου 36, Γραφ. 102, Στρόβολος 2003, Λευκωσία
Τηλέφωνο: 357 – 22378101, Φαξ: 357 – 22379122
cms@cms.org.cy, www.cms.org.cy

ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΕΒΔΟΜΑΔΑΣ

Ολυμπιαδες

Κωδικός: OLY2017-B05
Επιμέλεια: Δημήτρης Χριστοφίδης

Πρόβλημα

Να βρεθούν όλα τα ζεύγη (n, p) ώστε ο n να είναι θετικός ακέραιος, ο p πρώτος αριθμός, και ο

$$1^n + 2^n + \cdots + (p-1)^n$$

να είναι πολλαπλάσιο του p.

Προτεινόμενη Λύση

Έστω θετικός ακέραιος n και πρώτος αριθμός p. Γράφουμε $n = q(p-1) + r$ όπου q το πηλίκο και r το υπόλοιπο της διαίρεσης του n με τον $p-1$.

Από το μικρό θεώρημα του Φερμά, έχουμε:

$$\begin{aligned} 1^n + 2^n + \cdots + (p-1)^n &= 1^{(p-1)q+r} + 2^{(p-1)q+r} + \cdots + (p-1)^{q(p-1)+r} \\ &\equiv 1^r + 2^r + \cdots + (p-1)^r \bmod p \end{aligned} \tag{1}$$

Θα χρησιμοποιήσουμε το εξής:

Πρωταρχική ρίζα modulo p

Κάθε πρώτος αριθμός έχει πρωταρχική ρίζα.

Δηλαδή, αν p πρώτος αριθμός, τότε υπάρχει g ώστε η τάξη του g modulo p να ισούται με $p-1$. Δηλαδή, $g^{p-1} \equiv 1 \bmod p$ αλλά $g^m \not\equiv 1 \bmod p$ για $1 \leqslant m \leqslant p-1$.

Έστω λοιπόν g μια πρωταρχική ρίζα του p. Τότε οι $g, g^2, \ldots, g^{p-1}$ είναι όλοι διαφορετικοί modulo p. Πράγματι αν π.χ. ίσχυε ότι $g^a \equiv g^b$ με $1 \leqslant a < b \leqslant p-1$, τότε θα είχαμε $g^{b-a} \equiv 1 \bmod p$, άτοπο.

Άρα modulo p οι αριθμοί $g, g^2, \ldots, g^{p-1}$ είναι με κάποια σειρά ισότιμοι των $1, 2, \ldots, p-1$.

Από αυτήν την παρατήρηση και την (1) έχουμε:

$$1^n + 2^n + \cdots + (p-1)^n \equiv g^r + g^{2r} + \cdots + g^{(p-1)r} \bmod p \tag{2}$$

Αν $r = 0$ η (2) δίνει:

$$1^n + 2^n + \cdots + (p-1)^n \equiv p - 1 \not\equiv 0 \bmod p$$

Αν $r \neq 0$ τότε από την (2) και το μικρό θεώρημα του Φερμά παίρνουμε:

$$1^n + 2^n + \cdots + (p-1)^n \equiv g^r \frac{g^{(p-1)r} - 1}{g^r - 1} \equiv 0 \bmod p$$

Άρα ο

$$1^n + 2^n + \cdots + (p-1)^n$$

είναι πολλαπλάσιο του p αν και μόνο αν $n \not\equiv 0 \bmod (p-1)$.

Σχόλιο

Πιο γενικά, αν n θετικός ακέραιος, τότε ο g ονομάζεται πρωταρχική ρίζα modulo n αν $g^{\varphi(n)} \equiv 1 \bmod n$ αλλά $g^m \not\equiv 1 \bmod p$ για $1 \leqslant m \leqslant \varphi(n) - 1$. Εδώ, η $\varphi(n)$ είναι η συνάρτηση του Euler.

Ισχύει το εξής:

Πρωταρχική ρίζα modulo n

Ο n έχει πρωταρχική ρίζα αν και μόνο αν $n = 2, 4, p^k, 2p^k$ όπου p περιττός πρώτος και k θετικός ακέραιος.