



ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΕΒΔΟΜΑΔΑΣ
ΟΛΥΜΠΙΑΔΕΣ

Κωδικός: OLY2017-A02

Επιμέλεια: Δημήτρης Χριστοφίδης

Πρόβλημα

Δίνεται πρώτος p μεγαλύτερος του 3. Ναδειχθεί ότι ο $p^2 - 1$ είναι πολλαπλάσιος του 24.

Προτεινόμενη Λύση

Επειδή $24 = 2^3 \cdot 3$, αρκεί να δείξουμε ότι ο $p^2 - 1$ είναι πολλαπλάσιος του 8 και του 3. Αν και δεν είναι αναγκαίο για αυτό το πρόβλημα, θα χρησιμοποιήσουμε τον ακόλουθο συμβολισμό, ο οποίος είναι αρκετά χρήσιμος για πιο δύσκολα προβλήματα:

Ισοτιμία modulo n

Δίνονται ακέραιοι αριθμοί a, b και θετικός ακέραιος αριθμός n . Αν ο n είναι πολλαπλάσιος του $a - b$, τότε λέμε ότι οι a, b είναι **ισότιμοι modulo n** και γράφουμε:

$$a \equiv b \pmod{n}$$

Η χρησιμότητα του πιο πάνω συμβολισμού οφείλεται στις ακόλουθες ιδιότητες:

Ιδιότητες ισοτιμιών

Δίνονται ακέραιοι αριθμοί a, b, c, d, k και θετικοί ακέραιοι αριθμοί m, n . Αν ισχύει ότι $a \equiv b \pmod{n}$ και $c \equiv d \pmod{n}$, τότε:

- (1) $a + c \equiv b + d \pmod{n}$
- (2) $a - c \equiv b - d \pmod{n}$
- (3) $ac \equiv bd \pmod{n}$
- (4) $ka \equiv kb \pmod{n}$
- (5) $a^m \equiv b^m \pmod{n}$

Π.χ. για να αποδείξουμε την (3), αρχικά παρατηρούμε ότι:

$$ac - bd = c(a - b) + b(c - d)$$

Αφού τα $a-b, c-d$ είναι πολλαπλάσια του n , το ίδιο ισχύει και για το $ac-bd$. Επομένως, η (3) αποδείχθηκε. Οι υπόλοιπες ιδιότητες αποδεικνύονται με παρόμοιο τρόπο.

Πίσω στο πρόβλημά μας τώρα. Αφού $p > 3$, τότε $3 \nmid p$. Άρα, $p \equiv 1 \pmod{3}$ ή $p \equiv 2 \pmod{3}$. Στην πρώτη περίπτωση έχουμε $p^2 \equiv 1 \pmod{3}$ και στην δεύτερη περίπτωση έχουμε $p^2 \equiv 4 \equiv 1 \pmod{3}$. Άρα, και στις δύο περιπτώσεις καταλήγουμε στο $p^2 - 1 \equiv 0 \pmod{3}$, δηλαδή στο ότι το $p^2 - 1$ είναι πολλαπλάσιο του 3.

Για την διαιρετότητα με το 8, αφού $2 \nmid p$ πρέπει $p \equiv 1, 3, 5, 7 \pmod{8}$. Και στις τέσσερις περιπτώσεις παίρνουμε $p^2 - 1 \equiv 0 \pmod{8}$, οπότε η απόδειξη ολοκληρώθηκε.

