



ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΕΒΔΟΜΑΔΑΣ
ΟΛΥΜΠΙΑΔΕΣ

Κωδικός: OLY2018-B18

Επιμέλεια: Δημήτρης Χριστοφίδης

Πρόβλημα

Να βρεθούν όλα τα ζεύγη (p, n) όπου p πρώτος αριθμός, n θετικός ακέραιος και ο $p^n + 1$ να διαιρεί τον $n^p + 1$.

Πηγή: Ολυμπιάδα Ασίας - Ειρηνικού 2012

Προτεινόμενη Λύση

Λήμμα 1: Έστω r, s θετικοί ακέραιοι ώστε $r^s \leq s^r$. Τότε $r \geq s$ ή $r = 2$ και $s \leq 4$.

Θα δώσουμε δύο αποδείξεις του Λήμματος 1 στα σχόλια. Εδώ, προχωράμε με την λύση της άσκησης.

Για $p = 2$ πρέπει $2^n + 1 | n^2 + 1$ και άρα πρέπει και $n^2 \geq 2^n$. Από το Λήμμα 1 πρέπει $n \leq 4$. Εύκολα βρίσκουμε ότι το $n = 3$ απορρίπτεται ενώ τα $n = 2, 4$ είναι δεκτά.

Έστω τώρα ότι $p > 2$ και άρα $p \geq 5$. Επειδή $p^n \leq n^p$, πρέπει $p \geq n$. Θα δείξουμε ότι $p + 1 | n + 1$. Τότε πρέπει και $p \leq n$ οπότε και $p = n$.

Αφού ο p είναι περιττός, ο $p^n + 1$ είναι άρτιος. Άρα και ο $n^p + 1$ είναι άρτιος, και άρα ο n είναι επίσης περιττός. Έστω $p + 1 = q_1^{r_1} \cdots q_k^{r_k}$ ως γινόμενο πρώτων παραγόντων. Αρκεί να δείξουμε ότι $q_i^{r_i} | n + 1$ για κάθε $1 \leq i \leq k$.

Έστω χωρίς βλάβη της γενικότητας $t = q_1^{r_1}$. Έχουμε $p \equiv -1 \pmod t$, άρα $p^n \equiv -1 \pmod t$. Δηλαδή $t | p^n + 1$ και άρα $t | n^p + 1$. Οπότε $t | n^{2p} - 1$. Έστω $d = \text{ord}_t(n)$. Τότε $d | 2p$ και άρα $d = 1, 2, p$ ή $2p$. Όμως $d \leq n < p$. Άρα $d = 1$ ή $d = 2$.

Αν $d = 1$ τότε $t | n - 1$ και άρα $t | n^p - 1$. Ισχύει επίσης και ότι $t | n^p + 1$, άρα $t = 2$. Σε αυτήν την περίπτωση έχουμε και $t | n + 1$.

Αν $d = 2$ τότε $t | n^2 - 1$ αλλά $t \nmid n - 1$. Επειδή $(n + 1, n - 1) = 2$, και επειδή ο t είναι δύναμη πρώτου, αν t περιττός τότε $t | n + 1$. Έστω λοιπόν ότι ο t είναι άρτιος και άρα δύναμη του 2. Ας υποθέσουμε ότι $t \nmid n + 1$. Επειδή $t | n^p + 1$ και $n^p + 1 = (n + 1)(n^{p-1} - n^{p-2} + \cdots + 1)$ τότε θα ισχύει και ότι $2 | n^{p-1} - n^{p-2} + \cdots + 1$. Αφού όμως οι n, p είναι περιττοί, τότε και

ο $n^{p-1} - n^{p-2} + \dots + 1$ είναι περιττός, άτοπο. Άρα σε κάθε περίπτωση έχουμε δείξει ότι $t|n+1$.

Εν τέλει, τα μόνο ζεύγη (p, n) που ικανοποιούν τις συνθήκες είναι τα (p, p) όπου p πρώτος, καθώς και το $(2, 4)$.

Σχόλια

Θα δώσουμε δύο αποδείξεις του Λήμματος 1. Μια σύντομη χρησιμοποιώντας διαφορικό λογισμό και άλλη μία η οποία αποφεύγει την χρήση του.

Θεωρούμε την συνάρτηση $f : (0, \infty) \rightarrow (0, \infty)$ με τύπο $f(x) = x^{1/x} = e^{(\log x)/x}$. Τότε είναι:

$$f'(x) = \left(\frac{1}{x^2} - \frac{\log x}{x^2} \right) e^{\frac{\log x}{x}} = \frac{1}{x^2} (1 - \log x) e^{\frac{\log x}{x}}$$

Άρα η συνάρτηση είναι φθίνουσα στο $[e, \infty)$ και αφού $e < 3$, για $r, s \geq 3$ έχουμε:

$$r^s \leq s^r \Leftrightarrow f(r) \leq f(s) \Leftrightarrow r \geq s$$

Επίσης είναι απλό επαγωγικά ότι $2^n \geq n^2$ για $n \geq 4$. Επειδή επιπλέον έχουμε $2^3 < 3^2$ και $2^4 = 4^2$ η απόδειξη του λήμματος ολοκληρώθηκε.

Μπορούμε να αποφύγουμε την χρήση διαφορικού λογισμού ως εξής: Αρκεί να δείξουμε για $n \geq 3$ ότι $(n+1)^{1/(n+1)} \leq n^{1/n}$ αφού μετά η απόδειξη ολοκληρώνεται όπως στην προηγούμενη παράγραφο. Ισοδύναμα, θέλουμε να δείξουμε ότι $(n+1)^n \leq n^{n+1}$. Όμως:

$$\frac{(n+1)^n}{n^{n+1}} = \frac{1}{n} \left(1 + \frac{1}{n} \right)^n$$

Αφού $n \geq 3$, αρκεί να δείξουμε ότι $(1 + \frac{1}{n})^n \leq 3$. Από το διωνυμικό θεώρημα έχουμε:

$$\left(1 + \frac{1}{n} \right)^n = \sum_{k=0}^n \binom{n}{k} \frac{1}{n^k} \leq \sum_{k=0}^n \frac{1}{k!}$$

αφού:

$$\binom{n}{k} = \frac{n(n-1) \cdots (n-k+1)}{k!} \leq \frac{n^k}{k!}$$

Όμως είναι απλό επαγωγικά ότι $k! \geq 2^{k-1}$ για $k \geq 2$. Άρα:

$$\left(1 + \frac{1}{n} \right)^n \leq 2 + \sum_{k=2}^n \frac{1}{2^{k-1}} = 3 - \frac{1}{2^{n-1}} < 3$$