SOLUTIONS FOR THE 11^{TH} INTERNATIONAL TOURNAMENT OF YOUNG MATHEMATICIANS

Team Bulgaria

Problem 1: A Divisibility Problem

Author: Ivan Durev, Plamen Ivanov

Abstract

We have fully solved item 1.

Problem 1

Definition 1. Let a and n be two coprime numbers and $r \in \mathbb{Z}^+$ is the least number, for which $a^r \equiv 1 \pmod{n}$

Theorem 1. Let r be the order of a modulo n ($gcd(a; n) = 1$). Then $a^l \equiv 1 \pmod{n} \iff r \mid l$

Proof of the " $\Longrightarrow$ " direction. Let us suppose the opposite - that $r \nmid l$. Let $l = kr + q$, $k \in \mathbb{Z}$, $k \geq 0$ and $q \in \{1, 2, \ldots, r-1\}$

$$a^r \equiv 1 \pmod{n}$$
$$a^q r \equiv 1 \pmod{n}$$
$$a^q r + q \equiv 1 \pmod{n}$$
$$a^q \equiv 1 \pmod{n} \text{ But } q < r$$
$$\Longrightarrow \text{Contradiction with the definition of the order of a number.} \quad \blacksquare$$

Proof of the "$\Longleftarrow$" direction.

$$a^r \equiv 1 \pmod{n}$$
$$\text{As } \frac{l}{r} \in \mathbb{Z}^+ \implies (a^r)^{\frac{l}{r}} \equiv 1^{\frac{l}{r}} \pmod{n}$$
$$\Longrightarrow a^l \equiv 1 \pmod{n} \quad \blacksquare$$

Item 1. *Solution.* Let p be a prime divisor of $2^{2^n} + 1$. It follows that $2^{2^n} \equiv -1 \pmod{p}$. Thus, $2^{2^{n+1}} \equiv 1 \pmod{p}$. Let r be the order of 2 modulo p. From Theorem 1. $r \mid 2^{n+1}$, but $r > 2^n$. Therefore $r = 2^{n+1}$. From Fermat's Little Theorem $2^{p-1} \equiv 1 \pmod{p}$. It follows from Theorem 1. that $r \mid p - 1$. $\implies 2^{n+1} \mid p - 1$ $\blacksquare$