Problems Proposed For IMO

March 13, 2013

Here are the problems I intend to propose for the next IMO.

1. Define $k(n)$ as:

$$k(n) = \sum_{d|n, d+1 \in \mathbb{P}} 1$$

where $\mathbb{P}$ is the set of primes, and $C(n)$ is the number of positive integers x so that $x|a^n - a$ for all a. Prove that $C(n) \geq 2^{k(n-1)}$.

Solution. From the definition, $k(n-1)$ is the number of divisors d of $n-1$ for which $d+1$ is a prime. For any prime $p, p|a^p - a$ from Fermat's little theorem. Moreover, $p|a$ or $p|a^{p-1} - 1$. Also, $p|a^n - a$ implies $p|a$ or $p|a^{n-1} - 1$ because $\gcd(a, a^{n-1} - 1) = 1$. Therefore, for every divisor d of $n-1$ that gives us $d + 1 = p$, a prime, for that p, we can say

$$\begin{aligned} a^{n-1} &\equiv a^{dk} \pmod p \\ &\equiv a^{(p-1)k} \pmod p \\ &\equiv 1 \pmod p \end{aligned}$$

Thus, $p|a^{n-1} - 1$ or $p|a$ is satisfied. There are $k(n)$ such primes. Say the primes are $p_1, ..., p_{k(n-1)}$. Consider,

$$N = p_1 \cdots p_{k(n-1)}$$

Every divisor D, of N also satisfies $D|a^n - a$ for all a. Since N has

$$(1 + 1) \cdots (1 + 1) = 2^{k(n-1)}$$

divisors, we can say the number of such x will be greater than or equal to $2^{k(n-1)}$.

2. Take the polynomial

$$P(X) = X^k + \binom{n-k}{k} X^{k-1} + \binom{n}{\bullet}$$

3. Define c_n as the smallest positive integer such that $1 < c_n < n - 1$. Find all n such that c_n does not exist and prove that there are infinitely many n such that $\varphi(n)$ is the smallest positive integer such that $c_n^{\varphi(n)}$ has a remainder 1 upon division by n.

Solution.

LEMMA 1. *c_n is a prime for all n if c_n exists.*

Proof. For the sake of contradiction, let's say that c_n isn't a prime. Then it must have a prime factor $q < c_n$. But then q is a smaller number than c_n co-prime to n. Contradiction. □

Corollary. c_n is the smallest prime less than $n - 1$ that does not divide n.

Corollary. $c_n = 2$ for any odd $n > 3$.

LEMMA 2. *c_n exists if $n \neq 1, 2, 3, 4, 6$.*

Proof. We assume that $n > 6$ and even. Then since c_n needs to be a prime, we infer that every prime less than $n - 1$ must divide n. Because n is even, it's not a prime and hence the number of primes less than or equal to n is the number of primes less than or equal to $n - 1$. Let k be the index such that $p_k < n < p_{k+1}$. Then the number of primes less than n is k. Then, we have

$$p_1 p_2 \cdots p_k | n$$

Or

$$n \geq p_1 \cdots p_k$$

On the other hand, from BONSE'S INEQUALITY, for $k > 5$,

$$p_1 \cdots p_k > p_{k+1}^2 > n^2$$

a contradiction! So $k \leq 5$ and we check by hand for $n < 11$. □

This proves the first part. Now we prove the latter. We take a prime $p \equiv 1 \pmod 4$. Then, we know that

$$c_p = 2$$

We prove that, for all such p, $\varphi(p)$ is the order of 2 modulo p. From Euler's criterion, using Legendre symbol,

4. Find all n which has a sum of number of divisors of divisors of n is n.

Solution. We consider $n > 1$. Let $\tau(n)$ denote the number of divisors of n, and $p^\alpha || N$ means α is the maximum positive integer with $p^\alpha | N$ i.e. $p^\alpha | N$ but $p^{\alpha+1} \nmid N$. Then, We need,

$$\sum_{d|n} \tau(d) = n$$

Let's prove the following lemma.

LEMMA 1. *Let $F(n) = \sum_{d|n} \tau(d)$. Then,*

$$F(n) = \prod_{p|n, p^e||n} F(p^e)$$

Proof. Any divisor d, of n is of the form $\prod_{p|d} p^b$. And since τ is multiplicative, we can say that, any term that belongs to the right side, also belongs to the left side. And it's now easy to see that the converse is also true. Since both side has the same number of elements, namely $\prod_{p^e||n}(e+1)$ and every element of the right side belongs to the left side, both of them must be equal. □

Now, for a prime p,

$$\tau(p^e) = e + 1$$

$$\begin{aligned} F(p^e) &= \sum_{d|p^e} \tau(d) \\ &= \sum_{i=0}^{e} \tau(p^i) \\ &= \sum_{i=0}^{e} (i+1) \\ &= \frac{(e+1)(e+2)}{2} \end{aligned}$$

Now we try to bound the right side by finding $p \geq 3$ satisfying,

$$p^e > \frac{(e+1)(e+2)}{2}$$
$$\iff 2(p^e - 1) > e(e+3)$$

by induction on e. Indeed, it's true for $e = 2$ if $p > 3$ and true for $e = 1$ if $p = 3$. Assuming it's true for $e = 1$, we need to prove

$$2(p^{e+1} - 1) > (e+1)(e+4)$$

$$\begin{aligned} 2(p^{e+1} - 1) &= 2p(p^e - 1) + 2p - 2 \\ &> pe(e+3) + 2p - 2 \\ &> p(e+1)(e+2) - 2 \end{aligned}$$

Again, note that,

$$p(e+1)(e+2) - 2 > (e+1)(e+4)$$
$$\iff (e+1)(pe + 2p - e - 4) > 2$$

Obviously, $e + 1 \geq 2$ and $pe + 2p - e - 4 = e(p-1) + 2(p-2) \geq 2$. Thus, the inequality holds.

Next, we try to find p, e satisfying

$$p^e < \frac{(e+1)(e+2)}{2}$$

We know that p must be 2. So we find

$$2^{e+1} < (e+1)(e+2)$$

which is false for $e > 3$. Then for odd n, we can say that the condition can hold only if $n = 3$.