Problems for Number Theory Exam

Masum Billal

March 22, 2015

Problem 1 (Somewhat easy)**.** An integer is *square-free* if it is not divisible by the square of a prime. Prove that, $a^{a-1}-1$ is not square-free where a is an integer.

Solution. Let n be a divisor of $a-1$. We will show that $n^2|a^{a-1}-1$. Since $n|a-1$, assume that $a-1=nk$ and $a^k=x$. Then we have $n|x-1$ and want to show that $n^2|x^n-1$. We are done if we can show $\dfrac{x^n-1}{x-1}$ is divisible by n. Remember the identity:

$$x^n-1=(x-1)(x^{n-1}+x^{n-2}+\ldots+1)$$

Now, $x^{n-1}+x^{n-2}+\ldots+1\equiv 1+1+\ldots+1\equiv n\equiv 0 \pmod{n}$.

Note. A similar problem was shown as an exercise in the class.

Problem 2 (Another give away)**.** Decide(with proof) if $2^{2016}+3^{2016}+4^{2016}+5^{2016}$ is a prime.

Solution. This is quite easy in fact. See that $2^{2016}+3^{2016}+\equiv 4^{2016}\equiv 5^{2016}\equiv 1+0+1+1\equiv 0 \pmod{3}$.

Problem 3 (Depends on the contestant if s/he remembers something special)**.** For a prime $p>5$, prove that $\binom{2p-1}{p-1}-1$ is divisible by p^3.

Solution. Wolstenholme's theorem was shown in the class too, which states:

$$\binom{ap}{bp}\equiv\binom{a}{b} \pmod{p^3}$$

for a prime $p>3$. Now, setting $a=2, b=1$, we have

$$\binom{2p}{p}\equiv\binom{2}{1}\equiv 2 \pmod{p^3}$$

Next, the identity $\binom{n}{k}=\frac{n}{k}\binom{n-1}{k-1}$ was also shown. Using that,

$$\binom{2p}{p}=2\binom{2p-1}{p-1}$$

Therefore, $p|2\binom{2p-1}{p-1}-2=2\left(\binom{2p-1}{p-1}-1\right)$. And since $(p,2)=1$, we have the result.

Problem 4 (Give away)**.** Prove that for integer a,b and a prime p, a^pb-ab^p is divisible by p.

Solution. This should be fairly easy too if someone can write the expression as $a^pb-ab^p=ab(a^{p-1}-b^{p-1})$. Now, if p divides either of a or b, we are done. Otherwise, from *Fermat's Little Theorem*, we have $a^{p-1}\equiv 1\equiv b^{p-1} \pmod{p}$ i.e. $p|a^{p-1}-b^{p-1}$.

Problem 5 (For making some contestants think and pass some time)**.** Find the number of positive integers(with respect to n) d so that d divides $a^n - a$ for all integer a.

Solution. This problem uses the idea of *primitive root*. First we prove that d must be square-free. Let's say p is a prime divisor of d and $p^2|d$. Then $p^2|a^n - a$ for all a. Set $a = p$ and we have $p^2|p(p^{n-1} - 1)$ which gives a contradiction $p|p^{n-1} - 1$ or $p|1$.

Say, $\mathbb{P}$ is the set of primes. Now we have to find the condition for p to be a prime factor of d. Note that, for $(a, p) = 1$, $p|a^{n-1} - 1$. If we consider a primitive root g of p(which exists for each prime, as we know) we get $g^{p-1} \equiv 1 \pmod{p}$ and $g^{n-1} \equiv 1 \pmod{p}$. Combining these two, $g^{(n-1,p-1)} \equiv 1 \pmod{p}$. We see that $p-1$ must divide n. Otherwise, if $n-1 = (p-1)l + r$ with $r < p-1$, $g^r \equiv 1 \pmod{p}$ which contradicts the primitivity of g. Thus, $p-1|n-1$ and so the maximum positive integer for which $d|a^n - a$ for all a, we have

$$d = \prod_{\substack{p \in \mathbb{P} \\ p-1|n-1}} p$$

Every divisor of d satisfies the condition of the problem. Let, $C(n)$ be the number of distinct prime p so that $p-1|n-1$. We know that d is square-free and it has $C(n)$ prime factors. Thus, d has $2^{C(n)}$ divisors, which is the answer.

Problem 6 (Stopper)**.** For a positive real number $c > 0$, call a positive integer $c - good$ if for all positive integer $m < n$, $\frac{m}{n}$ can be represented as

$$\frac{m}{n} = \frac{a_0}{b_0} + \ldots + \frac{a_k}{b_k}$$

for some non-negative integers $k < \frac{n}{c}, 2b_i \leq n$ and $0 \leq a_i < b_j, 0 \leq j \leq k$. Show that, for any real c, there are infinite $c - good$ positive integers.