NTR6 – Lifting the Exponent

Problem 1. (1999 IMO P4) Find all pairs of positive integers (x, p) such that p is prime, $x \leq 2p$, and $x^{p-1} \mid (p-1)^x + 1$.

Problem 2. (1990 IMO P3) Find all natural n such that

$$\frac{2^n + 1}{n^2}$$

is an integer.

Problem 1. (1999 IMO P4) Find all pairs of positive integers (x, p) such that p is prime, $x \leq 2p$, and

$$x^{p-1} \mid (p-1)^x + 1.$$

Solution.

Obviously $(1, p)$ where p is an arbitrary prime is a solution.

Consider the case when $x, p \geq 3$. (i.e., $p\ is\ odd$)
Let q be a prime divisor of x which must also be odd.
[$\because$ $p-1$ is even, $(p-1)^x + 1$ is odd, x is odd.]

$$q \mid x \mid x^{p-1} \mid (p-1)^x + 1$$

$$(p-1)^x \equiv -1\ (mod\ q) \tag{1}$$

By Fermat's Little Theorem,

$$(p-1)^{q-1} \equiv 1\ (mod\ q) \tag{2}$$

Special choice for q

We want $\gcd(x, q-1) = 1$. So, let q be redefined as the smallest prime divisor of x.

We are going to prove $p = q$.

Alternative way 1

By Bezout's Identity, there exist two integers α and β such that

$$\alpha x - \beta(q-1) = 1. (\because \gcd(x, q-1) = 1)$$

α must be odd. [$\because$ $q-1$ is even]

$$(p-1)^{x\alpha} \equiv (p-1)^{\beta(q-1)+1}\ (mod\ q)$$

$$(-1)^{\alpha} \equiv ((p-1)^{q-1})^{\beta} \cdot (p-1)\ (mod\ q)$$
$$-1 \equiv p-1\ (mod\ q)$$
$$p \equiv 0\ (mod\ q)$$

Alternative way 2

By squaring equation 1 and 2,

$$(p-1)^{2x} \equiv 1\ (mod\ q)$$
$$(p-1)^{2(q-1)} \equiv 1\ (mod\ q)$$
$$ord_q(p-1)^2 \mid x, ord_q(p-1)^2 \mid q-1$$
$$ord_q(p-1)^2 \mid \gcd(x, q-1) = 1$$

$$(p-1)^2 \equiv 1\ (mod\ q)$$
$$p(p-2) \equiv 0\ (mod\ q)$$

If $p-2 \equiv 0 (mod\ q)$,

$$(p-1)^x + 1 \equiv 1^x + 1 \equiv 2 \not\equiv 0\ (mod\ q)$$

This contradicts to $q \mid (p-1)^x + 1$.

$$\therefore p \equiv 0\ (mod\ q)$$

Since p and q are both primes, $p = q$.

We are going to prove that $p > 3$ is impossible.

Alternative way 1

Since $p = q, q \mid x$, then $p \mid x$. But $x \leq 2p$.

For all $x, p \geq 3$, $x = p$.

$$p^{p-1} \mid (p-1)^p + 1 = p^p - \binom{p}{1} p^{p-1} + \cdots - \binom{p}{p-2} p^2 + \binom{p}{p-1} p - 1 + 1$$
$$= p^2 \left(p^{p-2} - \binom{p}{1} p^{p-3} + \cdots - \binom{p}{p-2} + 1\right)$$

Since the expression in the parentheses is not divisible by p, $p-1 \leq 2, p \leq 3$.

Alternative way 2

For odd primes,

$$x^{p-1} \mid (p-1)^x + 1$$

By lifting the exponent, (satisfying 3 conditions, $p \neq 2, \gcd(p, p-1) = \gcd(p, 1) = 1, p \mid (p-1) + 1$

For $x \leq 2p, p \neq 2, v_p(x^{p-1}) = p - 1$

$$v_p((p-1)^x+1) = 1 + v_p(x) \geq p-1$$

$$v_p(x) \geq p-2$$

$$x \geq p^{p-2} > 2p \; for \; p > 3$$

[$\because p^{p-2} > 2p$ for $p > 3$]

This contradicts to $x \leq 2p$. So, $p > 3$ is impossible.

Using manual case work,

$p = 2$ gives $x \mid 2$ or $x = 1,2$.

$p = 3$ gives $x^2 \mid 2^x + 1$ where $x \leq 6$. We have $x = 1,3$.

The only solutions are hence $(x, p) = (1, p), (2,2), (3,3)$.

∎