POW 23 - 10

2020 8142 최백준

Sol). $p^p+q^q+1 \equiv p^pq^q+p^p+q^q+1 \equiv (p^p+1)(q^q+1) \pmod{pq}$.

since $p \nmid p^p+1$, $q \nmid q^q+1$ & p, q are prime, $p \mid q^q+1$ & $q \mid p^p+1$

WLOG, $p>q$. Let a_q be the smallest number s.t $q^{a_q} \equiv 1 \pmod p$

Since $q^q \equiv -1 \pmod p$, $a_q \mid 2q$ (If not, then $\exists$. $0<r<a_q$

s.t $q^r \equiv 1 \pmod p$ where $2q \equiv r \pmod{a_q}$, which is contradiction)

So, $a_q = 1, 2, q, 2q$. For the case of $a_q = 1, q$, since

$q^q \equiv -1 \pmod p$, a_q could not be $1, q$. So a_q should be either 2 or $2q$.

i). $a_q = 2$.

Suppose $q>2$, then $q^q \equiv (q^2)^{\frac{q-1}{2}} \cdot q \equiv q \pmod p \Rightarrow q \equiv -1 \pmod p$

Since $p>q$, $p = q+1$. However, p, q are primes, so $p \neq q+1$.

For $q=2$, then $2^2 \equiv -1 \pmod p \Rightarrow p=5$.

Since $2^2+5^5+1 = 3130$, $(2, 5)$ satisfies the condition.

ii). $a_q = 2q$.

By Fermat's little theorem, $q^{p-1} \equiv 1 \pmod p$. By the definition of a_q,

$a_q \mid p-1$. $\Rightarrow$ $p = 2qk+1$ for some $k \in \mathbb{N}$. Then

$p^p+1 = (2qk+1)^p+1 = q \cdot G(q,k) + 2 \equiv 0 \pmod q$ (for some polynomial $G(q,k)$)

this indicates that $q \mid 2$, which means $q=2$.

As seen in i) $a_q = 2$, $(2, 5)$ satisfies the condition.

Hence, $(2, 5)$ is the only pair for $pq \mid p^p+q^q+1$, where p, q are prime