A Solution to OC722

Jonathan Kasongo

April 10, 2025

Problem statement: Let p and q be distinct prime numbers. Given an infinite decreasing arithmetic sequence in which each of the numbers p^{23}, p^{24}, q^{23} and q^{24} occurs, prove that the numbers p and q are sure to occur in this sequence.

WLOG assume that $p > q$. Let the common difference of consecutive terms in the sequence be d.

Claim: $d \leq q - 1$

For some $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$,

$$p^{24} - p^{23} = \lambda_1 d$$
$$q^{24} - q^{23} = \lambda_2 d$$
$$p^{24} - q^{24} = \lambda_3 d$$

We claim that d has to be coprime to both p and q. Assume that d divides p. Then reducing the third equation modulo p would imply that $q^{24} \equiv 0 \pmod{p}$ which is impossible since p and q are distinct prime numbers. By using the symmetry of the first 2 equations this also proves that d is coprime to q.

Now consider $q^{24} - q^{23} = q^{23}(q-1) = \lambda_2 d$. Since d is coprime with q, we must have $d \mid (q-1)$. So $q - 1 \geq d$ ■.

Now to prove that p and q are in the sequence it suffices to prove that there exists some $k_1, k_2 \in \mathbb{Z}$ so that,

$$p^{24} - p = k_1 d$$
$$q^{24} - q = k_2 d$$

Equivalently we will be done if we can show that,

$$p^{24} \equiv p \pmod{d}$$
$$q^{24} \equiv q \pmod{d}$$

It then suffices to prove that $p^{23} \equiv q^{23} \equiv 1 \pmod{d}$.
However we know that

$$p^{24} - p^{23} = \lambda_1 d$$
$$q^{24} - q^{23} = \lambda_2 d$$

Once we reduce modulo d on both of these equations and rearrange we end up seeing that $p \equiv q \equiv 1 \pmod{d}$ from which the target result follows immediately.