14TSTST6

Himadri Mandal

November 15, 2021

§1 Solution

Solution. Could not solve it but found it instructive. Let α be the first integer such that $p|ca^\alpha - db^\alpha$, λ is the order of a/b.

$$\nu_p\left(ca^{\alpha+n\lambda} - db^{\alpha+n\lambda}\right) = \nu_p\left(\left(\frac{a^\lambda}{b^\lambda}\right)^n - \frac{da^\alpha}{cb^\alpha}\right)$$

to be constant.

Proposition

$x \equiv y \equiv 1 \pmod p$. If the sequence $\nu_p\left(x^n - y\right)$ of positive integers is nonconstant, then it is unbounded.

Claim — Suppose m and n are positive integers such that

$$d = \nu_p(x^n - y) < \nu_p(x^m - y) = e.$$

Then there exists ℓ such that $\nu_p(x^\ell - y) \geq e + 1$.

Proof. $\nu_p(x^m - x^n) = \nu_p\left((x^m - y) - (x^n - y)\right) = d$

$$\nu_p(x^k - 1) = e$$

for $k = p^{e-d}|m - n|$. Now we set $x^k = p^e u + 1$ and $x^m = p^e v + y$. Thus we get for $1 \leq r \leq p - 1$

$$\begin{aligned} x^{kr+m} - y &= (p^e u + 1)^r \cdot (p^e v + y) - y \\ &= p^e\left(v + yu \cdot r\right) + p^{2e}\left(\dots\right). \end{aligned}$$

Choosing r with $r \equiv -\frac{v}{u} \pmod p$, we have $p^{e+1} \mid x^{kr+m} - y$, hence $\ell = kr + m$ proves the claim. □

This proves the proposition but as it was equivalent to the problem, we are done. □