Lemma (DPV 1.23)

x is unique (mod N), if

$$a \cdot x \equiv 1 \ (mod\ N). \tag{1}$$

Proof.

Note we are going to find $x \in [1, \ldots, N-1]$.
Assume $a = 1$, then x is unique at $x = 1$.
Assume $a \neq 1$ and $\exists y \neq x$, $y \in [1, \ldots, N-1]$ satisfying Eq. 1, we have

$$\begin{aligned} a \cdot x &= k_1 \cdot N + 1 \\ a \cdot y &= k_2 \cdot N + 1 \end{aligned}$$

Note x, y are in $[1, \ldots, N-1]$, without loss of generality, we assume $x > y$ and $x - y$ still falls in $[1, \ldots, N-1]$.
Then, $a \cdot (x - y) = (k_1 - k_2) \cdot N$. Since we assume $x \neq y$, note $a \neq 0$, $N \neq 0$, $k_1 \neq k_2$ (otherwise, $a \cdot x = a \cdot y$ results $x = y$ since $a \neq 0$), we know either $a|N$ or $a|(k_1 - k_2)$.
If $a|N$, say $a \cdot c = N$ where $c \neq 1$, then $a \cdot x = k_1 \cdot a \cdot c + 1$, which conflicts the fact $a \neq 1$.
Thus, $a|(k_1 - k_2)$ must hold. Assume $a \cdot d = (k_1 - k_2)$. Then $x - y = d \cdot N$. We conclude $d < 1$. Thus, $d = 0$.
So, $x \equiv y \ (\text{mod } N)$.

□

Problem (DPV 1.13)

Is the difference of 5^{30000} *and* 6^{123456} *a multiple of* 31*?*

Proof.

Note $31 = 5 \cdot 6 + 1$.
From Fermat's Little Theorem: If p is a prime, $\forall 1 \leq a < p, a^{p-1} \equiv 1 \mod p$.
31 is a prime. Then, we know $5^{30} \equiv 1 \mod 31$ and $6^{30} \equiv 1 \mod 31$.
$5^{30000} = (5^{30})^{1000} = (31 \cdot k_1 + 1)^{1000} \equiv 1 \mod 31$.
$6^{123456} = (6^{30})^{4115} \cdot 6^6 = (31 \cdot k_2 + 1)^{4115} \cdot 6^6 \equiv 1 \cdot 6^6 \equiv 6^6 \mod 31$.
Furthermore, $6^6 = (6^2)^3 = (31 + 5)^3 \equiv 5^3 \mod 31$.
Note $5^3 = 125 \equiv 1 \mod 31$. So, the difference is a multiple of 31.

□