Recall the challenge's RSA scheme:
Robin has 5 primes, $p_1, p_2, ..., p_5$, two semi-semi-primes $N_1 = p_1 p_2 p_3$ and $N_2 = p_3 p_4 p_5$,
a message $m \in \mathbb{Z}_{N_1}\mathbb{Z}_{N_2}$ (in practice, this just means $m < N_1$ and $m < N_2$), a public exponent $e = \texttt{0x10001}$, and two ciphertexts $c_1 \equiv m^e \mod N_1$ and $c_2 \equiv m^e \mod N_2$.

Note that given only N_1, N_2, we can efficiently compute $\gcd(N_1, N_2) = p_3$.

Robin can easily decrypt the ciphertexts:
By Fermat's little theorem, we can treat the exponents in $\mathbb{Z}_{N_1}$
as if they're under mod $\phi(N_2) = (p_3 - 1) \cdot (p_4 - 1) \cdot (p_5 - 1)$.
(This is one of the corollaries under "Generalizations" in https://en.wikipedia.org/wiki/Fermat's_little_theorem).

Note that there is a natural injection $f : \mathbb{Z}_{N_2} \to \mathbb{Z}_{p_3}$, which is just taking mod p_3 of the elements of $\mathbb{Z}_{N_2}$.
But, if we look at the restriction $S = \{x \in \mathbb{Z}_{N_2} : x < p_3\} \subseteq \mathbb{Z}_{N_2}$, then $f : S \to \mathbb{Z}_{p_3}$ *is* now a natural bijection.
(What we mean by "natural" above is just that the underlying elements from $\mathbb{N}$ don't change under f.)

In particular, if $m \in S$ (i.e, if m is *small enough*), then we would find $f(m) = m \in \mathbb{Z}_{p_3}$.
This means we might be able to use a different calculation to find m:

$$
\begin{aligned}
m &\equiv c^{\left(e^{-1} \mod \phi(N_2)\right)} && \mod N_2 \\
f(m) &\equiv f\left(c^{\left(e^{-1} \mod \phi(N_2)\right)}\right) && \mod p_3 \\
f(m) &\equiv f(c)^{\left(e^{-1} \mod \phi(N_2) \mod \phi(p_3)\right)} && \mod p_3 \quad \text{(because FLT must be true of } f(c) \text{ under mod } p_3) \\
f(m) &\equiv f(c)^{\left(e^{-1} \mod \phi(p_3)\right)} && \mod p_3 \quad \text{(because } p_3 \text{ divides } N_2) \\
m &\equiv f(c)^{\left(e^{-1} \mod p_3 - 1\right)} && \mod p_3
\end{aligned}
$$

See `solve.py` for what this calculation looks like in python.