CRT
F&T

Ex: $\begin{cases} n \equiv 2 \pmod 3 & ① \\ n \equiv 3 \pmod 5 & ② \\ n \equiv 2 \pmod 7 & ③ \end{cases}$

① ② $\Rightarrow$ 8 is one solution. So complete solution is $n \equiv 8 \pmod{15}$ ④

③ ④ $\Rightarrow$ $n = 8 + 15x$. Sub into ③:

$$8 + 15x \equiv 2 \pmod 7$$
$$x \equiv 1 \pmod 7$$

$x = 1$ is one soln $\Rightarrow n = 8 + 15x = 23$ is one solution to ③ ④.

So the complete solution (by CRT) is:

$$\boxed{x \equiv 23 \pmod{105}}$$

Generalized CRT. Let $m_1, \dots, m_k \in \mathbb{N}$ where $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. For any $a_1, \dots, a_k \in \mathbb{Z}$, there exist an int solution to

$$\begin{cases} n \equiv a_1 \pmod{m_1} \\ n \equiv a_2 \pmod{m_2} \\ \vdots \\ n \equiv a_k \pmod{m_k} \end{cases}$$

If n_0 is one solution, then the complete soln is $n \equiv n_0 \pmod{m_1, m_2, \dots, m_k}$

Proof: By induction. $\boxed{\text{done.}}$

Modulus Splitting: $a \equiv b \pmod{mn} \iff a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ when $\gcd(m,n)=1$.

Example: $13x \equiv 23 \pmod{42}$ $\quad 42 = 6 \cdot 7 \quad \gcd(6,7)=1$

$\iff 13x \equiv 23 \pmod{6}$ ①
$\quad\;\; 13x \equiv 23 \pmod{7}$ ②

① $\Rightarrow x \equiv 5 \pmod{6}$

② $\Rightarrow -x \equiv 2 \equiv -5 \pmod{7} \implies x \equiv 5 \pmod{7}$

$x=5$ is one soln, so by CRT, complete soln is $x \equiv 5 \pmod{42}$.

Fermat's little theorem (FlT)

Theorem (FlT): If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.
Or, if p is prime and $[a] \neq [0]$ in $\mathbb{Z}_p$, then $[a^{p-1}] = [1]$.

Example: $p=5$. $1^4 = 1 \pmod{5}$
$2^4 = 16 \equiv 1 \pmod{5}$
$3^4 = 81 \equiv 1 \pmod{5}$
$4^4 \equiv 256 \equiv 1 \pmod{5}$

Illustrated for 1st step: $\mathbb{Z}_7$ $\quad a=3$. $[a], [2a], [3a], [4a], [5a], [6a]$

$$\begin{array}{cccccc} [3] & [6] & [9] & [12] & [15] & [18] \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ [3] & [6] & [2] & [5] & [1] & [4] \end{array} \Bigg\} \text{all non-zero classes in } \mathbb{Z}_7$$

Proof of FlT: Consider $[a], [2a], \ldots, [(p-1)a]$ in $\mathbb{Z}_p$.
We claim that none are $[0]$: Suppose $[ka]=[0]$ for some $1 \le k \le p-1$. So $p \mid ka$. Since $p \nmid a$, $\gcd(p,a)=1$. By CAD, $p \mid k$.
But $1 \le k \le p-1$, contradiction. So $[ka] \ne [0]$
We claim that these are distinct congruence classes.
Suppose $[ka]=[la]$ for some $1 \le k, l \le p-1$. Since $\gcd(p,a)=1$, $[a]^{-1}$ exists. Then $[ka][a]^{-1} = [la][a]^{-1}$, so $[k]=[l]$.
Since $1 \le k, l \le p-1$, $k=l$. So $[a], [2a], \ldots, [(p-1)a]$ are distinct nonzero cong classes.

This means that $\{[a], \ldots, [(p-1)a]\}$ is a rearrangement of $\{[1], [2], \ldots, [p-1]\}$. Take the product of each set to get $[a][2a] \cdots [(p-1)a] = [1][2] \cdots [p-1]$

$$\Rightarrow [(p-1)!\, a^{p-1}] = [(p-1)!]$$

Since $1, 2, \ldots, p-1$ are coprime with p, $\gcd(p,(p-1)!)=1$.
So $[(p-1)!]^{-1}$ exists in $\mathbb{Z}_p$. Multiply by $[(p-1)!]^{-1}$ to get $[a^{p-1}]=[1]$ in $\mathbb{Z}_p$. $\square$

Example: 35^{8888} divided by 89.

By FlT, $35^{88} \equiv 1 \pmod{89}$.

So $35^{8888} \equiv 1^{101} \equiv 1 \pmod{89}$

Corollary: If p is prime, then $a^p \equiv a \pmod{p}$.

Proof: when $p \mid a$, $a^p \equiv 0 \equiv a \pmod{p}$

when $p \nmid a$, $a^p \equiv a^{p-1} a \equiv a \pmod{p}$ by FlT $\square$.