Find the remainder when 7^{92} is divided by 11.

Recall (FlT): If $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$ (for p a prime)

By FlT $7^{10} \equiv 1 \bmod 11$

$\Rightarrow 7^{90} \equiv 1 \bmod 11$

$\Rightarrow 7^{92} \equiv 7^2 \equiv 49 \equiv 5 \bmod 11.$

Option 2: $7^{92} \equiv 7^{9(10)+2} \bmod 11$

$\equiv (7^{10})^9 \cdot 7^2 \bmod 11$

FlT. $\equiv 1^9 \cdot 7^2 \bmod 11$

$\equiv 49 \bmod 11$

$\equiv 5 \bmod 11$

Corollary: If p is a prime and $a \in \mathbb{Z}$ then $a^p \equiv a \bmod p$

Pf: If $p \mid a$ then $a \equiv 0 \bmod p$
$\Rightarrow a^p \equiv 0 \equiv a \bmod p$.
If $p \nmid a$ then by FlT:
$a^{p-1} \equiv 1 \bmod p \Rightarrow a^p \equiv a \bmod p$! ■

Corollary: If p is a prime number and $[a] \neq [0]$ in $\mathbb{Z}_p$, then $\exists [b] \in \mathbb{Z}_p$ s.t. $[a][b] = [1]$.

Pf: Since $[a] \neq [0]$, $p \nmid a$. Hence by FlT $a^{p-1} \equiv 1 \bmod p$
$a a^{p-2} \equiv 1 \bmod p$
Sensible since $p-2 \geq 0$. Thus, take $[b] = [a^{p-2}]$. ■

Corollary: If $r = s + Kp$ then $a^r \equiv a^{s+K} \bmod p$ (p is a prime, $a, r, s, K \in \mathbb{Z}$)

Pf:

$$a^r \equiv a^{s+Kp} \bmod p$$

$$\equiv a^s (a^p)^K \bmod p$$

(Cor. to FLT) $$\equiv a^s (a)^K \bmod p$$

$$\equiv a^{s+K} \bmod p.$$

Prove that if $p \nmid a$ and $r \equiv s \mod (p-1)$ then $a^r \equiv a^s \mod p$.

Since $\cancel{p}$ $r \equiv s \mod (p-1)$

$(p-1) \mid r-s$

$\exists k \in \mathbb{Z}$ s.t. $(p-1)k = r-s$

$\Rightarrow r = s + (p-1)k$

$a^r \equiv a^{s+(p-1)k} \mod p$

$\equiv a^s (a^{p-1})^k \mod p$

(FLT) $\equiv a^s (1)^k \mod p$

$\because p \nmid a$

$\equiv a^s \mod p$

L30P5
Version 1

Chinese Remainder Theorem (CRT)

Solve
$$x \equiv 2 \bmod 7$$
$$x \equiv 7 \bmod 11$$

Using the first condition, write
$$x = 2 + 7k$$

Plug into the second condition
$$2 + 7k \equiv 7 \bmod 11$$
$$7k \equiv 5 \bmod 11$$

Multiply both sides by 3

Used that $\gcd(7,11)=1$ to find 7^{-1}.

$$3 \cdot 7k \equiv 15 \bmod 11$$
$$21k \equiv 4 \bmod 11$$
$$-k \equiv 4 \bmod 11$$
$$k \equiv -4 \equiv 7 \bmod 11$$
$$\therefore k = 7 + 11\ell \text{ for some } \ell \in \mathbb{Z}$$

Version 1

Recall $x = 2 + 7k$

$= 2 + 7(7 + 11\ell)$

$= 51 + 77\ell$

$\therefore x \equiv 51 \mod 77$

L30PS
Version2

Chinese Remainder Theorem (CRT)

Solve: $x \equiv 2 \mod 7$

$x \equiv 7 \mod 11$

Condition 1 says

$x = 2 + 7k$ for some $k \in \mathbb{Z}$

Plug into condition 2:

$$2 + 7k \equiv 7 \mod 11$$

$$7k \equiv 5 \mod 11$$

This is equivalent to

$$7k + 11y = 5$$

k	y	r	q
0	1	11	
1	0	7	
-1	1	4	1
2	-1	3	1
-3	2	1	1
		0	3

$\therefore 7(-3) + 11(2) = 1$

$\therefore 7(-15) + 11(10) = 5$

LDET2: $k = -15 + 11n$ for all $n \in \mathbb{Z}$

~~Needed~~ Used $\gcd(7, 11) = 1$.

$\therefore\ k \equiv -15 \equiv 7 \mod 11$

$k = 7 + 11\ell$ for some $\ell \in \mathbb{Z}$.

Recall: $x = 2 + 7k$

$= 2 + 7(7 + 11\ell)$

$= 51 + 77\ell$.

$\therefore\ x \equiv 51 \mod 77$ is the sol'n.

Theorem (Chinese Remainder Theorem (CRT)). *If* $\gcd(m_1, m_2) = 1$*, then for any choice of integers* a_1 *and* a_2*, there exists a solution to the simultaneous congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is* $n \equiv n_0 \pmod{m_1 m_2}$.

Theorem (Generalized CRT (GCRT)). *If* $m_1, m_2, \ldots, m_k$ *are integers and* $\gcd(m_i, m_j) = 1$ *whenever* $i \neq j$*, then for any choice of integers* $a_1, a_2, \ldots, a_k$*, there exists a solution to the simultaneous congruences*

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

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is*

$$n \equiv n_0 \pmod{m_1 m_2 \ldots m_k}$$