Lecture 30

Handout or Document Camera or Class Exercise

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

Solution: Recall (FℓT): If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$ where p is a prime.

By FℓT,

$$\begin{aligned} 7^{10} &\equiv 1 \pmod{11} \\ 7^{90} &\equiv 1 \pmod{11} && \text{Raise both sides to the power of 9} \\ 7^{92} &\equiv 7^2 \equiv 49 \equiv 5 \pmod{11} \end{aligned}$$

Alternatively,

$$\begin{aligned} 7^{92} &\equiv 7^{9(10)+2} \pmod{11} \\ &\equiv (7^{10})^9 7^2 \pmod{11} \\ &\equiv 1^9 \cdot 7^2 \pmod{11} && \text{By F}\ell\text{T since } 11 \nmid 7 \\ &\equiv 49 \pmod{11} \\ &\equiv 5 \pmod{11} \end{aligned}$$

completing the question. ∎

Instructor's Comments: This is the 10 minute mark

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

Proof: If $p \mid a$, then $a \equiv 0 \pmod{p}$. This implies that $a^p \equiv 0 \equiv a \pmod{p}$.

If $p \nmid a$, then by FℓT, $a^{p-1} \equiv 1 \pmod{p}$ and hence $a^p \equiv a \pmod{p}$ completing the proof. ■

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

Proof: Since $[a] \neq [0]$, we see that $p \nmid a$. Hence by FℓT, $a^{p-1} \equiv 1 \pmod{p}$ and thus $a \cdot a^{p-2} \equiv 1 \pmod{p}$. This is sensible since $p - 2 \geq 0$. Thus, take $[b] = [a^{p-2}]$. ■

Instructor's Comments: Students should be able to do the next one - give them a shot at it on their own first! There's a handout one that depends on this so it might be good to get them thinking.

Corollary: If $r = s + kp$, then $a^r \equiv a^{s+k} \pmod{p}$ where p is a prime and $a \in \mathbb{Z}$ and $r, s, k \in \mathbb{N}$.

Instructor's Comments: It should be noted that here we want r, s, k to be at least nonnegative. We haven't really talked about what it means to take a^k when $k < 0$ except for $k = -1$. It's not hard but in this corollary, the important fact is that a might not be invertible so things like a^{-3} don't make sense necessarily.

Proof: We have

$$\begin{aligned} a^r &\equiv a^{s+kp} \pmod{p} \\ &\equiv a^s(a^p)^k \pmod{p} \\ &\equiv a^s(a)^k \pmod{p} && \text{By corollary to F}\ell\text{T} \\ &\equiv a^{s+k} \pmod{p} \end{aligned}$$

Instructor's Comments: This is the 20 minute mark.

Handout or Document Camera or Class Exercise

Let p be a prime. Prove that if $p \nmid a$ and $r \equiv s \pmod{(p-1)}$, then $a^r \equiv a^s \pmod{p}$ for any $r, s \in \mathbb{Z}$.

Solution: Since $r \equiv s \pmod{(p-1)}$, we have that $(p-1) \mid (r-s)$. Thus, there exists a $k \in \mathbb{Z}$ such that $(p-1)k = r - s$. Hence $r = s + (p-1)k$. Thus,

$$\begin{aligned} a^r &\equiv a^{s+(p-1)k} \pmod{p} \\ &\equiv a^s (a^{p-1})^k \pmod{p} \\ &\equiv a^s (1)^k \pmod{p} && \text{By F}\ell\text{T since } p \nmid a \\ &\equiv a^s \pmod{p}. \end{aligned}$$

This completes the proof. ■

Instructor's Comments: This is the 30 minute mark

Chinese Remainder Theorem (CRT)

Solve

$$x \equiv 2 \pmod 7$$
$$x \equiv 7 \pmod{11}$$

Instructor's Comments: Note to students this is the first time they are seeing two congruences with different moduli.

Using the first condition, write $x = 2 + 7k$ for some $k \in \mathbb{Z}$. Plugging into the second condition gives

$$\begin{aligned} 2 + 7k &\equiv 7 \pmod{11} \\ 7k &\equiv 5 \pmod{11} \end{aligned}$$

Now there are a few ways to proceed. One could guess and check the inverse of 7. With this approach, we see that multiplying both sides by 3 gives

$$\begin{aligned} 3 \cdot 7k &\equiv 15 \pmod{11} \\ 21k &\equiv 4 \pmod{11} \\ -k &\equiv 4 \pmod{11} \\ k &\equiv -4 \pmod{11} \\ k &\equiv 7 \pmod{11} \end{aligned}$$

Therefore, $k = 7 + 11\ell$ for some $\ell \in \mathbb{Z}$. Alternatively, one can use the LDE approach on $7k + 11y = 5$ and use the Extended Euclidean Algorithm:

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

Hence $7(-3) + 11(2) = 1$ and thus $7(-15) + 11(10) = 5$. So by LDET2, we have that $k = -15 + 11n$ for all $n \in \mathbb{Z}$. Thus $k \equiv -15 \equiv 7 \pmod{11}$ and as above $k = 7 + 11\ell$ for some $\ell \in \mathbb{Z}$.

Instructor's Comments: Note here that to find all solution we need to use for all $n \in \mathbb{Z}$. Because out specific k is fixed however, we us for some at the end. What's happened here is that we've overloaded the use of k - once in the question but once in the LDE question process. This isn't a big deal and probably isn't worth mentioning unless a student asks.

Thus, since $x = 2 + 7k$ and $k = 7 + 11\ell$, we have

$$\begin{aligned} x &= 2 + 7k \\ &= 2 + 7(7 + 11\ell) \\ &= 51 + 77\ell \end{aligned}$$

Therefore, $x \equiv 51 \pmod{77}$ is the solution. ■

Instructor's Comments: This might take you to the 50 minute mark. Otherwise state the slide on the next lecture.