

Section 6 - Fermat's & Wilson's Theorems

Q: what is the LR of $(10)^{73} \pmod{11}$?

$$10^{73} \equiv (-1)^{73} \equiv -1 \equiv \boxed{10} \pmod{11}$$

Q: what is the LR of $3^{73} \pmod{11}$?

$$3^{73} \equiv \dots ?! \text{ too hard?}$$

Theorem 1 (Fermat's Theorem) Let $a, p \in \mathbb{Z}$. If p is prime and $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

$a \not\equiv 0 \pmod{p}$

Some reformulations — these can also be referenced as Fermat's Theorem:

- * if p is prime and $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$
- * if p is prime, then $a^p \equiv a \pmod{p}$.

Ex Find the LR of $3^{73} \pmod{11}$.

* By Fermat, $3^{10} \equiv 1 \pmod{11}$.

$$* 3^{73} \equiv 3^{70} \cdot 3^3 \equiv (3^{10})^7 \cdot 3^3 \equiv 1 \cdot 3^3 \equiv 27 \equiv \boxed{5} \pmod{11}$$

(Note: $27 \equiv 2 \cdot 11 + 5$)

Ex use a table to prove Fermat's theorem for the prime $p=5$.

a	a^2	a^3	a^4	$(\pmod{5})$
0	0	0	0	
1	1	1	1	
2	4	3	1	
3	4	2	1	
4	1	4	1	

$$a \not\equiv 0 \Rightarrow a^{p-1} \equiv 1$$

We now work to prove Fermat's Theorem.

Lemma 1 Let $m \in \mathbb{Z}^+$. If $(a, m) = 1$, then modulo m , the least residues of

$$a, 2a, 3a, \dots, (m-1)a$$

are

$$1, 2, 3, \dots, (m-1)$$

but not necessarily in order.

Ex Let $a = 5$. Find the least residues of the following modulo 8: $a, 2a, 3a, \dots, 7a$.

we want L.R. of $5, 10, 15, 20, 25, 30, 35 \pmod{8}$.

5	10	15	20	25	30	35
5	2	7	4	1	6	3

rearrange $\rightarrow 1, 2, 3, 4, 5, 6, 7$.

pt of Lemma 1

Step 1: $a, 2a, 3a, \dots, (m-1)a$ are all different mod m .

pf Assume $ra \equiv sa \pmod{m}$ with $1 \leq r, s \leq m-1$.
Since $(a, m) = 1$, a is cancellable, so $r \equiv s \pmod{m}$.
The only way $1 \leq r, s \leq m-1$ and $r \equiv s \pmod{m}$ is if $r = s$. Thus $ra \equiv sa \pmod{m}$ only if $r = s$.

Step 2: $a, 2a, 3a, \dots, (m-1)a$ are all nonzero mod m .

pt Assume $ra \equiv 0 \pmod{m}$. Since $(a, m) = 1$, a is cancellable, so $r \equiv 0 \pmod{m}$. Thus, $ra \not\equiv 0$ for $r = 1, 2, \dots, (m-1)$.

Step 3: Putting it together.

◦ $a, 2a, 3a, \dots, (m-1)a$ are different mod m
so their LR's are all different

◦ $a, 2a, 3a, \dots, (m-1)a$ are all nonzero mod m
so no LR is 0.

Thus, the only possibility is that the LR's are

$1, 2, 3, \dots, (m-1)$

in some order.

□

pt of Fermat's Thm

Let p be prime. Assume $(a, p) = 1$. We want to prove $a^{p-1} \equiv 1 \pmod{p}$

Observe that

$$1 \cdot 2 \cdot 3 \cdots (p-1) a^{p-1} \equiv a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

factor (pointing to a^{p-1}) by lemma 1 (pointing to $a \cdot 2a \cdot 3a \cdots (p-1)a$)

Thus,

$$\cancel{(p-1)!} a^{p-1} \equiv \cancel{(p-1)!} \pmod{p}$$

∴ $(p-1)!$ is rel. prime to p , so $(p-1)!$ is cancellable.

Hence

$$a^{p-1} \equiv 1 \pmod{p}$$

□

Ex (Dudley - #12 p. 48) In 1732, Euler wrote

"I derived [certain] result... although I have no proof:
 $a^n - b^n$ is divisible by the prime $n+1$ if neither
 a nor b is."

① check the result for various choices of a, b, n

$$n+1=3, a=5, b=4 \rightarrow 5^2 - 4^2 = 25 - 16 = 9$$

$$n+1=3, a=7, b=8 \rightarrow 7^2 - 8^2 = 49 - 64 = -15$$

② Prove the result (using Fermat's Theorem)

◦ $n+1=p$. $n+1 \mid a^n - b^n \iff p \mid a^{p-1} - b^{p-1}$

$$\iff a^{p-1} - b^{p-1} \equiv 0 \pmod{p}$$

◦ Now, $a^{p-1} - b^{p-1} \equiv 1 - 1 \equiv 0$ by Fermat's Thm. \square

Ex Find the last digit of 8^{213} .

want LR of $8^{213} \pmod{10}$.

⚠ 10 is not prime, so we cannot use Fermat's Theorem

Technique: work mod 2 and mod 5 ($10=2 \cdot 5$)

◦ let a be the LR of $8^{213} \pmod{10}$.

— $0 \leq a < 9$

— let's find $a \pmod{2}$ and $a \pmod{5}$.

◦ $8^{213} \equiv 0^{213} \equiv 0 \pmod{2}$

◦ $8^{213} \equiv 3^{213} \equiv 3^{200} \cdot 3^{13} = \underbrace{(3^4)^{50}}_{\text{Fermat}} \cdot 3^{13} \equiv \underbrace{(3^4)^3}_{\text{Fermat}} \cdot 3 \equiv 3 \pmod{5}$

◦ $a = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$

$\Rightarrow 8^{213} \equiv 8 \pmod{10} \Rightarrow$ last digit of 8^{213} is $\boxed{8}$

Theorem 2 (Wilson?) Let $p \in \mathbb{Z}$. Then p is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Ex Compute

(a) $12! \pmod{13}$ (Wilson) $12! \equiv \boxed{-1} \pmod{13}$ $LR = 12$

(b) $11! \pmod{13}$ $11! \equiv a \Rightarrow 12! \equiv 12a \equiv -a \pmod{13}$
 $\Rightarrow -1 \equiv -a \Rightarrow a \equiv 1 \Rightarrow 11! \equiv \boxed{1}$

conjectures? (c) $14! \pmod{15}$ $14! \equiv 1 \cdot 2 \cdot \boxed{3} \cdot 4 \cdot \boxed{5} \cdot \dots \cdot 14 \equiv \boxed{0} \pmod{15}$
 LHS is mult. of 15

Generalize (b)...

Lemma Let $p \in \mathbb{Z}$. If p is prime, then $(p-2)! \equiv 1 \pmod{p}$.

pf

Let $(p-2)! \equiv a \pmod{p}$. WTS $a=1$. Observe,

$$\begin{aligned} (p-2)! \equiv a &\Rightarrow (p-1) \cdot (p-2)! \equiv (p-1) \cdot a \\ &\Rightarrow \cancel{(p-1)}! \equiv -a \\ &\Rightarrow -1 \equiv -a \\ &\Rightarrow a \equiv 1. \end{aligned}$$

□

Lemma Let $p \in \mathbb{Z}$. If p is prime, then $2 \cdot (p-3)! + 1 \equiv 0 \pmod{p}$

↑ Homework.

Generalize (c)...

Lemma Let $n \in \mathbb{Z}^+$. If n is composite, then either $(p-1)! \equiv 0 \pmod{n}$ or $n=4$ and $(p-1)! \equiv 2$.

pf

n composite $\Rightarrow n = a \cdot b$ $2 \leq a, b \leq n-1$

Case 1: it is possible to choose $a \neq b$ (i.e. $n \neq p^2$)

$$(n-1)! = 1 \cdot 2 \cdot 3 \cdots a \cdots b \cdots (n-1) \Rightarrow a \cdot b \mid (n-1)! \Rightarrow (n-1)! \equiv 0 \pmod{n}$$

Case 2 $n = p^2$ for p a prime.

① If $p=2$, $n=4$, then $(n-1)! \equiv 6 \equiv 2 \pmod{4}$.

② If $p \geq 3$, then $2p \leq (n-1) = p^2 - 1$ ($x^2 - 2x - 1$ incr. when $x > 1$
and $x^2 - 2x - 1 > 0$ when $x \geq 3$)

so $(n-1)! = 1 \cdot 2 \cdots p \cdots 2p \cdots (n-1)$.

Thus $p^2 \mid (n-1)! \Rightarrow (n-1)! \equiv 0 \pmod{n}$

□

pt of Theorem 2

Two things to prove:

① If p is prime, then $(p-1)! \equiv -1 \pmod{p}$

② If $(p-1)! \equiv -1 \pmod{p}$, then p is prime.

* pt of ②

If $(p-1)! \equiv -1 \pmod{p}$ then $(p-1)! \not\equiv 0 \pmod{p}$,

so p is NOT composite by previous lemma.

* pt of ① — need some preparation.

Lemma Let p be prime. If $a \not\equiv 0 \pmod{p}$ then $ax \equiv 1 \pmod{p}$ has a unique solution mod p .

pt $(a, p) = 1$ □

Def Let p be prime. If $a \not\equiv 0 \pmod{p}$, then the solution to $ax \equiv 1 \pmod{p}$ is denoted a^{-1} . Thus, $a \cdot a^{-1} \equiv 1 \pmod{p}$.

Ex For all a , find $a^{-1} \pmod{11}$.

a	0	1	2	3	4	5	6	7	8	9	10
a^{-1}	$0 \notin \mathbb{Z}$	1	6	4	3	9	2	8	7	5	10

solve $ax \equiv 1$

$$a \equiv 1: 1x \equiv 1 \Rightarrow x = 1$$

$$a \equiv 2: 2x \equiv 1 \Rightarrow 2x \equiv 12 \Rightarrow x \equiv 6$$

$$a \equiv 3: 3x \equiv 1 \Rightarrow 3x \equiv 12 \Rightarrow x \equiv 4$$

$$a \equiv 4: 4x \equiv 1 \text{ (we know } 3 \cdot 4 \equiv 1 \text{ so } 4 \cdot 3 \equiv 1)$$

$$a \equiv 5: 5x \equiv 1 \Rightarrow 5x \equiv -10 \Rightarrow x \equiv -2 \equiv 9$$

$$a \equiv 7 \equiv -4: 4^{-1} \equiv 3 \Rightarrow \underset{\substack{||| \\ 7}}{(-4)}^{-1} \equiv \underset{\substack{||| \\ 8}}{(-3)}$$

$$a \equiv 10 \equiv -1: -1 \cdot x \equiv 1 \Rightarrow x \equiv -1$$

Q: when is $a \equiv a^{-1}$?

$$a \equiv 1, -1, \dots? \quad a \equiv a^{-1} \Rightarrow a \cdot a \equiv a \cdot a^{-1} \equiv 1 \Rightarrow a^2 \equiv 1.$$

Lemma 2 Let p be prime. Then the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv 1, -1$.

pf

$$x^2 \equiv 1 \pmod{p} \iff x^2 - 1 \equiv 0 \pmod{p}$$

$$\iff (x-1)(x+1) \equiv 0 \pmod{p}$$

$$\iff p \mid (x-1)(x+1)$$

$$\iff p \mid x-1 \text{ or } p \mid x+1$$

$$\iff x-1 \equiv 0 \pmod{p} \text{ or } x+1 \equiv 0 \pmod{p}$$

$$\iff x \equiv 1 \pmod{p} \text{ or } x \equiv -1 \pmod{p}.$$

□

pt of Theorem 2 mod 11

want to show $(p-1)! \equiv -1 \pmod{p}$ so

$$(10)! \equiv -1 \pmod{11}$$

Recall:

a	0	1	2	3	4	5	6	7	8	9	10
a ⁻¹	∞	1	6	4	3	9	2	8	7	5	10

Thus,

$$10! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$$

$$\equiv 1 \cdot 2 \cdot \cancel{3} \cdot \cancel{3^{-1}} \cdot 5 \cdot \cancel{2^{-1}} \cdot \cancel{7} \cdot \cancel{7^{-1}} \cdot \cancel{5^{-1}} \cdot 10$$

$$\equiv 1 \cdot 10$$

$$\equiv 10 \equiv \boxed{-1}$$

For a general prime:

- pair numbers with their inverses
- by Lemma 2, only 1 and -1 are unpaired.
- pairs cancel to 1
- all that is left is $1 \cdot -1 \equiv \boxed{-1}$.

□

Lemma Let p be prime. If $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} = \frac{a}{b}$ then a is divisible by p .

pt

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} = \frac{a}{b}$$

$$\Rightarrow \frac{(p-1)!}{(p-1)!} + \overset{\text{omit}}{\frac{1 \cdot 2 \cdot 3 \dots (p-1)}{(p-1)!}} + \overset{\text{omit}}{\frac{1 \cdot 2 \cdot 3 \dots (p-1)}{(p-1)!}} + \overset{\text{omit}}{\frac{1 \cdot 2 \cdot 3 \dots (p-1)}{(p-1)!}} = \frac{a}{b}$$

optional

$$\Rightarrow b \cdot \left[(p-1)! + 1 \cdot \overline{2} \cdot 3 \cdots (p-1) + 1 \cdot 2 \cdot \overline{3} \cdots (p-1) + \cdots + 1 \cdot 2 \cdot 3 \cdots \overline{(p-1)} \right] \equiv a(p-1)! \pmod{p}$$

$$\Rightarrow b \cdot \left[(p-1)! + 2^{-1} \cdot (p-1)! + 3^{-1} \cdot (p-1)! + \cdots + (p-1)^{-1} \cdot (p-1)! \right] \equiv a(p-1)! \pmod{p}$$

$$\Rightarrow b \cdot (p-1)! \left[1 + 2^{-1} + 3^{-1} + \cdots + (p-1)^{-1} \right] \equiv a(p-1)! \pmod{p}$$

wilson

$$\Rightarrow \cancel{b} \cdot \underbrace{\left[1 + 2^{-1} + 3^{-1} + \cdots + (p-1)^{-1} \right]}_{\text{reorder}} \equiv \cancel{b} \cdot a \pmod{p}$$

$$\Rightarrow b \left[1 + 2 + 3 + \cdots + (p-1) \right] \equiv a \pmod{p}$$

$$\Rightarrow b \left[1 + 2 + 3 + \cdots + 3 + 2 + 1 \right] \equiv a \pmod{p}$$

$$\Rightarrow b \cdot 0 \equiv a \pmod{p}$$

$$\Rightarrow a \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid a \quad \square$$

optimal