Goal: Get to quadratic reciprocity

↳ when do quadratic eqns. have solns. mod p ?

To get there: need ingredients

① Special congruences

- Wilson's Thm
- Fermat's Little Theorem

Section 6.1 - Wilson's Thm and Fermat's Little Thm

· When proving ∞ many primes, we looked at

$$n!+1$$

n	1	2	3	4	5	6
$n!+1$	2	3	7	25	121	721
prime factors of $n!+1$	2	3	7	5	11	7, 103

it looks like $n+1$ is a factor of $n!+1$

when $n+1$ is prime

replace $n+1$ by p

it looks like p is a factor of $(p-1)!+1$ when p is prime

Thm (Wilson): If p is prime, then $p \mid (p-1)!+1$, i.e. $(p-1)!+1 \equiv 0 \mod p$

or $(p-1)! \equiv -1 \mod p$

Lemma: Inverses mod p are unique

I.e. If $1 \le a < p$ and $ac \equiv 1 \mod p$ and $ab \equiv 1 \mod p$

then $c \equiv b \mod p$

Hint: a is rel. prime to p

Hint: $ac \equiv 1 \equiv ab \mod p$

Pf: Recall if $xz \equiv yz \mod m$

then $x \equiv y \mod \frac{m}{(m,z)}$

So if $ac \equiv ab \mod p$

then $c \equiv b \mod \frac{p}{(a,p)} = p$ ✓

Lemma: If x is its own inverse mod p, then $x \equiv \pm 1 \mod p$ (supposing p prime)

Pf. If x is its own inverse, then

$$x^2 \equiv 1 \mod p$$

From HW, $x \equiv \pm 1 \mod p$

Recall: If p prime, $(p-1)! \equiv -1 \mod p$

Pf:
$$(p-1)! = \boxed{(p-1)} \underbrace{(p-2)(p-3)\cdots 3 \cdot 2}_{\text{none are } \pm 1 \text{ mod } p} \cdot \boxed{1} \mod p$$

$$\equiv (p-1) \cdot \underbrace{(p-2)(p-2)^{-1}} \underbrace{(p-3)(p-3)^{-1}} \cdots \cdot 1 \mod p$$

$$\equiv (p-1)\ 1 \cdot 1 \cdot \cdots \cdot 1 \mod p$$

$$\equiv -1 \mod p$$

Ex: What is the least positive residue of $40! \mod 1763$?

Note $1763 = 41 \cdot 43$

Now consider 1 $40!$ mod 41

and $40!$ mod 43

By Wilson's Thm $40! \equiv -1 \mod 41$

$40! \mod 43$

$$42 \cdot 41 \cdot (40!) = 42! \equiv -1 \mod 43$$

"divide by $42 \cdot 41$"

$$40! \equiv 42^{-1}\, 41^{-1} \cdot (-1) \mod 43$$

$$\equiv (-1)^{-1} \cdot (-2)^{-1} \cdot (-1) \mod 43$$

$$\equiv (-1) \cdot (-22)\,(-1) \mod 43$$

$$\equiv 21 \mod 43$$

Summary: $40! \equiv -1 \mod 41$

$40! \equiv 21 \mod 43$

$40! \equiv ? \mod 41 \cdot 43$

Sun Tsu's Thm: $x = 40!$

$x \equiv -1 \mod 41$

$x \equiv 21 \mod 43$ $\longrightarrow$ $x \equiv 1311 \mod 1763$

so $40! \equiv 1311 \mod 1763$

Fact: The converse to Wilson's Thm is true!

If $(n-1)! \equiv -1 \mod n$, then n is prime

Fermat's Little Theorem

Note: $\forall a: 2 \mid a^2 - a = a(a-1)$

$\forall a: 3 \mid a^3 - a = a(a-1)(a+1)$

$\neg \forall a: 4 \mid a^4 - a = a(a-1)(a^2+a+1)$

not

$\forall a: 5 \mid a^5 - a \leftarrow$ see HW

Thm: If p is prime, then $p \mid a^p - a$ for all $a \in \mathbb{Z}$

Pf: If $p \mid a$, then we're done

Suppose $p \nmid a$

Then p does not divide any of

$a, 2a, 3a, \ldots, (p-1)a$

Claim: The numbers $a, 2a, \dots, (p-1)a$ are pairwise incongruent mod p

Pf of claim If $ja \equiv ka \mod p$ for $1 \leq j, k \leq p-1$

a rel prime to p, so $j \equiv k \mod p$

Hence $j = k$

As a consequence: $\{\underbrace{0, a, 2a, \dots, (p-1)a}^{p \text{ elts.}}\}$ is a complete set of residues mod p.

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \mod p$$

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

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

only useful when $p \nmid a$

$$* \quad a^{p-1} \equiv 1 \mod p \quad *$$

$$a^p \equiv a \mod p$$

i.e. $p \mid a^p - a$

Cor: If $p \nmid a$ and p prime, then

a^{p-2} is the inverse of a mod p.

Pf: $a \cdot a^{p-2} \equiv a^{p-1} \equiv 1 \mod p$

Ex: Show $30 \mid n^9 - n \quad \forall n \in \mathbb{Z}$

Note $30 = 2 \cdot 3 \cdot 5$

<u>$p=2$</u>

If n even, $n^9 - n$ even
If n odd, $n^9 - n$ even $\Rightarrow 2 \mid n^9 - n$

ad hoc - arbitrary, nonsystematic

<u>$p=3$</u>

$$n^9 - n \equiv (n^3)^3 - n \equiv n^3 - n \mod 3$$
$$\equiv 0 \mod 3$$

<u>$p=5$</u>

$$n^9 - n \equiv n^5 \cdot n^4 - n \equiv n \cdot n^4 - n \mod 5$$

$$\equiv n^5 - n \equiv 0 \mod 5$$

We know $n^9 - n \equiv 0 \mod 2$

$n^9 - n \equiv 0 \mod 3$

$n^9 - n \equiv 0 \mod 5$

By Sun-Tsu's Thm, there is only one soln. to this system of congruences mod $2 \cdot 3 \cdot 5 = 30$

Since 0 is a soln.

$$\rightarrow n^9 - n \equiv 0 \mod 30$$

Ex: Compute the least pos. res. of 3^{201} mod 11.

$$3^{201} = 3^{200} \cdot 3 = (3^{10})^{20} \cdot 3$$

$$\equiv 1^{20} \cdot 3 \mod 11$$

$$\equiv 3 \mod 11$$

Ex: Compute the least pos. res. of

$$5^{4328} \bmod 101$$

prime

$$5^{4300}5^{28} = (5^{100})^{43}5^{28} \equiv 1^{43}5^{28} \bmod 101$$
$$= 5^{28} \bmod 101$$

$$5^2 \equiv 25 \bmod 101$$
$$5^4 \equiv 25^2 \equiv 625 \equiv 19 \bmod 101$$
$$5^8 \equiv 19^2 \equiv 361 \equiv 58 \bmod 101$$
$$5^{16} \equiv 31 \bmod 101$$
$$5^{28} \equiv 5^{16} \cdot 5^8 \cdot 5^4 \equiv 31 \cdot 58 \cdot 19 \equiv 24 \bmod 101$$