Proving congruences

p = prime

$a \equiv b \pmod n \iff a-b$ divisible by n

Lemma. G = group of size p, $g \in G$ be a generator.
G acts on a set X. Then

$$|X| \equiv |X^g| \pmod p.$$

Pf. From orbit-stabilizer, every orbit has either size p or 1.

$\Rightarrow |X| \equiv (\#\text{ orbits of size } 1) \pmod p$

An orbit of size 1 is an element $x \in X$ s.t. $h \cdot x = x$ for all $h \in G \iff g \cdot x = x \iff x \in X^g$

$\Rightarrow |X| \equiv |X^g| \pmod p$ □

Thm (Fermat's little theorem) Pick $a \in \mathbb{Z}$. Then

$$a^p \equiv a \pmod p.$$

Pf. If $a \equiv b \pmod p$, Then $a^p \equiv b^p \pmod p$

so suffices to prove thm for one representative of each mod p class. Pick $a \in \{1, \dots, p\}$.

$X = \{\text{functions } \mathbb{Z}/p \to [a]\}$, $|X| = a^p$

let $g \in S_X$ defined by $(g \cdot f)(i) = f(i+1)$

for $f \in X$, $i \in \mathbb{Z}/p$, g has order p,

let G = group generated by g.

If $f \in X^g$, then $f(i) = f(i+1)$ for all $i \in \mathbb{Z}/p$

i.e., f is constant $\Rightarrow |X^g| = a$

Apply Lemma. □

Thm (Wilson) $(p-1)! \equiv -1 \pmod p$

Pf. Let X = cyclic orderings of $\mathbb{Z}/p$.

= placements of elements of $\mathbb{Z}/p$ in a circle.

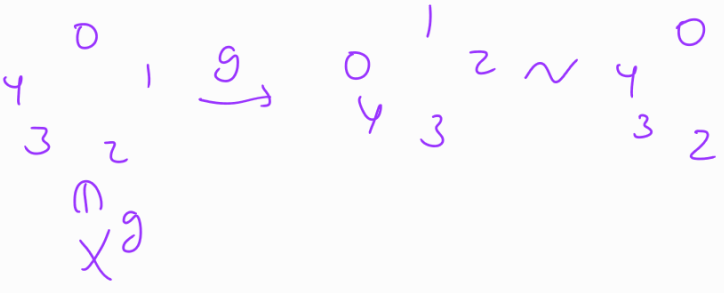
$|X| = (p-1)!$

Let $g \in S_X$ be permutation which adds 1 to each entry in a placement

Ex. $p=5$

g has order p, G = group generated by g.

Pick $x \in X^g$ **Ex.**



List elements as $a_0, a_1, \ldots a_{p-1}$ where $a_0 = 0$ going clockwise

There is unique i s.t. $a_i = 1$. $(1 \le i \le p-1)$

Apply g gives $a_0+1, a_1+1, \ldots a_{p-1}+1$

$\parallel$

a_i

since this is fixed, rotating i places gives original sequence.

$\Rightarrow a_{2i} = a_i + 1 = 2$, $a_{3i} = a_{2i} + 1 = 3$, ...

$a_{ki} = k$ for $k = 1, \dots p-1$.

Note: $\{i, 2i, 3i, \dots (p-1)i\}$ are all distinct in $\mathbb{Z}/p$.

(so for any i, can get element of X^g by setting $a_{ki} = k$ for $k = 1, \dots p-1$)

$\Rightarrow |X^g| = p-1$ (choice of distance between 0 and 1 going clockwise)

$\Rightarrow (p-1)! \equiv p-1 \pmod p \equiv -1 \pmod p$. □

Lemma. $n \geq p$. Then

$$\binom{n}{k} \equiv \binom{n-p}{k-p} + \binom{n-p}{k} \pmod p.$$

Pf. $X =$ k-element subsets of $[n]$.

let $\sigma = (1\ 2 \cdots p)$ (cycle notation)

Define $g \in \mathfrak{S}_X$ by $g \cdot \{s_1, \dots s_k\} = \{\sigma(s_1), \dots \sigma(s_k)\}$

Suppose $S \in X^g$. Two cases:

Type I: $S \cap [p] = \emptyset$. σ does nothing to elements of S, so $S \in X^g \Rightarrow \binom{n-p}{k}$ many.

Type II. S contains some number between 1 and p.

Suppose $i \in S$, $1 \leq i \leq p$ since $g \cdot S = S$, $\sigma(i) \in S$

Also, $\sigma^2(i) \in S$ and in fact $\sigma^k(i) \in S$ for all k.

$\Rightarrow [p] \subseteq S \Rightarrow \binom{n-p}{k-p}$ many of them.

Apply lemma. □