Last time:

Legendre Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{otherwise} \end{cases}$$

From Euler's criterion

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

We also saw

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

Aside observe that if

$x^2 \equiv a \pmod p$ has a solution

then a cannot be a primitive root modulo p.

Permutations

Bijections from $\{1, \ldots, n\}$ to itself

→ Set of all permutations is denoted by S_n

→ You can compose two permutations

→ (Not needed for this course!) but good to know that S_n is a group with respect to composition.

Let's discuss some examples and do some computations.

Q1: What are all the permutations of $\{1, 2, 3\}$?

Q2: Write down each one of them in cycle notation.

Q3: Compute composition of

(1234) and (1324), i.e

$$(1234)(1324).$$

Transpositions

A cycle of length 2 is called a transposition ie it is a bijection from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$ such that it fixes $n-2$ elements and interchanges remaining 2.

Example: $f: \{1,2,3,4,5\} \longrightarrow \{1,2,3,4,5\}$

$f(1)=2$ $\quad f(3)=3$ $\quad f(5)=5$

$f(2)=1$ $\quad f(4)=4$

in cycle notation $f = (1\,2)$

In general, a transposition looks like $(i\,j)$.

Thm: Every permutation can be written down as product of transpositions, and number of transpositions needed only depend on that permutation.

Example: $(12345) = (15)(14)(13)(12)$

In general $(c_1 c_2 \cdots c_\ell) = (c_1 c_\ell)(c_1 c_{\ell-1}) \cdots (c_1 c_2)$

To finish the proof, we just observe that any permutation is just product of cycles.

Signature of permutation $= (-1)^m$

m is the minimum no. of transpositions needed to write it down

(You can denote it by $\mathrm{sgn}(\sigma)$)

<u>Defn:</u> σ is called <u>even</u> if $\mathrm{sgn}(\sigma) = 1$

σ is called <u>odd</u> if $\mathrm{sgn}(\sigma) = -1$

S_3	σ	sgn
	id	
	(123)	
	(132)	
	(12)	
	(13)	
	(12)	

How does signature behave under compositions?

$$\operatorname{sgn}(\sigma\tau) \qquad \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$$

$$\operatorname{sgn}(\tau\sigma)$$

How are these 3 quantities related to each other?

Let's go back to working modulo p.

Fix $a \not\equiv 0 \pmod p$.

Multiplication by a gives a permutation of $\{1, 2, \ldots, p-1\}$, say σ_a

(Zolotarev's lemma) $\left(\frac{a}{p}\right) = \operatorname{sgn}(\sigma_a)$

<u>Example:</u> $a = 2$ $p = 7$

$$\sigma_a \quad \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{matrix}$$

In cycle notation $\sigma_a = (1\,2\,4)(3\,6\,5)$

$$\operatorname{sgn}(\sigma_a) = \operatorname{sgn}((1\,2\,4))\operatorname{sgn}((3\,6\,5))$$
$$= 1$$

Want to show $\left(\frac{a}{p}\right) = \operatorname{sgn}(\sigma_a)$

Pf: Suppose multiplication by a gives a cycle of length l and there are c cycles so

$$l \cdot c = p-1$$

$$\operatorname{sgn}(\sigma_a) = \left((-1)^{l-1}\right)^{c}$$

$$\operatorname{sgn}(\sigma_a) = \left((-1)^{l-1}\right)^{c}$$

c even then $\operatorname{sgn}(\sigma_a) = 1$

$$\left(\frac{a}{p}\right) = (a)^{(p-1)/2} = (a)^{l\,c/2}$$

$$= 1$$

c odd $lc = p-1 \Rightarrow l$ is even

$$\operatorname{sgn}(\sigma_a) = -1$$

Consider $a^{l/2} \pmod p$

$$\left(a^{l/2}\right)^2 \equiv 1 \quad \& \quad (a)^{l/2} \not\equiv 1 \pmod p$$

$$\Rightarrow (a)^{l/2} \equiv -1 \pmod p$$

$$\left(\frac{a}{p}\right) \equiv (a)^{(p-1)/2} \equiv \left((a)^{l/2}\right)^c$$

$$\equiv (-1)^c \equiv -1 \pmod p$$

We are heading towards <u>quadratic reciprocity</u>.

$p \neq q$ $\quad$ p, q odd primes

$$\boxed{\left(\frac{p}{q}\right) \text{ is connected to } \left(\frac{q}{p}\right)}$$