Last time: Fermat's two-square thm

Let p be a prime.

$p = x^2 + y^2 \iff p = 2$ or

$p \equiv 1 \pmod 4$

This proves following.

p splits in $\mathbb{Z}[i] \iff p \equiv 1 \pmod 4$

p is inert in $\mathbb{Z}[i] \iff p \equiv 3 \pmod 4$

LEGENDRE SYMBOL

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod p \\ 1 & a \text{ is Square mod } p \\ -1 & a \text{ is non square mod } p \end{cases}$$

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

We saw last time

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

We can construct square root of -1 also, in case it exists!

Let us discuss $\left(\frac{2}{p}\right)$

$$H = 1 \times 2 \times 3 \times 4 \times \cdots \times \frac{p-3}{2} \times \frac{p-1}{2}$$

$$E = 2 \times 4 \times 6 \times \cdots \times (p-3) \times p-1$$

$$O = 1 \times 3 \times 5 \times \cdots \times (p-4) \times (p-2)$$

$$2^{\frac{p-1}{2}} H = 2 \times 4 \times 6 \times 8 \times \cdots \times p-3 \times p-1$$

$$= E$$

$$\left(\frac{2}{p}\right) \cdot H \equiv (2)^{\frac{p-1}{2}} H = \varepsilon \pmod p$$

$$(-1)^{\frac{p-1}{2}} \cdot O = -1 \times (-3) \times (-5) \times \cdots \times -(p-4) \times -(p-2)$$

$$\equiv (p-1) \times (p-3) \times (p-5) \times \cdots \times 4 \times 2$$

$$\equiv \varepsilon \pmod p$$

In $H = 1 \times 2 \times 3 \times 4 \times \cdots \times \frac{p-1}{2}$

multiply even terms with -1 to get

$$(-1)^{\left[\frac{p-1}{4}\right]} \cdot H = O$$

$$2^{(p-1)/2} H = \varepsilon \pmod{p} \quad \text{— (1)}$$

$$(-1)^{(p-1)/2} \cdot 0 = \varepsilon \quad \text{— (2)}$$

$$(-1)^{\left[\frac{p-1}{4}\right]} \cdot H = 0 \quad \text{— (3)}$$

$$(2)^{p/2} H = (-1)^{p-1/2} \cdot 0$$

$$= (-1)^{p/2} (-1)^{\left[\frac{p-1}{4}\right]} H$$

$$(2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (-1)^{\left[\frac{p-1}{4}\right]} \pmod{p}$$

p	$\frac{p-1}{2}$	$\left[\frac{p-1}{4}\right]$	$\left(\frac{2}{p}\right)$
$8k+1$	even	even	1
$8k+3$	odd	even	-1
$8k+5$	even	odd	-1
$8k+7$	odd	odd	1

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

Legendre Symbol is Connected with multiplication dynamics mod p which is Connected with permutations.

Permutations are basically bijections.

Example: $\{1,2,3\} \longrightarrow \{1,2,3\}$

$1 \longmapsto 2$

$2 \longmapsto 3$

$3 \longmapsto 1$

is an example.

$p = 7$

$3 \xrightarrow{3} 2 \xrightarrow{3} 6 \xrightarrow{3} 4 \xrightarrow{3} 5 \xrightarrow{3} 1$

1	2	3	4	5	6
3	2	6	4	5	1

Think of them as reordering.

1	2	3
↓	↓	↓
2	3	1

Cycle notation

$(1\ 2\ 3)$

What is the cycle notation for the following permutation?

1	2	3
↓	↓	↓
3	1	2

$(1\ 3\ 2)$

Composition

$(1234)(2341) = (13)(24)$

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

$f(1)=2 \quad f(2)=3 \quad f(3)=4 \quad f(4)=2$

$g: \{1,2,3,4\} \longrightarrow \{1,2,3,4\}$

$g(2)=3 \quad g(3)=4 \quad g(4)=1$

$g(1)=2$

[Aside: Group Theory]

Fix a set $S = \{1, 2, \ldots, n\}$.

Let S_n be set of all <u>permutations</u> of S. Then

i) You can compose any two permutations to get another permutation.

ii) $f \circ (g \circ h) = (f \circ g) \circ h$

iii) There is an identity permutation id

Such that $f \circ id = id \circ f = f$

iv) For any permutation f, there is another permutation f^{-1} such that

$$f \circ f^{-1} = id = f^{-1} \circ f.$$

$S = \{1, 2, 3\}$

$S_3 = \{ Id, (123), (132), \}$

e

$(1)(2)(3)$

$(1\ 2\ 3)$

$1 \mapsto 2$

$2 \mapsto 3$

$3 \mapsto 1$

$(1)(2)(3)$

$(1\ 3\ 2)$

$1 \mapsto 3$

$3 \mapsto 2$

$2 \mapsto 1$

$\{1,2,3\} \longrightarrow \{1,2,3\}$

(1)

$1 \longmapsto 1$

$2 \longmapsto 2$

$3 \longmapsto 3$

(2)

$1 \longmapsto 1$

$2 \longmapsto 3$

$3 \longmapsto 2$

$3 \times 2 \times 1 = 3! = 6$

$|S_n| = n!$

A cycle of length 2 is called a transposition.

For eg: (12)

Thm: S_n is generated by transpositions.

It means that any permutation can be written as composition of transpositions.

Eg: $S_3 = \{ id, (123), (132), (12), (23), (13) \}$

$id = (12)(12)$

$(123) = (13)(12)$

$(132) = (12)(13)$

Let σ be a permutation & σ = Composition of r transpositions

Signature of σ ; $\boxed{sgn(\sigma) = (-1)^r}$

If $sgn(\sigma) = 1$, we say σ is even permutation.

If $sgn(\sigma) = -1$, we say σ is odd permutation.

S_3	even	odd
	id	(12)
	(123)	(13)
	(132)	(23)