$\mathbb{F}_q$ finite field with $q = p^t$ elements

$\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ multiplicative group

<u>Theorem</u>

$\mathbb{F}_q^\times$ is cyclic.

Particular case of

<u>Theorem</u>

K field

Let G finite subgroup of $K^\times$

$\rightsquigarrow$ G cyclic.

Pf.

$|G| = n$

Let $e = \exp(G)$ = smallest $m > 0$ s.t.

$x^m = 1$ for every $x \in G$

$\exp(G) \leq |G| = n$

We have $x^e = 1 \quad \forall x \in G$

$\downarrow$

at most e solutions because K is a field

$\Rightarrow e = n$

G finite abelian $\Rightarrow \exists\, x_0 \in G$ s.t

$\operatorname{ord}(x_0) = e = n$

$\Rightarrow G = \{1, x_0, x_0^2, \dots, x_0^{n-1}\} = \langle x_0 \rangle$. $\blacksquare$

Exercise

Show that $\overline{x+1}$ is a generator in

$$\mathbb{F}_{27} = \frac{\mathbb{F}_3[x]}{x^3+x^2+x+2} \qquad |\mathbb{F}_{27}| = 27$$

$$|\mathbb{F}_{27}^{\times}| = 26 = 13 \times 2$$

so it suffices to show that

$$(x+1)^2 \neq 1 \qquad (x+1)^{13} \neq 1 \qquad \text{in } \mathbb{F}_{27}.$$

Fact $\mathbb{F}_q^{\times}$ cyclic. $\Rightarrow \exists\, \theta : \mathbb{F}_q^{\times} \longrightarrow \mathbb{Z}/_{q-1}$

$\quad = \langle g \rangle \qquad\qquad g \longmapsto 1$

$\rightsquigarrow$ $\mathbb{F}_q^{\times}$ contains exactly $\varphi(q-1)$ generators.

Consider the equation

$$x^2 = a \qquad a \in \mathbb{F}_q$$

if $x_0 \in \mathbb{F}_q$ is a solution a is called a square in $\mathbb{F}_q$.

Example

squares in $\mathbb{F}_7 = \{0, 1, 2, 4\}$

x	0,	1,	2,	3,	4,	5,	6
	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
x^2	0	1	4	2	2	4	1

Notice that $x^2 = (-x)^2$ in $\mathbb{F}_q$

In general squares in $\mathbb{F}_q^\times$ are $\frac{q-1}{2}$

Consider the case $q = p$

If $a \in \mathbb{Z}$ is a square in $\mathbb{F}_p$ then we say that it is a quadratic residue mod p

otherwise " non residue " .

Legendre symbol. $a \in \mathbb{Z}$, p prime

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ quadratic res. mod } p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ " non res mod } p. \end{cases}$$

Prop. for odd p $\in \mathbb{Z}$.

$$\boxed{\left(\frac{a}{p}\right) = (a)^{\frac{p-1}{2}} \mod p}$$

Proof. if $p \mid a$ then $\left(\frac{a}{p}\right) = 0 = (a)^{\frac{p-1}{2}} \mod p$

if $p \nmid a$

Let g be a generator of $\mathbb{F}_p^\times$

$\leadsto a = g^h$ in $\mathbb{F}_p^\times$

$\left(\frac{a}{p}\right) = 1 \iff h$ is even

if $\left(\frac{a}{p}\right) = 1$ $\quad a = g^{2k} \implies a^{\frac{p-1}{2}} = g^{\cancel{2}k\frac{p-1}{\cancel{2}}} = (\underbrace{g^{p-1}}_{=1})^k$

if $\left(\frac{a}{p}\right) = -1$ $a = g^{2k+1} \Rightarrow a^{\frac{p-1}{2}} = g^{(2k+1)\left(\frac{p-1}{2}\right)}$

$$= \underbrace{g^{k(p-1)}}_{=1} \cdot \underbrace{g^{\frac{p-1}{2}}}_{x} =$$

we have $x^2 = 1 \Rightarrow x = \pm 1$.
but $x \neq 1$ because g generator
$\Rightarrow x = -1$. $\square$

Properties of legendre symbol

a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

b) $\left(\frac{a^2}{p}\right) = 1$

c) $\left(\frac{1}{p}\right) = 1$

d) $\left(\frac{-1}{p}\right) \overset{p \text{ odd.}}{=} (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$

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

Quadratic reciprocity law

For p, q odd primes

$$\boxed{\left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \left(\frac{q}{p}\right)}$$

Example

Compute $\left(\frac{7411}{9283}\right)$ prime, prime

$7411 \equiv 9283 \equiv 3 \mod 4$

$$\left(\frac{7411}{9283}\right) = (-1)\left(\frac{9283}{7411}\right)$$

reduce $9283 \mod 7411$

$9283 \equiv 1872$

$$= -\left(\frac{1872}{7411}\right)$$

$1872 = 2^4 \cdot 3^2 \cdot 13$

$$= -\left(\frac{2^4}{7411}\right)\left(\frac{3^2}{7411}\right)\left(\frac{13}{7411}\right) = -\left(\frac{13}{7411}\right)$$

squares

$13 \equiv 1 \mod 4$

$$= -(-1)^{\frac{13-1}{2}\cdots}\left(\frac{7411}{13}\right) = -\left(\frac{7411}{13}\right)$$

reduce $7411 \equiv 1 \mod 13$ $\rightsquigarrow -\left(\frac{1}{13}\right) = -1$

Application to Fermat primes

Fermat numbers

$F_n : 2^{2^n} + 1$

Fermat prime $\rightsquigarrow$ F. number which is a prime

Ex

3, 5, 17, 257, 65537

No other Fermat prime is known.

Assume that $F_n = p$ Fermat prime.

$$\bmod p \qquad F_n = 2^{2^n} + 1$$

$$\hookrightarrow \quad 2^{2^n} + 1 \equiv 0 \mod p$$

$$2^{2^n} \equiv -1 \mod p$$

$$2^{2^{n+1}} \equiv 1 \mod p$$

$$\Rightarrow \operatorname{ord}(2) \leq \underbrace{2^{n+1}}_{\substack{\wedge\\ p-1 = 2^{2^n}}} \text{ in } \mathbb{F}_q^\times$$

$\rightsquigarrow$ 2 is not a primitive root mod p

$F_n \equiv 1 \mod 4$ and $F_n \equiv 2 \mod 3$

$(2^{2^n} \equiv 1 \mod 3)$

so $\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{-1}{3}\right) = -1$

$\rightsquigarrow 3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$

that is

$3^{\frac{\varphi(F_n)}{2}} \equiv -1 \mod F_n$

$\varphi(F_n) = 2^{2^n}$

If $\operatorname{ord}(3)$ in $\mathbb{F}_p^\times$ were a proper divisor of $\varphi(F_n) = 2^{2^n}$ then it would also divide $\frac{\varphi(n)}{2}$. $\rightsquigarrow 3^{\frac{\varphi(n)}{2}} = 1$ contradiction.

- 2 not primitive root mod F_n
- 3 primitive root mod F_n. $\blacksquare$