Prop p prime. $a \in \mathbb{Z}/p\mathbb{Z}$ nonzero then $\exists$ unique $b \in \mathbb{Z}/p\mathbb{Z}$ s.t.

$ab \equiv 1 \bmod p$

Call $b = a^{-1}$

Proof $\gcd(a,p) = 1$ $\emptyset$

Consequence

$(\mathbb{Z}/p\mathbb{Z})^*$

$= \{a \in \mathbb{Z}/p\mathbb{Z} \mid \gcd(a,p) = 1\}$

$= \{1, 2, 3, \dots, p-1\}$

$= \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$

minus

Corollary p prime.

$\phi(p) = \#(\mathbb{Z}/p\mathbb{Z})^*$

$= p-1$

Exercise

Notice

$\mathbb{Z}/p\mathbb{Z}$ set with $+, -, \times, \div$ (except 0)

Example a field

Defn A field is a set $\mathbb{F}$ w/ $+, -, \times, \div$ (except by 0.)

Example

$\mathbb{Q}$ - rational numbers (fraction)

$\mathbb{R}$ - real #s.

$\mathbb{C}$ - complex #s.

Defn The finite field w/ p elements is $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z})$ for p prime.

Fact $\mathbb{F}$ a field

$|\mathbb{F}| = \#\mathbb{F} = p$

$\Longrightarrow \mathbb{F} \simeq \mathbb{F}_p$

Remark If $q = p^n$ then there is a unique field w/ q elts: $\mathbb{F}_q$.

Study exponentiation in $\mathbb{F}_p^*$ from a math standpoint.

Example

$\mathbb{F}_7^* = \mathbb{F}_7 \setminus \{0\}$

$= \{1, 2, 3, 4, 5, 6\}$

---

a	a^2	a^3	a^4	a^5	a^6	…
1	1	1	1	1	1	
2	4	1	2	4	1	
3	2	6	4	5	1	
4	2	1	4	2	1	
5	4	6	2	3	1	
6	1	6	1	6	1	

1) Column 2

2) Column 3

$x^3 \equiv 2 \bmod 7$ for x

no solution

$\sqrt[3]{2} \notin \mathbb{F}_7$

$x^3 \equiv 6 \bmod 7$

3 solutions

$3, 5, 6 \in \mathbb{F}_7$

3) Column 6 says

$a \in \mathbb{F}_7^*$

$a^6 \equiv 1 \bmod 7$

$a \in \mathbb{Z}$

$$a^6 \equiv \begin{cases} 0 & \bmod 7 \text{ if } 7 \mid a \\ 1 & \bmod 7 \text{ if } 7 \nmid a \end{cases}$$

$p = 5$

$2^4 = 16 \equiv 1 \bmod 5$

$3^4 = 81 \equiv 1 \bmod 5$

Notice following pattern

p prime. $a \in \mathbb{F}_p^*$

$a^{p-1} \equiv 1 \bmod p$

Theorem (Fermat's Little Theorem)

p prime. $a \in \mathbb{Z}$.

$$a^{p-1} \equiv \begin{cases} 0 \bmod p & p \mid a \\ 1 \bmod p & p \nmid a \end{cases}$$

Pf/ Direct Proof

$p \mid a \Rightarrow p \mid a^p$

$\Longrightarrow a^p \equiv 0 \bmod p.$

Else $p \nmid a \leftarrow$

So $a \in \mathbb{F}_p^*$

List $a, 2a, 3a, \dots, (p-1)a \pmod p$

Claim These are all different.

Pf/ Assume $ja = ka \bmod p$

$p \mid (ja - ka) = (j-k)a$

$\Longrightarrow p \mid j-k$ or $\cancel{p \mid a}$

$1 \le j, k \le p-1$

$-(p-2) \le j-k \le p-2$

$-p \quad -(p-2) \quad 0 \quad p-2 \quad p$

$j-k = 0$ or $j = k$ $\emptyset$

$\{a, 2a, \dots, (p-1)a\} \subseteq \mathbb{F}_p^*$

$p-1$ elts $\qquad$ $p-1$ elts

So

$\{a, 2a, 3a, \dots (p-1)a\}$

$\| $

$\{1, 2, 3, \dots, p-1\} = \mathbb{F}_p^*$

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

$\cancel{(p-1)}!\, a^{p-1} \equiv \cancel{(p-1)}! \bmod p$

$(p-1)! \neq 0$ why

$p \mid (p-1)(p-2)\cdots 2 \cdot 1$

$\Longrightarrow p \mid i \quad i = 1, \dots, p-1$

not true

so can divide by $(p-1)!$

so $a^{p-1} \equiv 1 \bmod p$

$\emptyset$

Remark:

Lagrange: G a group. $|G| = \#G = n$ $g \in G$

$g^n = 1_G$

Proof of FLT

$\mathbb{F}_p^*$ a gp under $\times$

$|\mathbb{F}_p^*| = p-1$ so $a \in \mathbb{F}_p^*$

$a^{p-1} = 1$

Ex 20202019 prime.

$2^{20202018} \equiv 1 \bmod 20202019$

Corollary $a \in \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$

$a^{-1} \equiv a^{p-2} \bmod p$

Pf/ $a \cdot a^{p-2} = a^{p-1}$

$\equiv 1 \bmod p$ $\emptyset$

Notice

Find Inverse of a in $\mathbb{F}_p^*$

1) Extended Euc Alg

u, v s.t.

$au + pv = 1$

So $a^{-1} = u$

2) Fast Power

$a^{-1} \equiv a^{p-2} \bmod p$

Both $\approx \log_2 p$

Ex $p = 17449$

$a = 7814$

find a^{-1} in $\mathbb{F}_p^*$

Ex/ $m = 15485207$

$2^{m-1} \not\equiv 1 \bmod m$

m not prime

$a \in \mathbb{F}_p^*$ FLT $a^{p-1} \equiv 1 \bmod p$

but doesn't say that's smallest power of $a \equiv 1$.

E.g/ in $\mathbb{F}_7$ $2^3 \equiv 1$, $6^2 \equiv 1$ mod 7

Defn $a \in \mathbb{F}_p^*$ The order of a mod p is the min $k > 0$ s.t. $a^k \equiv 1 \bmod p$

Ex/ Order 2 is 3; order 6 is 2. Both divide 6

Prop $a \in \mathbb{F}_p^*$. $a^n \equiv 1 \bmod p$

k: order a.

$\Longrightarrow k \mid n.$ $(k \mid p-1)$

pf/ $n = 0$, k done.

assume $n > k$

long divide $n = kq + r$ $\quad 0 \le r < k$

$1 \equiv a^n = a^{kq+r}$

$= (a^k)^q \cdot a^r$

$\equiv a^r \bmod p$

minimality of k

$\Longrightarrow r = 0$ $\emptyset$

Ex/ $3 \in \mathbb{F}_7$

order $= 6$

powers of 3

$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$

$= \{3, 2, 6, 4, 5, 1\} = \mathbb{F}_7^*$

Prop $a \in \mathbb{F}_p^*$

order $a = p-1$

$\Longrightarrow \#\{a, a^2, \dots, a^{p-1}\} \subseteq \mathbb{F}_p^*$ #

pf/ suffices to show all elts left are distinct.

$a^n = a^m \bmod p \quad (n \ge m)$

$a^{n-m} \equiv 1 \bmod p$

$0 \le n-m < p-1$

minimality of $p-1$

$n-m = 0$ so $n = m$ $\emptyset$

Slogan an element of order $p-1$ in $\mathbb{F}_p^*$ generates $\mathbb{F}_p^*$

i.e. every elt of $\mathbb{F}_p^*$ is a power of A.

Defn If $g \in \mathbb{F}_p^*$ & $\{g, g^2, \dots, g^{p-1}\} = \mathbb{F}_p^*$

$\Longrightarrow g$ is a primitive root mod p.

Prop g primitive root mod p $\Longleftrightarrow$ order $g = p-1$.

Remarks

1) Not 100% obvious that a primitive root exists.

2) $\mathbb{F}_p^*$ has a primitive root $\Longleftrightarrow$ it is cyclic.

Theorem (Primitive root theorem)

$\mathbb{F}_p^*$ has a primitive root.

$\exists\, g \in \mathbb{F}_p^*$ s.t. $\forall a \in \mathbb{F}_p^*$ $a = g^k$ some k

Rmk

* Are $\phi(p-1)$ primitive roots

* If $k \mid p-1$ are $\phi(k)$ elts of order k.

Examples Powers of 2 in $\mathbb{F}_{11}$

$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$

$\Longrightarrow 2$ prim root.

* powers of 2 in $\mathbb{F}_{17}$

$2, 4, 8, 16, 15, 13, 9, 1$

8 of these.

3 not 2^k any k.

CK

3 is a prim root in $\mathbb{F}_{17}$

---

① Finding a primitive root in general is hard.