

Prop p prime. $a \in \mathbb{Z}/p\mathbb{Z}$ nonzero then \exists unique $b \in \mathbb{Z}/p\mathbb{Z}$ s.t. $ab \equiv 1 \pmod p$
 Call $b = a^{-1}$
 Proof $\gcd(a, p) = 1$

Consequence $(\mathbb{Z}/p\mathbb{Z})^*$
 $= \{a \in \mathbb{Z}/p\mathbb{Z} \mid \gcd(a, p) = 1\}$
 $= \{1, 2, 3, \dots, p-1\}$
 $= \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$

Corollary p prime.
 $\phi(p) = \#(\mathbb{Z}/p\mathbb{Z})^* = p-1$

Exercise

Notice $\mathbb{Z}/p\mathbb{Z}$ set with $+, -, \times, \div$
 Lexic O

Example a field
 Defn A field is a set F w/ $+, -, \times, \div$ except by 0.

Example \mathbb{Q} - rational numbers (fraction)
 \mathbb{R} - real #s.
 \mathbb{C} - complex #s.

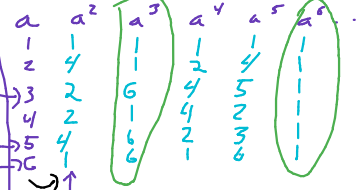
Defn The finite field w/ p elements is $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z})^*$ for p prime.

Fact \mathbb{F} a field $|\mathbb{F}| = \#\mathbb{F} = p \Rightarrow \mathbb{F} \cong \mathbb{F}_p$

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

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

Example $\mathbb{F}_7^* = \mathbb{F}_7 \setminus \{0\} = \{1, 2, 3, 4, 5, 6\}$



1) Column 2
 2) Column 3 $x^3 \equiv 2 \pmod 7$ s.t. x no solution $\sqrt[3]{2} \notin \mathbb{F}_7$
 $x^3 \equiv 6 \pmod 7$ 3 solutions 3, 5, 6 $\in \mathbb{F}_7$

3) Column 6 says $a \in \mathbb{F}_7^*$ $a^6 \equiv 1 \pmod 7$
 $a \in \mathbb{Z}$
 $a^6 \equiv \begin{cases} 0 \pmod 7 & \text{if } 7|a \\ 1 \pmod 7 & \text{if } 7 \nmid a \end{cases}$

$p=5$
 $2^4 = 16 \equiv 1 \pmod 5$
 $3^4 = 81 \equiv 1 \pmod 5$

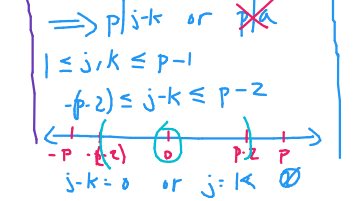
Notice following pattern
 p prime. $a \in \mathbb{F}_p^*$
 $a^{p-1} \equiv 1 \pmod p$

Theorem (Fermat's Little Theorem)
 p prime. $a \in \mathbb{Z}$.
 $a^{p-1} \equiv \begin{cases} 0 \pmod p & \text{if } p|a \\ 1 \pmod p & \text{if } p \nmid a \end{cases}$

Proof Direct Proof
 $p|a \Rightarrow p|a^p \Rightarrow a^p \equiv 0 \pmod p$
 Else $p \nmid a$
 So $a \in \mathbb{F}_p^*$

List $\{a, 2a, 3a, \dots, (p-1)a\} \pmod p$
 Claim These are all different.
 Assume $ja = ka \pmod p$
 $p|(ja-ka) = (j-k)a$
 $\Rightarrow p|j-k$ or $p|a$
 $1 \leq j, k \leq p-1$
 $-(p-2) \leq j-k \leq p-2$

Proof of FLT
 \mathbb{F}_p^* a gp under \times
 $|\mathbb{F}_p^*| = p-1$ so $a \in \mathbb{F}_p^*$
 $a^{p-1} = 1$



s.t. $2a, 3a, \dots, (p-1)a \in \mathbb{F}_p^*$
 $\{1, 2, 3, \dots, p-1\} = \mathbb{F}_p^*$

$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod p$
 $(p-1)! a^{p-1} \equiv (p-1)! \pmod p$
 $(p-1)! \neq 0$ why $p \nmid (p-1)(p-2)\dots 2 \cdot 1$
 $\Rightarrow p \nmid i$ $i=1, \dots, p-1$ not true
 so can divide by $(p-1)!$
 so $a^{p-1} \equiv 1 \pmod p$

Remark: Lagrange: G a group. $|G| = \#G = n$ $g \in G$
 $g^n = 1a$
 Proof of FLT

Ex 20202019 prime.
 $2^{20202018} \equiv 1 \pmod{20202019}$
 Corollary $a \in \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$
 $a^{-1} \equiv a^{p-2} \pmod p$
 Pf/ $a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod p$

Notice Find Inverse of a in \mathbb{F}_p^*
 1) Extended Euc Alg
 u, v s.t. $au + pv = 1$
 so $u^{-1} = u$
 2) Fast Power
 $a^{-1} \equiv a^{p-2} \pmod p$

Both $\approx \log_2 p$
 Ex $p = 17449$
 $a = 7814$
 Find a^{-1} in \mathbb{F}_p^*
 Ex/ $m = 15485267$
 $2^{m-1} \not\equiv 1 \pmod m$
 m not prime

$a \in \mathbb{F}_p^*$ FLT $a^{p-1} \equiv 1 \pmod p$
 but doesn't say that's smallest power of $a \equiv 1$.
 E.g. in \mathbb{F}_7 $a^3 \equiv 1 \pmod 7$
 $6^2 \equiv 1 \pmod 7$

Defn $a \in \mathbb{F}_p^*$ The order of $a \pmod p$ is the min $k > 0$ s.t. $a^k \equiv 1 \pmod p$
 Ex/ Order 2 is 3
 order 6 is 2

Prop $a \in \mathbb{F}_p^*$ $a^n \equiv 1 \pmod p$
 k : order a .
 $\Rightarrow k | n$. ($k | p-1$)
 Pf/ $n = 0, k$ done. assume $n > k$
 long divide $n = kg + r$ $0 \leq r < k$
 $1 \equiv a^n = a^{kg+r} = (a^k)^g \cdot a^r \equiv a^r \pmod p$
 minimality of $k \Rightarrow r=0$

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 $a = p-1$
 $\Rightarrow \{a, a^2, \dots, a^{p-1}\} = \mathbb{F}_p^*$
 Pf/ so if: as to show all elts left are distinct.
 $a^n = a^m \pmod p$ ($n \equiv m$)
 $a^{n-m} \equiv 1 \pmod p$
 $\leq n-m < p-1$
 minimality of $p-1$ $n-m=0$ so $n=m$
 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 Is $g \in \mathbb{F}_p^*$ & $\{g, g^2, \dots, g^{p-1}\} = \mathbb{F}_p^*$
 $\Rightarrow g$ is a primitive root mod p .
 Prop g primitive root mod $p \iff$ order $g = p-1$.

Remarks
 1) Not 100% obvious that a primitive root exists.
 2) \mathbb{F}_p^* has a primitive root \iff it is cyclic.

Theorem (Primitive root theorem)
 \mathbb{F}_p^* has a primitive root.
 $\uparrow \exists g \in \mathbb{F}_p^*$ s.t. $\forall a \in \mathbb{F}_p^*$ $a = g^k$ some k

Rmk
 * Are $\phi(p-1)$ primitive roots
 * If $k | p-1$ are $\phi(k)$ elts of order k .

Examples Powers of 2 in \mathbb{F}_{11}
 $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$
 $\Rightarrow 2$ prim root.
 * Powers of 2 in \mathbb{F}_{13}
 $2, 4, 8, 16, 15, 13, 9, 1$
 8 of these.
 3 not 2^k any k .
 (OK) 3 is a prim root in \mathbb{F}_{13}

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

Example a field

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

Example $\mathbb{F}_7^* = \mathbb{F}_7 \setminus \{0\} = \{1, 2, 3, 4, 5, 6\}$

Notice following pattern

Theorem (Fermat's Little Theorem)

Proof Direct Proof

Proof of FLT

Ex 20202019 prime.

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

Both $\approx \log_2 p$

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

Remarks