II Finite field $\mathbb{F}_p$.

§1 Arimetic of integers.

(1) Divisibity in $\mathbb{Z}$.

$ax = b$ in $\mathbb{Z}$.

Def: "$a \mid b$". Let $a, b \in \mathbb{Z}$. We say a divides b & denote it by $a \mid b$ if there exists an integer $c \in \mathbb{Z}$ s.t. $b = a \cdot c$.

Rmk: By definition, to decide whether two integers have the divisibility relation, one need to solve the equation.

Define a partial order on $\mathbb{N}\setminus\{0\}$

(1) $\forall\, a \in \mathbb{N}\setminus\{0\}$, we have $a \mid a$ (since $a \cdot 1 = a$)

(2) If $a, b \in \mathbb{N}_{>0}$ & $a \mid b$, $b \mid a$, then we have $a = b$

(3) If $a, b, c \in \mathbb{N}_{>0}$ & $a \mid b$, $b \mid c$, then $a \mid c$

If a doesn't divide b (i.e. $ax = b$ has no solution in $\mathbb{Z}$), then we denote it by $a \nmid b$.

In general, in $\mathbb{Z}$, it's not always possible to do division.

But, we have the following Euclidean division:

Thm (Euclidean division).

Let $a \in \mathbb{Z}$, $b \in \mathbb{N}_{>0}$. Then there exists a unique pair $(q, r) \in \mathbb{Z} \times \mathbb{N}$ s.t. $a = bq + r$, with $0 \leq r < b$

We call r is the residue of ~~a mod b~~ Euclidean division of a by b. & q is the quotient of

Pf: Existence: (1) If $b \mid a$, then $a = b \cdot q$ ($\exists q \in \mathbb{Z}$ s.t.), take $r = 0$

(2) If $b \nmid a$, Consider the set.

$$S = \{ a - bk : k \in \mathbb{Z} \} \cap \mathbb{N}$$

Since $\mathbb{N}$ is well-ordering, we take the minimal element r of $S \Rightarrow r = a - bq \Rightarrow 0 \le r < b$

($\exists q \in \mathbb{Z}$ s.t.)

Uniqueness: Suppose (q', r') is another pair satisfying the properties.

$$a = bq + r = bq' + r' \quad \text{Assume } r' \le r$$

$$\Rightarrow b \cdot (q - q') = r - r'$$

$$\Rightarrow |b| \, |q - q'| = |r - r'|, \qquad 0 \le r - r' \le r < b$$

$$\Rightarrow q - q' = 0 \quad \& \quad r - r' = 0.$$

□

$\forall n \in \mathbb{Z}_{>0}$ the notion of mod n congruence class

Def: $n\mathbb{Z} := \{ n \cdot k : k \in \mathbb{Z} \}$

For $x, y \in \mathbb{Z}$, we say x is congruent to y mod n, if $x - y \in n\mathbb{Z}$ (i.e. $x - y = n \cdot X$ has a solution in $\mathbb{Z}$)

Denote it by $x \equiv y \pmod{n}$

Claim: This is an equivalence relation.

① $\forall x \in \mathbb{Z}$, $x - x = 0 \cdot n$
$\Leftrightarrow x \equiv x \bmod n$.

② If $x \equiv y \bmod n$ $(\exists k \in \mathbb{Z}$ s.t. $x - y = kn)$
$\Rightarrow y - x = -kn$
$\Rightarrow y \equiv x \bmod n$

③ For $x, y, z \in \mathbb{Z}$
If $x \equiv y \bmod n$, $y \equiv z \bmod n$
then $x - z = x - y + y - z = k_1 n + k_2 n = (k_1 + k_2) \cdot n$
$x \equiv z \bmod n$

$(\mathbb{Z}, \equiv \bmod n)$

Then there exists a canonical quotient map.

$$\begin{array}{ccc} \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/n\mathbb{Z} \quad \left(:= \text{the quotient of } \mathbb{Z} \text{ by the mod } n \text{ equivalence relation}\right) \\ \cup & & \\ x & \longmapsto & C_x := x + n\mathbb{Z} \end{array}$$

But on $\mathbb{Z}$, we have two binary operations $+$ & $\cdot$: using $+$ $\cdot$ on $\mathbb{Z}$

We want to see if we can define two binary operations canonically on $\mathbb{Z}/n\mathbb{Z}$.

(canonically)

Such a question can be generalized to a commutative ring equipped with an equivalence relation $\sim$

i.e. if R is a commutative ring, then

equipped with $\sim$

$$R \twoheadrightarrow R/\sim$$

$$\begin{array}{ccc} R\times R & \xrightarrow{+} & R \\ \downarrow & & \downarrow \\ R/\sim \times R/\sim & & R/\sim \end{array}$$

$$((x,y)\in R/\sim \times R/\sim) \longmapsto x+y$$

$$\begin{array}{ccc} R\times R & \xrightarrow{*} & R \\ \downarrow & & \downarrow \\ R/\sim \times R/\sim & & R/\sim \end{array}$$

$(R,+)$ Commutative group

Let $(G,*)$ be a group (not necessary abelian i.e. $x*y=y*x \;\forall x,y\in G$)

equipped with an equivalence relation $\sim$ on G.

then we consider $G \twoheadrightarrow G/\sim$

Question:

$$\begin{array}{ccccc} (G_x,G_y)\subset G\times G & \xrightarrow{*} & G & \supset & G_x * G_y := \{ z_1 * z_2 \,:\, z_1\in G_x,\ z_2\in G_y\} \\ \downarrow & & \downarrow \pi & & \downarrow \\ (G_x,G_y)\in G/\sim \times G/\sim & & G/\sim \ni G_{x*y} & \in & \pi(G_x * G_y) \end{array}$$

We need $\{G_{x*y}\} = \pi(G_x * G_y)$

(*) $\{C_{x*y}\} = \pi(C_x * C_y)$ $\forall\, x, y \in G$.

Since G is a group, we have a distinguish element $e \in G$ (unit of G).

claim: $C_e \in G/\sim$

If (*) is true, then C_e is a subgroup of G s.t.

$\forall\, x \in G,\ x * C_e * x^{-1} = C_e$.

Pf: Recall for a subset X of a group G, X is a subgp iff

$\forall\, x, y \in X,\ x * y^{-1} \in X$

Take $x, y \in C_e$. ? $x * y^{-1} \in C_e$.

$$\{C_{x*y^{-1}}\} \overset{(*)}{=\!=} \pi(C_x * C_{y^{-1}})$$

$$C_x = C_y \quad =\!= \pi(C_y * C_{y^{-1}})$$

$$\overset{(*)}{=\!=} \pi(C_{y*y^{-1}}) = \{C_e\}$$

$\Rightarrow x * y^{-1} \in C_e$. $\Rightarrow$ C_e is a subgroup of G.

$\forall x \in G$.

$x * C_e \subset G$

$C_x * C_e$

$C_x \in \{C_x\}$ $\in$ $G/\sim$

$C_e * x$

$C_x \overset{?}{=} C_e * x$

$= x * C_e$

$G_x \overset{?}{=} C_e * x$

By definition, $G_x = \{ y \in G. \quad x \sim y \}$

$(*)$ is true.

But ~~this~~ implies ~~this~~ ~~equiv~~ equivalence relation is defined by the subgroup C_e.

(i.e $x \sim y$ iff $x * y^{-1} \in C_e$) $\Longrightarrow x \in C_e * y$

$\Rightarrow$ equivalence class are of the ~~right~~ form $C_e * x$, for some $x \in G$

$$x * C_e = C_x = C_e * x$$

$$\Rightarrow \quad x * C_e * x^{-1} = C_e \qquad (**)$$

Def: If a subgroup H of G satisfies the condition $(**)$.

$$\left(\text{i.e. } \forall\, g \in G,\ g * H * g^{-1} = H\right).$$

then we call H is a normal subgroup of G.

denoted by $H \triangleleft G$.

Conclusion:
$(*)$ is true $\Rightarrow$ $C_e \triangleleft G$

Conversely, if $H \lhd G$, the equivalence relation defined by H.

has a group structure

Canonical.

the quotient set of G for. (i.e. $\forall x, y \in G$

$x \sim y$ iff $x * y^{-1} \in H$

$\Downarrow$

$x \in H * y$.

$\Rightarrow$

$$\pi(G_x * G_y) = \{ G_{x*y} \} \qquad \forall x, y \in G.$$

$$\pi(Hx * Hy) \underset{H \lhd G}{=} \pi(H * x * H * x^{-1} * x * y)$$

$$= \pi(H * H * x * y) = \pi(H * x * y)$$

$$\{ G_{x*y} \}$$

As a result. $H \lhd G$, $G/\sim$ has a canonical gp. struct. $\Leftrightarrow$ $\sim$ is defined by a $H \lhd G$ | H is a group

$(R, +, *)$ $\sim$ is an equivalence relation on R

Want: a canonical ring structure on $R/\sim$

$\Updownarrow$

$\underline{(R,+)}$ has a canonical gp. structure.
$\sim$

$\Updownarrow$

$\sim$ is defined by a (normal) subgp $I = C_0$ of $(R,+)$ (since $(R,+)$ is commutative, any subgp is normal)

$\forall y \in R$.
$C_0 = I$
$y \cdot I \subseteq C_0 * C_y$
$\pi \downarrow$
$\{C_0\}$
$\Rightarrow y \cdot I \subseteq I$.

$(x, y) \in R \times R \xrightarrow{*} R \supset C_x * C_y$

$\downarrow$ $\qquad$ $\downarrow \pi$ $\qquad$ $\downarrow$

$(C_x, C_y) \in R/\sim \times R/\sim$ $\qquad$ $R/\sim \ni [C_{x*y}] = \pi(C_x * C_y)$

$\forall y \in R$

$\Rightarrow \pi(\underline{C_0 * C_y}) = \{C_{0*y}\} = \{C_0\}$

Conclusion: $((R,+,*),\sim)$. If $R/\sim$ (the quotient set) has a canonical ring structure

then $\sim$ is defined by a subgp I of $(R,+)$.

s.t. $\forall y \in R$, $\begin{cases} y \cdot I \subseteq I \\ I \cdot y \subseteq I \end{cases}$ (If R is commutative, then take one condition is enough)

I

Def: **An ideal** of a commutative ring $(R,+,*)$ is a subgp.

I of R s.t. $\forall y \in R$, $y \cdot I \subseteq I$.

Conversely, if $I \subset R$ is an ideal, then R/I is a ring.

$(\mathbb{Z}, +, \cdot)$ is a commutative ring.

integral domain

Def. Let R be a commutative ring.

(1) $0 \neq a \in R$ is called a zero divisor if $\exists\ 0 \neq b \in R$ s.t. $a * b = 0$

non-trivial.

⚠ this doesn't happen in $\mathbb{Z}$ (by Peano axioms ⇓ order on $\mathbb{N}$)

(2) If R is a commutative ring without zero-divisors, ~~call~~ Say then we R is an integral domain.

Recall: $n\cdot\mathbb{Z} = \{n\cdot k : k \in \mathbb{Z}\}$ is an equivalence relation on $\mathbb{Z}$

$\cap$ subgp.

$\mathbb{Z}$

Claim: $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$

$\forall\, m \in \mathbb{Z}.\quad m \cdot n\cdot\mathbb{Z} \subset n\cdot\mathbb{Z}$ $\vee$

$\Longrightarrow$ $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ has a canonical ring structure.

Def: Let R be a commutative ring. & $I \subset R$ is an ideal.

If $\exists\, x \in R$ s.t. $I = x\cdot R$. then we call I is a principal ideal.

Def. An integral domain R is call. principal ideal domain. (P.I.D).
if any ideal of R is principal.

Ex. $\mathbb{Z}$ is a P.I.D.

Pf. $I \subset \mathbb{Z}$ an ideal. $I \cap \mathbb{N}_{>0}$ has a minimal element a.

$(a) \subset I$. In fact. $(a) = I$.

Otherwise. if $r \in I$, $r \notin (a)$ Euclidean division of a & r.

$\Rightarrow \exists (q, a') \in \mathbb{Z} \times \mathbb{N}_{>0}$ s.t. $r = a \cdot q + r'$ $0 \le r' < a$ □

If $r' \neq 0 \Rightarrow 0 < r' < a$ X

$\Rightarrow r' = 0 \Rightarrow r \in (a)$

Greatest common divisor (gcd.)

Def. Let $a_1, \cdots a_n \in \mathbb{Z}$.

$$I = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$$

$$:= \left\{ \sum_{i=1}^{n} a_i x_i \;:\; x_i \in \mathbb{Z} \right\}$$

is the ideal generated by $a_1, \cdots, a_n$.

(1). $\exists!\ \underline{d \in \mathbb{N}}$ s.t. $I = d\mathbb{Z}$.

We call this d is the gcd of $a_1, \cdots, a_n$.

(2) If $\gcd(a_1, \cdots, a_n) = 1$, then we say $a_1, \cdots, a_n$ are coprime.

(3) If $\forall\ 1 \le i \ne j \le n$, we have $\gcd(a_i, a_j) = 1$, then we say $a_1, \cdots, a_n$ are pairwise coprime.

Note.

$$\mathbb{Z}^\times = \{\pm 1\}$$

Rmk: In general, a GCD domain is an integral domain R with the property that any two elements of R has a gcd. (i.e. $\exists!$ minimal principal ideal containing the ideal generated by the two elements)

Take $n=6$. Consider the ring $\mathbb{Z}/6\mathbb{Z} := \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{2} \neq \bar{0}$ $\quad \bar{2}\cdot\bar{3} \overset{\text{def}}{=} \overline{2\cdot 3} = \bar{6} = \bar{0}$ $\quad \bar{0}$ is the unit for $(\mathbb{Z}/6\mathbb{Z}, \cdot)$

$\bar{3} \neq \bar{0}$ $\Rightarrow \bar{2}, \bar{3}$ are non-trivial zero divisors in $\mathbb{Z}/6\mathbb{Z}$ $\quad \bar{1}$ is the unit for $\cdot$.

Thm (Bézout) Let $a_1, \dots, a_n \in \mathbb{Z}$

Then. $a_1, \dots, a_n$ are coprime iff. $\exists\, u_1, \dots, u_n \in \mathbb{Z}$

s.t. $\sum_{i=1}^{n} u_i a_i = 1$.

pf: $\Rightarrow$ By the def. of coprime., $\gcd(a_1, \dots, a_n) = 1$

$$I = (a_1, \dots, a_n) = \left(\gcd(a_1, \dots, a_n)\right) = (1)$$

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z}$$

$$\Rightarrow a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = \mathbb{Z} \ni 1 \Rightarrow 1 = \sum_{i=1}^{n} u_i a_i \text{ with } u_i \in \mathbb{Z}$$

Conversely, if $a_1, \dots, a_n$ are not coprime., then $\gcd(a_1, \dots, a_n) > 1$ Contradiction

Rmk: Bézout's thm ensures that for $a, b \in \mathbb{Z}$ coprime, there exists $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ s.t. $u \cdot a + v \cdot b = 1$.

In practice, we have the Euclidean algorithm to compute the pair (u, v).

Lemma (~~Gauss~~ Gauss). Let $a, b, c \in \mathbb{Z}$

If $a \mid b \cdot c$ & $\gcd(a, b) = 1$, then $a \mid c$.

pf.: By def. of $a \mid b \cdot c$, there exists $d \in \mathbb{Z}$ s.t. $ad = b \cdot c$.

Since $\gcd(a, b) = 1$, by Bézout's thm, $\exists\, x, y \in \mathbb{Z}$, s.t. $ax + by = 1$.

$\Rightarrow c = c \cdot 1 = c \cdot (ax + by)$

$= acx + bcy$.

$= a \cdot cx + a \cdot dy$

$= a(cx + dy)$

$\Rightarrow a \mid c$. □

Prop: ① Let $a_1, \dots, a_n \in \mathbb{Z}$, $b \in \mathbb{Z}$

If $\forall 1 \le i \le n$, $\gcd(a_i, b) = 1$, then $\gcd\left(\prod_{i=1}^{n} a_i, b\right) = 1$.

② Let $a_1, \dots, a_n$ be n coprime integers, $b \in \mathbb{Z}$.

$\gcd(a_1, \dots, a_n) = 1$.

Then TFAE: (a) $a_1 \cdots a_n \mid b$

(b) $\forall 1 \le i \le n$, $a_i \mid b$.

$\gcd\left(\prod_{i=1}^{n} a_i, b\right) = 1$

Pf: ① By Bezout, $\exists x_i, y_i \in \mathbb{Z}$ s.t. $a_i x_i + b y_i = 1$

$\Rightarrow \prod_{i=1}^{n} (a_i x_i + b y_i) = 1$ & expand the product

$\Rightarrow \exists m \in \mathbb{Z}$. $a_1 \cdots a_n x_1 \cdots x_n + m \cdot b = 1$ $\Rightarrow$ Except the term $a_1 \cdots a_n x_1 \cdots x_n$, the other terms are divided by b

(2) Assume (a). (i.e. $\prod_{i=1}^{n} a_i \mid b$)

Then $\forall\ 1 \le i \le n.\ a_i \mid \prod_{i=1}^{n} a_i \mid b \Rightarrow a \mid b$

Assume (b). (i.e. $\forall\ 1 \le i \le n.\ a_i \mid b$)

By induction on n.

if $n=1$. ✓

if $n=2$. $\Rightarrow$

Since $a_i \mid b \Rightarrow \exists\ n_i \in \mathbb{Z}$ s.t. $a_i n_i = b$

$a_1 \mid b = a_2 \cdot n_2 \xrightarrow[\text{Gauss' lemma}]{\gcd(a_1, a_2)=1} a_1 \mid n_2 \Rightarrow a_1 a_2 \mid a_2 n_2$

In general, one can ~~the~~ use the associativity of multiplication to reduce to the case ~~with two factors~~ $n=2$. $\Rightarrow a_1 \cdot a_2 \mid b$

□

Let R be a commutative ring.

$I_1, \ldots, I_r$ be ideals of R.

<u>operation on sets</u> : $\cup$ $\cap$

$I_1 \cup \cdots \cup I_r$ is not an ideal in general. X

$I_1 \cap \cdots \cap I_r$ is an ideal of R.

(i.e. $\bigcap_{i=1}^{r} I_i$ is a subgp of $(R,+)$

s.t. $\forall x \in R.\ x \cdot \bigcap_{i=1}^{r} I_i \subset \bigcap_{i=1}^{r} I_i$)

$\cup$

$I_1 \cdots I_r$ is an ideal of R

Def: Let $a_1, \dots, a_r \in \mathbb{Z}$

$I = (a_1) \cap \cdots \cap (a_r)$ is an ideal of $\mathbb{Z}$

Since $\mathbb{Z}$ is P.I.D., $\exists!$ $d \in \mathbb{N}$ s.t. ~~(d)~~ $I = (d)$.

We call this nature # d the least common multiple of $a_1, \dots, a_r$ denoted by $\operatorname{lcm}(a_1, \dots, a_r)$.

Rmk: $\forall a \in \mathbb{Z}$, $\operatorname{lcm}(aa_1, \dots, a a_k) = |a| \cdot \operatorname{lcm}(a_1, \dots, a_k)$

Prop: Let $a_1, \dots, a_r$ be pairwise coprime integers. Then $\operatorname{lcm}(a_1, \dots a_r) = |a_1 \cdots a_r| \in \mathbb{N}$

Pf: $\forall\ 1 \le i \le r$. By the def. of lcm, $d = \operatorname{lcm}(a_1, \cdots, a_r)$. we have $d \in a_i\mathbb{Z}$ $\left(\Leftrightarrow a_i \mid d\right)$.

Since $a_1, \cdots, a_r$ are pairwise coprime, $\left|\prod_{i=1}^{r} a_i\right| \mid d$.

On the other hand, $a_i \mid \left|\prod_{i=1}^{r} a_i\right| \quad \forall\ 1 \le i \le r$.

$$\Rightarrow \left|\prod_{i=1}^{r} a_i\right| \in d\mathbb{Z} = \bigcap_{i=1}^{r} (a_i) \Rightarrow d \mid \left|\prod_{i=1}^{r} a_i\right|.$$

Pf: Let $a, b \in \mathbb{Z}$. Then $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = |a \cdot b|$

Pf: By def. of gcd, $\exists\ x, y \in \mathbb{Z}$ s.t. $\gcd(a,b) = ax + by$. $\Rightarrow \begin{cases} (ax+by) \cdot \operatorname{lcm}(a,b) \\ a \mid \operatorname{lcm}(a,b),\ b \mid \operatorname{lcm}(a,b) \end{cases}$ □

$$\Rightarrow \quad |a \cdot b| \;\Big|\; \underbrace{(ax+by)\cdot \operatorname{lcm}(a,b)}_{ax\cdot \operatorname{lcm}(a,b) \;+\; by\cdot \operatorname{lcm}(a,b)} \;=\; \gcd(a,b)\cdot \operatorname{lcm}(a,b)$$

On the other hand, $\begin{cases} \gcd(a,b) \mid a \\ \gcd(a,b) \mid b \end{cases} \Longrightarrow$ $\exists\, x, y \in \mathbb{Z}$ s.t. $\begin{cases} a = \gcd(a,b)\cdot x \\ b = \gcd(a,b)\cdot y \end{cases}$

$$\Rightarrow \begin{cases} a \mid \gcd(a,b)\cdot x\cdot y \\ b \mid \gcd(a,b)\cdot x\cdot y \end{cases}$$

by def lcm.

$$\Rightarrow \gcd(a,b)\cdot x\cdot y\cdot \mathbb{Z} \subseteq \operatorname{lcm}(a,b)\cdot\mathbb{Z}$$

$$\Rightarrow \operatorname{lcm}(a,b) \mid \gcd(a,b)\cdot x\cdot y.$$

$$\Rightarrow \operatorname{lcm}(a,b)\cdot\gcd(a,b) \mid \underbrace{\gcd(a,b)\cdot x}\cdot \underbrace{\gcd(a,b)\cdot y} = a\cdot b$$

$$a\mathbb{Z} \cap b\mathbb{Z} = \text{“}$$

□

§1.2 Primes.

Def:6 An integer $p \in \mathbb{Z}$ is called a prime.

if. $\forall\, a, b \in \mathbb{Z}$. & $p \mid a \cdot b$, then we have. $p \mid a$ or $p \mid b$

II. ~ Special. for $\mathbb{Z}$

An integer p has no. non-trivial factors (i.e. the only factors of p are. ± 1. $\pm p$)

(1) Relatively easy to check (with the help of computer).

(2) If an integer is not a prime, then we call it a composite #.

Ex: 2, 3, 5, 7, 11, 17, 19, ..., 15485863, ...

are primes.

---

(1) Do multiplication is easy, do factorization is hard.

1776, Anton Felkel gave a table containing the factorization of integers n with $1 \le n \le 408000$ which are divided by 2, 3, 5.

$\rightsquigarrow$ planned to extend this table to 1 million.

2. 3. 5. 7.

11 13 17 19.

23 29.

31. 37.

41. 43 47

53 59.

61 67.

71 73 79

83 89.

97

25 primes which is less than 100

Can you find a formula for primes?

Fermat: $F_n = 2^{2^n} + 1 \quad n \in \mathbb{N}$

primes $\begin{cases} F_0 = 3, \quad F_1 = 5, \quad F_2 = 17 \\ F_3 = 257, \quad F_4 = 65537 \end{cases}$

$$F_n - 2 = 2^{2^n} + 1 - 2 = 2^{2^n} - 1 = \left(2^{2^{n-1}} + 1\right) \cdot \left(2^{2^{n-1}} - 1\right)$$

$$= F_0 \cdot \cdots \cdot F_{n-1}$$

$\bigstar$ $F_n = F_0 \cdots F_{n-1} + 2$.

Thm: There are infinitely many primes.

Pf: $(F_n, F_{n-1}) = 1$. There are infinitely many Fermat #'s.

If there are only finitely many primes, then $\exists N$ big enough,

F_n $n \leq N$ $\square$

1732. Euler. $F_5 = 2^{2^5} + 1 = 4294967297$

$= 641 * 6700417.$

Again: Factorization is difficult.

1855. Clausen gave a factorization of F_6.

Mersenne prime: $2^n - 1$, the necessary condition: n is a prime.

of the form

Observation: Once we have a prime p, consider $2^p - 1$ to find a bigger prime

- $2^2 - 1 = 3$
- $2^3 - 1 = 7$
- $2^5 - 1 = 31$
- $2^7 - 1 = 127$

$2^{136279841} - 1$ ... (is) the 9 Largest known prime # Oct. 21, 2024.

by

The first one obtained using GPU.

$\mathcal{P} = \{ \text{prime \#'s} \}$ $\quad \# \mathcal{P} = +\infty$

Thm : (fundamental thm of arithmetic).

$\forall$ nonzero natural #. n, we can write in a unique way (up to ordering)

$$n = \prod_{i=1}^{r} p_i^{a_i} \quad , \quad p_i \in \mathcal{P} \quad a_i \in \mathbb{N}_{>0}$$

$p_i \neq p_j$ if $i \neq j$.

$\forall$ $a, b \in \mathbb{Z}$, if we know the factorization of a & b, then it's easy to compute the gcd of a, b ~~& lcm~~

$$a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$$

$$b = \prod_{p \in \mathcal{P}} p^{v_p(b)}$$

$$\gcd(a,b) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$$

$$\operatorname{lcm}(a,b) = \prod_{p \in \mathcal{P}} p^{\max(\,,\,)}$$

Prop: If p is a prime, $k \in \{1, \dots, p-1\}$, then

$$p \mid \binom{p}{k}.$$

Pf: If p_0 is a prime dividing $k! = 1 \cdots k$

then $p_0 \leq k$

$\Rightarrow p \nmid k!$ & $p \nmid (p-k)!$ & $\Rightarrow p \mid p! = \binom{p}{k} \cdot k!(p-k)!$

$\Rightarrow p \mid \binom{p}{k}$

Thm. (Wilson) An integer $p \geq 2$ is a prime.

iff $(p-1)! \equiv -1 \mod p$

---

pf: Let $A = \{1, 2, \cdots, p-1\}$

"$\Leftarrow$" Assume p is a composite #.

then $p = a \cdot b$ with $a, b \in A \setminus \{1\}$

By the assumption $(p-1)! \equiv -1 \mod p$, $\Rightarrow \exists\, t \in \mathbb{Z}$ s.t.

$(p-1)! - t \cdot p = -1$

$\Rightarrow 1 = t \cdot p - (p-1)! = a\left(t \cdot b - (a-1)! \cdot (a+1) \cdots (p-1)\right) \Rightarrow a \mid 1$ ×

$\therefore \Longleftarrow$ if $p=2$ ✓

Assume $p \geq 3$

Claim: $\forall\, i \in A,\ \exists!\ j \in A$ s.t. $ij \equiv 1 \bmod p$.

✱ In particular, $i=j \iff i=1$ or $i=p-1$.

Pf of claim: $\gcd(i,p)=1$ (since p is a prime, $i<p$)

$\exists!\ j \in A$ s.t. $j \equiv x \bmod p$

$\therefore ij \equiv 1 \bmod p$

$\Longrightarrow \exists\, x, y \in \mathbb{Z}$ s.t. $ix + py = 1$.

$\Longrightarrow ix \equiv 1 \bmod p$

But A is a set of representatives of $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$

Assume. $i = j$. $\quad i^2 \equiv 1 \bmod p \implies p \mid (i^2 - 1) = (i+1)(i-1)$.

$\implies p \mid (i-1)$ or $p \mid (i+1)$.

(1) if $p \mid (i+1)$. $\implies i \equiv p-1 \bmod p \implies i = p-1$.

(2) if $p \mid (i-1) \implies x \equiv 1 \bmod p \implies i = 1$

Use the relation $ij \equiv 1 \bmod p$ to pair the elements in A.

Except 1 & $p-1$. $\implies (p-1)! \equiv 1 \cdot (p-1) \cdot \prod_{1<k<p-1} k \equiv 1 \cdot (p-1) \cdot 1^{\frac{p-3}{2}}$ D

$\equiv -1 \bmod p$

Rmk: In Wilson's thm, $(p-1)! \equiv -1 \mod p$

$\Longleftrightarrow p \mid (p-1)! + 1$

But consider $p^2 \mid (p-1)! + 1$? , $p^3 \mid (p-1)! + 1$?

If p is prime & $p^2 \mid (p-1)! + 1$, then p is called a Wilson prime

5, 13, 563 are Wilson prime.

? $\#\{\text{Wilson prime}\} = +\infty$ or not

Take $n = p$ a prime.

$$\mathbb{F}_p := \frac{\mathbb{Z}}{p\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots \overline{p-1}\}$$

$\ker\varphi := \{m \in \mathbb{Z} \text{ s.t. } \varphi(m) = 0\}$

- If $\ker\varphi = (0)$, then k is of characteristic 0
- If $\ker\varphi = (p)$, k is of characteristic p

(Since p is a prime, $\forall\, 1 \le i \le p-1$, $\exists\, j$ s.t. $ij \equiv 1 \bmod p$

$\mathbb{Q}$ is a field

$\Rightarrow \begin{cases} \mathbb{Q} \hookrightarrow k \\ \mathbb{F}_p \hookrightarrow k \end{cases}$

The field $\mathbb{Q}$ & $\mathbb{F}_p$ $\forall$ p prime are called **prime field**.

$\forall$ k an abstract field.

$\mathbb{Z} \xrightarrow{\varphi} k$

$\mathbb{Q}^* \longmapsto$ e unit for multiplication

$n \cdot e = \underbrace{e + e + \dots + e}_{n}$