FORMULA SHEET

Division Algorithm

Let $a \in \mathbb{Z}, b \in W$. $\exists!\ q, r$ st $a = bq + r, \quad 0 \le r < b$.

- $q = \lfloor a/b \rfloor = a \text{ div } b$

  $r = a - bq = a \bmod b$

PHP: n holes + $n+1$ pigeons $\Rightarrow$ $\exists$ atleast 1 hole with ≥ 1 pigeons.

Divisibility

- If $r = 0$, $a \mid b$
- $a \mid b$, $b \mid c \Rightarrow a \mid c$
- $a \mid b$, $a \mid c \Rightarrow a \mid \alpha a + \beta b$
- # of integers $\le a$ & div by $b = \lfloor \frac{a}{b} \rfloor$

IEP: $|\cup A_i| = \sum A_i - \sum A_i \cap A_j + \cdots + (-1)^{n+1} \left| \bigcap_{i=1}^{n} A_i \right|$

Prime & Composite

- $p \in W$, p has only 2 factors $\rightarrow$ p is prime
- q is not prime $\rightarrow$ composite
- Every number ≥ 2 has a prime factor.
- $\exists$ inf. many primes
- Every composite no. has a prime factor $\le \lfloor \sqrt{n} \rfloor$

Fibonacci

$F_1 = 1 = F_2$

$F_n = F_{n-1} + F_{n-2} \quad \forall\ n \ge 3$

$F_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-i-1}{i} \quad i \ge 1$

Properties

- $\sum_{i=1}^{n} f_i = F_{n+2} - 1$
- $f_{n-1} f_{n+1} - f_n^2 = (-1)^n \quad \forall\ n \ge 1$
- $f_n = 2f_{n-2} + f_{n-3} \quad \forall\ n \ge 4$
- $5 \mid f_{5n}$
- $\sum f_{2i-1} = f_{2n}$

- $\sum f_{2i} = f_{2n+1} - 1$

Lucas sequence

$L_1 = 1, \quad L_2 = 3$

$L_n = L_{n-1} + L_{n-2}$

$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ (α, β) are roots of $x^2 = x + 1$.

$L_n = \alpha^n + \beta^n$

Properties
- $\sum L_i = L_{n+2} - 3$
- $\sum L_{2i-1} = L_{2n} - 2$
- $\sum L_{2i} = L_{2n+1} - 1$
- $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$
- $\sum L_i^2 = L_n L_{n+1} - 2$

- $F_{2n} = F_n L_n$
- $F_{n-1} + F_{n+1} = L_n$

Format numbers

$f_n = f_{n-1}^2 - 2f_{n-1} + 2$

$f_n = 2^{2^n} + 1$

f_n is prime $\Rightarrow$ Fermat prime.

- Every prime factor of f_n is of the form $k 2^{n+2} + 1$

Chapter - 3 : GCD

GCD
- Greatest common divisor
- $d = (a, b)$
  - $\rightarrow d|a, \; d|b$
  - $\rightarrow \forall \; d'|a, \; d'|b \Rightarrow d' \leq d$
- $(a, b) = 1 \Rightarrow$ coprime
- $f_0 f_1 \ldots f_{n-1} = f_n - 2$
- $(f_m, f_n) = 1 \quad \forall \; m \neq n$

- $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
- $d = (a, a-b)$
- $\forall\ x, y \in \mathbb{Z},\ d = ax + by$
- $(a,b) = 1 \Leftrightarrow \exists \alpha, \beta \in \mathbb{Z}$ s.t. $a\alpha + b\beta = 1$
- $d' \mid a,\ d' \mid b,\ d' \neq d \Rightarrow d' \mid d$.
- $d = (a,b)$
  - $\rightarrow d \mid a,\ d \mid b$
  - $\rightarrow \forall\ d' \mid a,\ d' \mid b \Rightarrow d' \mid d$.
- $(ac, bc) = c(a,b)$
- $(a,b) = 1$ & $a \mid cb \Rightarrow a \mid c$
- $a \mid c,\ b \mid c,\ (a,b) = 1 \Rightarrow ab \mid c$
- $(a_1, a_2 \ldots, a_n) = ((a_1, \ldots a_{n-1}), a_n)$

Euclidean Algorithm.

To find (a,b)

- $r = a \bmod b \Rightarrow (a,b) = (b,r)$

Fundamental Thm of Arithmetic

Let p be prime.

- $p \mid ab \Rightarrow p \mid a$ or $p \mid b$
- $p \mid a_1 a_2 \ldots a_n \Rightarrow p \mid a_i$ for some i
- Every $a \in \mathbb{N}$, $a \geq 2$
  - is either a prime
  - can be expressed as a product of primes.

Canonical decomposition

- $N = \prod_{i=1}^{n} p_i^{a_i}$
- Unique upto order
- $a, a+b, a+2b, \ldots$ has inf many primes, if $(a,b) = 1$

Least Common Multiple

- $m = [a,b]$ if
  - $\rightarrow a|m,\ b|m$
  - $\rightarrow a|m',\ b|m' \rightarrow m' \geq m$
- $[a,b](a,b) = a \cdot b$
- $[a_1, a_2, \dots, a_n] = [[a_1, \dots a_{n-1}], a_n]$
- $(a_i, a_j) = 1\ \forall\ i \neq j,\ [a_1, \dots a_n] = a_1 \cdot a_2 \cdots a_n$

Linear Diophantine Equations

$$ax + by = c, \quad a,b,c \in \mathbb{Z} \rightarrow (1)$$

- We want $(x,y) \in \mathbb{Z}^2$
- (1) is solvable $\Leftrightarrow (a,b) \mid c$
- $x = x_0 + \left(\frac{b}{d}\right)t,\ y = y_0 - \left(\frac{a}{d}\right)t$

Euler's method

- Division Algorithm
- Recursive Substitution

Congruences

- $a \equiv b \pmod m \Longleftrightarrow m \mid a-b$
- $\equiv$ is eq. relation
- If $a \equiv b \pmod m$
  - $\rightarrow ac \equiv bc \pmod m$
  - $\rightarrow a^n \equiv b^n \pmod m$

If $c \equiv d \pmod m$

- $\rightarrow a \pm c \equiv b \pm d \pmod m$

If $ac \equiv bc \pmod m,\ (c,m) = 1$

- $\Rightarrow a \equiv b \pmod m$

If $ac \equiv bc \pmod m,\ (c,m) = d$

- $\Rightarrow a \equiv b \pmod{m/d}$

If $a \equiv b \pmod{m_i}$ $i = 1$ to k

$a \equiv b \pmod{[m_1, \ldots m_k]}$

Linear congruences

- $ax \equiv b \pmod{m}$
- Solvable $\Leftrightarrow d \mid b$, $d = (a, m)$

  → has d incongruent solutions
- When $d = 1$, 1 soln.

  x is called least residue of $a^{-1}b$ modulo m.

Systems of Congruences

CRT: Consider the system

$x \equiv a_i \pmod{m_i}$ $1 \le i \le k$

- $(m_i, m_j) = 1$ $\forall\, i \neq j$
- has a unique soln mod $m_1 m_2 \cdots m_k$

$$x \equiv \sum_{i=1}^{k} a_i M_i y_i \pmod{M}$$

→ $M = \prod_{i=1}^{k} m_i$

→ $M_i = \frac{M}{m_i}$

→ y_i is an inverse of M_i mod m_i

② Solvable $\Leftrightarrow$ $(m_i, m_j) \mid a_j - a_i$ $\forall\, j \neq i$

→ when solvable, has a unique soln mod $[m_1, m_2, \ldots, m_k]$

Wilson's Theorem

- a is self invertible mod $p \Leftrightarrow a \equiv \pm 1 \pmod{p}$
- p prime; $(p-1)! \equiv -1 \pmod{p}$
- If $(n-1)! \equiv -1 \bmod n$, n is prime

Fermat's Little Theorem

- Let $a \in \mathbb{Z}$ st $p \nmid a$.

  $a, 2a, \ldots, (p-1)a$ are a permutation of $1, 2, 3, \ldots, p-1$.

- $a^{p-1} \equiv 1 \pmod p$
- a^{p-2} is an inverse of $a \bmod p$.
- $ax \equiv b \pmod p$, $p \nmid a$

$\Rightarrow x \equiv a^{-1} b \pmod p$

- $p \nmid a \Rightarrow a^p \equiv a \pmod p$
- $\{p_i\}_{i=1}^{k}$ be primes, $a \in \mathbb{Z}$

$l = [p_1 - 1, \dots, p_k - 1]$

$a^{l+1} \equiv a \pmod{p_1 p_2 \cdots p_k}$

Carmichael Number: $n \in \mathbb{N}$ be composite s.t.

$a^{n-1} \equiv 1 \pmod n \quad \forall (a, n) = 1$

Euler's Theorem

$\varphi(x) = \#$ of $x \in \mathbb{Z}^+ \le m$ and $(x, m) = 1$

$\varphi(p) = p - 1$

- Let $a \in \mathbb{Z}$ s.t. $(a, m) = 1$, Let $r_1, r_2, \dots, r_{\varphi(m)} \le m$, $(r_i, m) = 1$.

Then $ar_1, ar_2, \dots, ar_{\varphi(m)} \pmod m \cong$ permutation of $r_1, r_2, \dots, r_{\varphi(m)}$

- Let $a \in \mathbb{Z}$, s.t. $(a, m) = 1$.

$a^{\varphi(m)-1}$ is an inverse of $a \bmod m$.

- $\varphi(p^e) = p^e - p^{e-1}$

Well ordering Principle (Axiom of choice)

1. Every non-empty set of natural numbers has a least element.

First Principle of Mathematical induction (weak induction)

Let S be a subset of natural numbers satisfying the foll. properties.

(1) $1 \in S$

(2.) If k is an arbitrary positive integer st $k \in S$, then $k+1 \in S$

Then $S = \mathbb{N}$.

Proof

Let $S' = \mathbb{N} - S$

If $S \neq \mathbb{N} \Rightarrow S' \neq \phi$

By wop, S' has a least element, say l. $(\neq 1)$

Then $l-1 \in S$. (Otherwise, $l-1 \in S'$)

$\Rightarrow (l-1)+1 \in S$

$\Rightarrow l \in S$

$\Rightarrow\leftarrow$ as $l \in S'$

$\therefore S' = \phi$

$\Rightarrow \boxed{S = \mathbb{N}}$

Proving statements using PMI.

Eg: $\sum_{k=1}^{n} \frac{1}{k^2} \leq 2 - \frac{1}{n} \rightarrow (1)$

$S = \{n \in \mathbb{N} :$ inequality (1) is true $\}$

To prove: $S \in \mathbb{N}$

For $n=1$,

$\frac{1}{1^2} \leq 2 - \frac{1}{1} = 1$ is true

$\therefore 1 \in S$.

Let $k \in S$.

$$\frac{1}{1^2} + \frac{1}{2^2} + \dots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$$

To show $k+1 \in S$.

$$\frac{1}{1^2} + \frac{1}{2^2} + \dots + \frac{1}{k^2} + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{k} + \frac{1}{(k+1)^2}$$

$$\leq 2 - \left(\frac{1}{k} - \frac{1}{(k+1)^2} \right)$$

$$\leq 2 - \left(\frac{(k+1)^2 - k}{k(k+1)^2} \right)$$

$$\leq 2 - \left(\frac{k^2 + k + 1}{k(k+1)^2} \right)$$

$$\leq 2 - \frac{1}{k+1} - \frac{1}{k(k+1)^2}$$

$$\leq 2 - \frac{1}{k+1}$$

$\boxed{S = \mathbb{N}}$

Prove that

$$1^2 - 2^2 + 3^2 - 4^2 + \dots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}$$

$S = \{ n \in \mathbb{N} : \text{inequality } ① \text{ is true} \}$

① $1^2 = (-1)^0 (1) \frac{(2)}{2} = 1 \in S$

② let $k \in S$.

$$1^2 - 2^2 + 3^2 - 4^2 + \dots + (-1)^{k-1} k^2 = (-1)^{k-1} \frac{k(k+1)}{2}$$

To prove: $k+1 \in S$.

$$1^2 - 2^2 + \dots + (-1)^{k-1} k^2 + (-1)^k (k+1)^2$$

$$= (-1)^{k-1} \frac{k(k+1)}{2} + (-1)^k (k+1)^2$$

$$= (-1)^k (k+1) \left\{ \frac{-k}{2} + k+1 \right\}$$

$$= (-1)^k \frac{(k+1)}{2} \{ -k + 2k + 2 \}$$

$$= (-1)^k \frac{(k+1)(k+2)}{2}$$

$\therefore S = \mathbb{N}$

Lecture - 2

12.01.25

Floor function

$x \in \mathbb{R}$

$\lfloor x \rfloor$ = greatest integer less than or equal to x.

$\lfloor \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$

Eg: 1. $\lfloor 1.5 \rfloor = 1$

Ceil function

$x \in \mathbb{R}$

$\lceil \rceil : \mathbb{R} \longrightarrow \mathbb{Z}$

$\lceil x \rceil$ = least integer greater than or equal to x.

Eg: $\lceil 1.5 \rceil = 2$

Note: If $x \in \mathbb{Z}$, $\lfloor x \rfloor = \lceil x \rceil$

If $x \in \mathbb{R} - \mathbb{Z}$, $\lfloor x \rfloor = \lceil x \rceil - 1$

Notations

① Summation

i) $\sum_{i=1}^{n} a_i = a_1 + \dots + a_n$

ii) $\sum_{i=m}^{n} a_i = a_m + \dots + a_n$

$= \sum_{i \in \Lambda} a_i$, $\Lambda = \{a_m, a_{m+1}, \dots a_n\}$

② Product

i) $\prod_{i=1}^{n} a_i = a_1 a_2 \dots a_n$

ii) $\prod_{i=m}^{n} a_i = a_m a_{m+1} \dots a_n$

$= \prod_{i \in \Lambda} a_i$

$\Lambda = \{a_m, \dots, a_n\}$

EXAMPLES

① $\prod_{K=0}^{50} (-1)^K = -1$

② $\sum_{i=m}^{n} m+n-i = \sum_{i=1}^{m} i$

③ $\sum_{d \mid 12} d = 1+2+3+4+6+12$

$= 28$

④ If n is odd,

$\lfloor n \rfloor = n$

$\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$

$\left\lceil \frac{n}{2} \right\rceil = \frac{n+1}{2}$

5. Find the # of 0s at the end of $f(9)$

$f(9) = \sum_{K=1}^{n} K \cdot K!$

$= 1 \cdot 1! + 2 \cdot 2! + \cdots + 9 \cdot 9!$

$= \sum_{K=1}^{9} K \cdot K!$

$= \sum_{K=1}^{9} (K+1-1) K!$

$= \sum_{K=1}^{9} (K+1)! - \sum_{i=9} K!$

$= 10! - 1$ $\Rightarrow$ No zeros

SECOND PRINCIPLE OF MATHEMATICAL INDUCTION (Strong version)

Example:

$a_1 = 1, \quad a_2 = 3$

$a_n = a_{n-1} + a_{n-2} \qquad n \geq 3$

To show: $a_n < \left(\frac{7}{4}\right)^n$

Vanilla induction fails! Not enough info.

Statement

Let S be a subset of natural numbers satisfying the foll:

① $1 \in S$

② If $1, 2, 3, \ldots, k-1, k \in S$, then $k+1 \in S$.

Then $S = \mathbb{N}$

We will solve the example now.

We have

① $1 \in S$

② $1, 2, 3, \ldots, k-1, k \in S$

$$a_{k+1} = a_k + a_{k-1}$$

$$< \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1}$$

$$< \left(\frac{7}{4}\right)^{k-1}\left(1 + 7/4\right)$$

$$< \left(\frac{7}{4}\right)^{k-1}\left(\frac{11}{4}\right)$$

$$< \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2$$

$$< \left(\frac{7}{4}\right)^{k+1}$$

$\Rightarrow k+1 \in S$

By 2nd PMI, $S = \mathbb{N}$.

$$a_n < \left(\frac{1}{4}\right)^n \quad \forall\, n \in \mathbb{N}$$

Example

Show that $n! > n^2$

Doesn't hold for $n \leq 3$.

Generalised First PMI

Let $S \subseteq \mathbb{N}$ be satisfying the foll:

① $n_0 \in S$

② If $k \in \mathbb{Z}^+ > n_0$ st $k \in S$, then $k+1 \in S$

Then $S = \mathbb{N}_{\geq n_0}$

Generalized Second PMI

Let $S \subseteq \mathbb{N}$ be satisfying the foll.

① $n_0 \in S$

② $n_0, n_0+1, \ldots, k-1, k \in S$, then $k+1 \in S$.

Then $S = \mathbb{N}_{\geq n_0}$.

Problem:

$$n! \geq n^2 \quad \forall\ n \geq 4$$

Invoke generalized 1st PMI

- Clearly true for $n_0 = 4$
- Assume that $k \geq 4 \in S$
- To show $k+1 \in S$

$k \in S \Rightarrow k! \geq k^2$

$$(k+1)! = (k+1)\,k!$$
$$\geq (k+1)\,k^2$$
$$\geq (k+1)(k+1) \quad [\text{As } k^2 > k+1 \ \forall\, k \geq 1]$$
$$\geq (k+1)^2$$

$\Rightarrow k+1 \in S$

$\boxed{S = \mathbb{N}_{n \geq 4}}$

Problem:

PT: any postage of n stamps $n \geq 2$ can be made with 2 and 3 cent cent stamps.

Soln:

$\forall\, n \geq 2$, $n = 2a + 3b$ $\quad a, b \in \mathbb{N} \cup \{0\}$

Let S be the set for which this is true.

- 2 is made with 1 2 cent Stamp.
  $\Rightarrow 2 \in S$
- Suppose $k \in S \Rightarrow k = a + 3b$

  To show $k+1 \in S$

$$k+1 = 2a + 3b + 1$$
$$= 2a + 3b + 3 - 2$$
$$= 2(a-1) + 3(b+1)$$

Pitfall:
$a = 0$
$\Rightarrow a - 1 < 0$

Strong PMI

Assume this is true for $2, 3, \ldots, k-1, k$.

Suppose $k-1 = 2a_1 + 3b_1$

$k = 2a_2 + 3b_2$

where $a_1, a_2, b_1, b_2 \in S$.

Then $k+1 = k-1+2$

$= 2a_1 + 3b_1 + 2$

$= 2(a_1+1) + 3b_1$

$\Rightarrow k+1 \in S \qquad S = \mathbb{N}_{n \geq 2}$

Recursive definition of a function

Factorial

$f(0) = 1$

$f(1) = 1$

$f(n) = n\, f(n-1) \quad \forall\ n \geq 2$

Problems

The handshake problem

17.01.25

There are n guests at a party. Each person shakes hand with everybody. Define recursively the # of handshakes.

Suppose $h(n)$ denotes # of handshakes with n guests at a party.

Then

$h(1) = 0$

$h(n) = h(n-1) + n-1 \quad \forall\ n \geq 2$

$= (n-1) + (n-2) + (n-3) + \cdots + 1$

$= \frac{n(n-1)}{2}$

Binomial Theorem

Binomial coefficients

Let $n, r \in \mathbb{Z}^+ \cup \{0\}$.

$$nC_r := \binom{n}{r} = \begin{cases} \frac{n!}{r!\,n-r!} & r \leq n \\ 0 & \text{otherwise} \end{cases}$$

Pascal's Identity

Let $n, r \in \mathbb{N}$

$$\boxed{\binom{n-1}{r} + \binom{n-1}{r-1} = \binom{n}{r}}$$

Proof

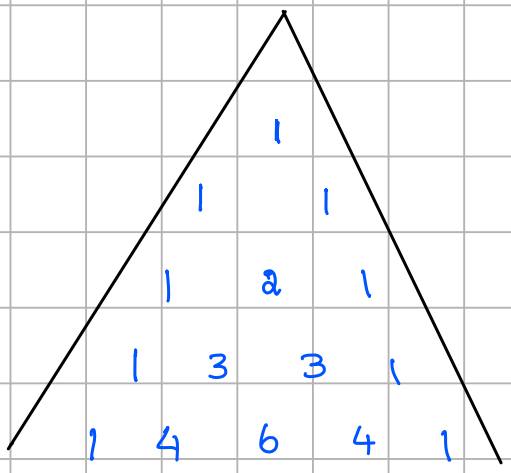
$$\binom{n-1}{r} + \binom{n-1}{r-1} = \frac{(n-1)!}{r!\,(n-r-1)!} + \frac{(n-1)!}{(r-1)!\,(n-r)!}$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r-1)!}\left\{\frac{1}{r} + \frac{1}{n-r}\right\}$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r-1)!}\left\{\frac{n}{r\,(n-r)}\right\}$$

$$= \frac{n!}{r!\,(n-r)!}$$

Pascal's Triangle



① $\binom{n}{r}$ appears as $(r+1)^{th}$ entry in the $(n+1)^{th}$ row

② r^{th} row represents 11^r.

③ This Δ^{le} is symmetric about vertical line through the middle.

Binomial Theorem.

Let $n \in \mathbb{W}$. Then

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$$

where $x, y \in \mathbb{R}$

PROOF:

$n=0$; $(x+y)^0 = 1$

RHS $= x^0 y^0 = 1$

Suppose this holds for $n=k$.

i.e.,

$$(x+y)^k = \sum_{r=0}^{k} \binom{k}{r} x^{k-r} y^r$$

Now, for $n = k+1$

$$(x+y)^{k+1} = (x+y)(x+y)^k$$

$$= (x+y) \sum_{r=0}^{k} \binom{k}{r} x^{k-r} y^r$$

$$= \sum_{r=0}^{k} \binom{k}{r} x^{k+1-r} y^r + \sum_{r=0}^{k} x^{k-r} y^{r+1} \binom{k}{r}$$

$$= x^{k+1} + \sum_{r=1}^{k} \binom{k}{r} x^{k+1-r} y^r + \sum_{r=0}^{k-1} x^{k-r} y^{r+1} \binom{k}{r} + y^{k+1}$$

$$= x^{k+1} + \sum_{r=1}^{k} \binom{k}{r} x^{k+1-r} y^r + \sum_{r=1}^{k} x^{k-r+1} y^r \binom{k}{r-1} + y^{k+1}$$

$$= x^{k+1} + \sum_{r=1}^{k} \binom{k+1}{r} x^{k+1-r} y^r + y^{k+1}$$

$$= \sum_{r=0}^{k+1} \binom{k+1}{r} x^{k+1-r} y^r$$

IDENTITIES

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$$

① $2^n = \sum_{r=0}^{n} \binom{n}{r} = {}^nC_0 + {}^nC_1 + \cdots + {}^nC_n$

② # of subsets from a set of size n $\} = 2^n$

③ $0 = {}^nC_0 - {}^nC_1 + {}^nC_2 + \cdots + (-1)^n {}^nC_n$

④ Adding ① and ③

$\Rightarrow 2^n = 2\left[{}^nC_0 + {}^nC_2 + \cdots\right]$

$\Rightarrow \boxed{{}^nC_0 + {}^nC_2 + \cdots = 2^{n-1}}$

Ily $\boxed{{}^nC_1 + {}^nC_3 + {}^nC_5 + \cdots = 2^{n-1}}$

Qn

PT:

$${}^2C_2 + {}^3C_2 + \cdots + {}^nC_2 = \binom{n+1}{3} \quad \forall n \geq 2$$

Base case

${}^2C_2 = 1 = {}^3C_3$

Suppose it holds for $n = k$

$$2C_2 + 3C_2 + \cdots + {}^kC_2 = \binom{k+1}{3}$$

$${}^nC_r + {}^nC_{r-1} = {}^{n+1}C_r$$

We show it for $n = k+1$

$$2C_2 + 3C_2 + \cdots + {}^kC_2 + {}^{k+1}C_2 = {}^{k+1}C_3 + {}^{k+1}C_2$$

$$= {}^{k+2}C_3$$

$$= \binom{(k+2)+1}{3}$$

PT: $1\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n} = n2^{n-1} \quad \forall\, n \geq 1$

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$$

Sub $y = 1$

$$(1+x)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r}$$

Diff wrt n

$$n(1+x)^{n-1} = \sum_{r=0}^{n} (n-r)\binom{n}{r} x^{n-r-1}$$

Sub $x = 1$

$$n\,2^{n-1} = \sum_{r=0}^{n} (n-r)\binom{n}{r}$$

$$= \sum_{r=0}^{n} (n-r)\binom{n}{n-r}$$

$$= n\binom{n}{n} + (n-1)\binom{n}{n-1} + \cdots + 2\binom{n}{2} + 1\binom{n}{1}$$

■

19.01.25

Recall the WOP. It says that

"Any non-empty subset of $\mathbb{N}$ has a least element"

We now generalize this to any non-empty subset of $\mathbb{Z}_{\geq 0}$ as:

"Any non-empty subset of $\mathbb{Z}_{\geq 0}$ has a least element"

Proof:

Suppose $S \subseteq \mathbb{N} \cup \{0\}$.

If $0 \in S$, 0 is the least element.

If $0 \notin S$, by (weak) WOP, S has a least element.

Think: does any set which is bounded on one side well ordered?

Division Algorithm:

- Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$. Then $\exists!\ q, r \in \mathbb{Z}$ st $a = bq + r$ st $0 \leq r < b$: Here q is called quotient, r is called reminder.
- Here we are interested only in the existence of such integers.

PROOF:

Consider $S = \{a - bx : x \in \mathbb{Z},\ a - bx \geq 0\}$

We apply GWOP.

Step-1: S is non-empty.

If $a \geq 0$, $a = a - b \cdot 0 \in S$ $(x = 0)$

If $a < 0$, take $x = -a$.

More generally, we can take $x = -|a|$.

Then $a - b(-|a|) = a + b|a| \in S$

$\Rightarrow S \neq \phi$

By GWOP, every non-empty subset of S has a least element, say r.

Then $r \in S$

$\Rightarrow r = a - bq$, for some $q \in \mathbb{Z}$.

$a = bq + r$

We have 2 things left now

① $0 \leq r < b$

② Uniqueness.

Suppose, if $r \geq b$

$r = a - bq$

$r - b = a - bq - q$

$= a - b(q+1)$

But $r - b \geq 0$

$\Rightarrow r - b < r \in S$

$\Rightarrow\Leftarrow$

$\therefore 0 \leq b < r$

We are left with uniqueness.

Suppose $\exists\ q_1, r_1$ st

$a = bq_1 + r_1 \rightarrow ①$ and $a = bq_2 + r_2 \rightarrow ②$

$0 \leq r_1 < b$ $\quad 0 \leq r_2 < b$

① - ②

$\Rightarrow 0 = b(q_1 - q_2) + (r_1 - r_2)$

$\boxed{-b < r_1 - r_2 < b}$

If $q_1 \neq q_2$

- $q_1 > q_2 \Rightarrow r_1 - r_2 = b(q_2 - q_1) < -b$ $\Rightarrow\Leftarrow$
- $q_1 < q_2 \Rightarrow r_1 - r_2 = b(q_2 - q_1) > b$ $\Rightarrow\Leftarrow$

$\therefore q_1 = q_2$

$\Rightarrow r_1 = r_2$

$q = \tilde{q}$

$r = \tilde{r}$

Convention:

When $r = 0$, we say $b \mid a$ ("b divides a") or a is a multiple of b.

Properties

① $a \mid b,\ a \mid c \Rightarrow a \mid b \pm c$

② $a \mid b,\ b \mid c \Rightarrow a \mid c$

Problems

① Prove that $\forall n \in \mathbb{Z}_{\geq 0},\ \frac{n(n^2+2)}{3} \in \mathbb{Z}$

i.e., to show $\forall n \in \mathbb{N}$ $\quad 3 \mid n(n^2+2)$

Say $n = 3q + r, \quad 0 \leq r < 3$

Case-1 : $r = 0$

$n = 3q$

$$\frac{n(n^2+2)}{3} = \frac{3q(9q^2+2)}{3} = q(9q^2+2) \in \mathbb{Z}$$

Case-2 : $r = 1$

$n = 3q + 1$

$$\frac{n(n^2+2)}{3} = \frac{3q+1\left((3q+1)^2+2\right)}{3} = \frac{(3q+1)(9q^2+3+6q)}{3}$$

$$= (3q+1)(3q^2+1+2q)$$

Case-3 : $n = 3q+2$

$$n(n^2+2) = (3q+2)\left[(3q+2)^2+2\right] = (3q+2)(9q^2+6+12q)$$
$$= 3(3q+2)(3q^2+2+4q)$$

② PT : $\forall a \in \mathbb{Z}$, $b \in \mathbb{N}$, $\exists!\ q, r$ st
$a = bq + r$ st $2b \le r < 3b$

Proof :

By division algorithm, $\exists!\ \tilde{q}, \tilde{r}$ st $a = b\tilde{q} + \tilde{r}$ $0 \le \tilde{r} < b$.

$$a = b\tilde{q} + \tilde{r} + 2b - 2b$$
$$= b(\tilde{q} - 2) + \tilde{r} + 2b$$

$$\boxed{\begin{aligned} q &= \tilde{q} - 2 \\ r &= \tilde{r} + 2b \end{aligned}}$$

■

③ If an integer is simultaneously a square and a cube, it must be of the form $7k$ or $7k+1$

Suppose n is square or a cube.

$n = 7k + r$ $0 \le r < b$.

let $n = s^2$, $n = t^3$

$n = s^2$

$\Rightarrow s = 7q + r$ $0 \le r < 6$

$s^2 = 49q^2 + 14qr + r^2$ $0 \le r < 6$ $r^2 \in \{0, 1, 4, 9, 16, 25, 36\}$

$= 7(7q^2 + 2qr) + r'$

Choices for $\tilde{r} = \{0, 1, 4, 2\}$

$\Rightarrow s = 7q + r$, $r \in \{0, 1, 2, 4\}$

$t = 7q + r_2 \qquad 0 \le r_2 < 6$

$t^3 = 7k_2 + \tilde{r} \qquad 0, 1, 8, 27, 64, 125, 216$

$\tilde{r} \in \{0, 1, 6\}$

Now $n = s^2$, $n = t^3$

Possible choices for $\tilde{r}$ are $\{0, 1\}$

$\therefore n = 7k$ or $7k+1$.

④ Prove that no integer in the foll. sequence is a square of an integer

$S = 11, 111, 1111, 11111, \ldots$

Each entry is of the form $n = 10q + 1$, $n, q \in \mathbb{Z}_{\ge 0}$

These are all odd numbers.

Any odd # $a = 2k+1$

$a^2 = 4k^2 + 4k + 1$

$= 4\tilde{k} + 1$

$11 + \sum_{i=2}^{n-1} 10^i$

$\therefore$ Any odd square is of the form $4k+1$.

We show the elements of S are of the form $4k+3$.

Finish this

The i^{th} element of sequence is of the form $11 + \sum_{i=2}^{n-1} 10^i$, for $n \ge 3$.

24.01.25

Result

Let $a, b \in \mathbb{N}$. Then the number of positive integers multiples of b and $\leq a$ is $\left\lfloor \frac{a}{b} \right\rfloor$

Proof:

By Division algorithm,

$\exists\ q, r$ $\quad a = bq + r \quad 0 \leq r < b$

$$\frac{a}{b} = q + \frac{r}{b}$$

$$\Rightarrow \boxed{q = \left\lfloor \frac{a}{b} \right\rfloor} \quad \text{since} \quad 0 \leq \frac{r}{b} < 1$$

Example:

Find the number of positive integers ≤ 1000 which are multiples of 7.

$$n = \left\lfloor \frac{1000}{7} \right\rfloor = \lfloor 142.8 \rfloor = 142$$

Result-2

Inclusion - Exclusion principle

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Let $A_1, A_2, \ldots, A_n$ be finite sets. Then

$$\bigcup_{i=1}^{n} A_i = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{n+1} \left| \bigcap_{i=1}^{n} A_i \right|$$

Example:

Find the number of positive integers ≤ 3000 and divisible by 3, 5, or 7.

$$n = \left\lfloor \frac{3000}{3} \right\rfloor + \left\lfloor \frac{3000}{5} \right\rfloor + \left\lfloor \frac{3000}{7} \right\rfloor - \left\lfloor \frac{3000}{15} \right\rfloor - \left\lfloor \frac{3000}{35} \right\rfloor - \left\lfloor \frac{3000}{21} \right\rfloor + \left\lfloor \frac{3000}{105} \right\rfloor$$

$$= 1000 + 600 + 428 - 200 - 85 - 142 + 28$$

$$= 1629$$

Prime numbers

A positive integer >1 is called a prime if it has exactly 2 divisors.

Composite numbers

A positive integer >1 is called composite if it is not prime.

$$\mathbb{N} = \{1\} \sqcup \{\text{PRIMES}\} \sqcup \{\text{composites}\}$$

Lemma 1:

Every positive integer ≥ 2 is divisible by a prime.

Proof:

- We proceed by strong induction.
- For $n=2$, the result holds.
- Assume the result holds for all positive integers $\leq k$.
- To show: It is true for $n = k+1$.
  - If $k+1$ is itself a prime, we are done.
  - If $k+1$ is not a prime, then $\exists$ a divisor d of n st $d \mid k+1$, $2 \leq d \leq k$.
  - By induction hypothesis, $\exists\ p$ st $p \mid d$, p is prime.

By $d \mid k+1 \Rightarrow p \mid k+1$

∴ Result holds true for $n = k+1$

∴ By strong PHI, lemma holds.

Theorem:

There are infinitely many primes.

Proof:

- Suppose there are only finitely many primes, say $p_1, p_2, \ldots, p_k$.
- Construct a new number $n = p_1 p_2 \ldots p_k + 1$

- Since $N \geq 2$, $\exists$ a prime p_i st $p_i | n$ (by the lemma)

  $\Rightarrow p_i | 1$ $\quad \Rightarrow \Leftarrow$

  ∴ There are infinitely many primes.

Proof -2

Consider $N = n! + 1$

$N \geq 2$

$\Rightarrow$ N must be divisible by a prime p.

If $p \leq N$, $p | n!$ and $p | 1$

∴ $p > N$

As p is unbounded, we are done.

Result

Any composite number has a prime divisor p st $2 \le p \le \lfloor \sqrt{n} \rfloor$.

Proof.

Suppose n is composite. Then

$n = ab$,

where atleast one of a or b is $2 \le a \le \lfloor \sqrt{n} \rfloor$.

$\Rightarrow a$ has a prime divisor p st $p \mid n$, $2 \le p \le \lfloor \sqrt{n} \rfloor$

Example

$p = 1601$ is a prime.

$2 \le p \le 40$

$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$

$\nexists\ x \in P$ st $x \mid p$

$\therefore$ p is prime.

25.01.24

Euler (1772)

$f(n) = n^2 - n + 41$

$n = 1, 2, \ldots, 40 \implies$ primes

For $n = 41$, $f(41)$ is not a prime.

Result

There is no polynomial $y(n)$ with integer coefficents that produce primes for any $n \in \mathbb{N}$

Proof:

Suppose there exists such a function.

$f(n) = \sum_{i=0}^{k} a_i n^i$, $a_k \neq 0$, $a_i \in \mathbb{Z}$

Suppose $b \in \mathbb{N}$ is some fixed integer

Then $f(b) = p$, p is a prime

For any $t \in \mathbb{Z}$

$$f(b+tp) = \sum_{i=0}^{k} a_i (b+tp)^i$$

$$= \sum_{i=0}^{k} a_i b^i + p g_1(t)$$

$$\Rightarrow f(b+tp) = p + p g_1(t) \quad \text{for any } t \in \mathbb{Z}$$

$$= p(1 + g_1(t))$$

$p \mid$ RHS

$\Rightarrow \quad f(b+tp) = p \quad \forall t$

Consider

$$h(t) = f(b+tp) - p$$

$$= 0 \qquad \forall t \in \mathbb{Z}$$

$\Rightarrow\Leftarrow$

Largest known non prime

$p = 2^{82589933} - 1$

It has 24862048 digits

- 2, 3 are the only consecutive primes
-

Result:

For any n, one can produce n consecutive composite numbers. as:

$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+n+1 \qquad n \geq 1$

They are divisible by $2, 3, \ldots, n+1$

Various types of primes

① Palindromic primes: 11, 101, 16661

Largest palindromic prime has 1888527 digits.

② Repunit primes

$$R_n = \frac{10^n - 1}{9}$$

$n = 2, 19, 317, 1031$

③ Twin Primes

Primes that differ by 2.

(3,5), (5,7), (17,19) etc.

④ Largest twin prime has 388342 digits.

Goldbach Conjecture

Any even positive integer ≥ 6 can be written as sum of 2 odd primes.

Verified for $n \leq 4.1 \times 10^{18}$

Problem:

Prove that 3,5,7 are the only three consecutive odd integers that are prime:

Proof:

Suppose $\exists$ another triplet $n, n+2, n+4$. , n is odd, is any such triplet.

If $n \neq 3$, then $n = 3k+1$ or $n = 3k+2$

If $n = 3k+1$, $3 \mid n+2$

If $n = 3k+2$, $3 \mid n+1$

$\Rightarrow n = 3, n+2 = 5, n+4 = 7$

Problem:

If p and p^2+2 are primes, p^3+2 is also a prime

Proof:

If $p = 3k+1$,

$$p^2+2 = 9k^2+6k+3$$
$$= 3(3k^2+2k+1)$$

If $p = 3k+2$

$$p^2+2 = 9k^2+12k+6$$
$$= 3(3k^2+4k+2)$$

$\therefore p = 3$.

Problem:

Let P_K denote the k^{th} prime. Prove that $P_{n+1} \leq P_1 P_2 \dots P_n + 1 \quad \forall n \geq 1$.

Proof:

$$N = P_1 P_2 \dots P_n + 1$$

If any of P_i, $1 \leq i \leq n$ divides N.

$\Rightarrow P_i \mid 1$

$\Rightarrow\Leftarrow$

$\Rightarrow P_i \nmid N$.

$\therefore P_{n+1} \leq P_1 P_2 \dots P_n + 1$

29.01.24

Fibonacci numbers

1, 1, 2, 3, 5, 8, . .

n^{th} term: n^{th} fib number

denoted by f_n

$f_1 = 1$

$f_2 = 1$

$\forall n > 2 \quad f_n = f_{n-1} + f_{n-2}$

Basic properties

$$\sum_{i=1}^{n} f_i = f_{n+2} - 1$$

① $n=3$

$f_1 + f_2 + f_3 = 4 = 5-1$

② $n=4$

$f_1 + f_2 + \ldots + f_4 = 7 = 8-1$

Proof.

We proceed by induction

This holds true $\forall\ n = 1 : k$.

We try to prove it for $n = k+1$

$$\sum_{i=1}^{k} f_i = f_{k+2} - 1$$

$$\sum_{i=1}^{k+1} f_i = f_{k+2} - 1 + f_{k+1}$$

$$= f_{k+3} - 1$$

$$= f_{(k+1)+2} - 1$$

② $f_{n-1} f_{n+1} - f_n^2 = (-1)^n \quad \forall\ n \geq 2$

Proof: This holds for $n=2$.

Hypo: Assume this holds for $n=k$, i.e.,

$f_{k-1} f_{k+1} - f_k^2 = (-1)^k \longrightarrow ①$

$F_K = F_{K-1} + F_{K-2}$

$F_{K+1} = F_K + F_{K-1}$

For $n = k+1$

$F_K F_{K+2} - F_{K+1}^2$

$= F_K (F_{K+1} + F_K) - F_{K+1}^2$

$= F_K F_{K+1} + F_K^2 - F_{K+1}^2$

$= F_K F_{K+1} - F_{K+1}^2 + F_{K-1} F_{K+1} + (-1)^{K+1}$

$= F_{K+1} (F_K - F_{K+1} + F_{K-1}) + (-1)^{K+1}$ ($F_K - F_{K+1} + F_{K-1} \to 0$)

$= (-1)^{K+1}$

Pascal's Triangle

Sum along n^{th} diagonal gives F_n

Lucas

$$F_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-i-1}{i} \quad \forall\, n \geq 1$$

- Follows from Pascal's Triangle.

Proof:

Proceed by induction.

$F_2 = \binom{2-1}{0} = 1$ $\therefore$ holds

Lucas sequence:

$1, 3, 4, 7, 11, 18, 29$

n^{th} term of this sequence is called Lucas number "L_n"

$L_1 = 1$

$L_2 = 3$

$L_n = L_{n-1} + L_{n-2} \quad \forall\ n \geq 2$

Binet's formula

Suppose α, β denote the root of the polynomial $x^2 - x - 1 = 0$.

$\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$

$\alpha + \beta = 1$

$\alpha\beta = -1$

$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$

$L_n = \alpha^n + \beta^n$

Problems

① $F_{2n} = F_n L_n$

Let α, β be the roots of $x^2 - x - 1$.

From Binet's formula,

$$F_{2n} = \frac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta}$$

$$= \frac{(\alpha^n + \beta^n)(\alpha^n - \beta^n)}{\alpha - \beta}$$

$$= L_n F_n$$

② $F_{n+2} - F_{n-2} = L_n \quad \forall\ n \geq 3$

From Binet's Formula,

$$F_{n+2} - F_{n-2} = F_{n+1} + F_n - F_{n-2}$$

$$= F_{n+1} + F_{n-1} + F_{n-2} - F_{n-2}$$

$$= F_{n+1} + F_{n-1}$$

$$= \frac{\alpha^{n+1} - \beta^{n+1} + \alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}$$

$$= \frac{\alpha^n(\alpha + 1/\alpha) - \beta^n(\beta + 1/\beta)}{\alpha - \beta}$$

$$= \frac{\alpha^n(\alpha + 1/\alpha) + (-1)^n \alpha^{-n}(\alpha + 1/\alpha)}{\alpha + 1/\alpha}$$

$$= \alpha^n + (-1)^n \alpha^{-n}$$

$$= \alpha^n + (-\alpha)^{-n}$$

$$= \alpha^n + \beta^n$$

$(\alpha^n + \beta^n)(\alpha - \beta)$
$= \alpha^{n+1} + \alpha\beta^n - \alpha^n\beta - \beta^{n+1}$

$\alpha\beta = -1$

$\beta = -1/\alpha$

3. $F_{n+1}^2 + F_n^2 = F_{2n+1}$

$$\frac{(\alpha^{n+1} - \beta^{n+1})^2 + (\alpha^n - \beta^n)^2}{(\alpha - \beta)^2}$$

$$= \frac{\alpha^{2(n+1)} + \beta^{2(n+1)} - 2\alpha^{n+1}\beta^{n+1} + \alpha^{2n} + \beta^{2n} - 2\alpha^n\beta^n}{(\alpha - \beta)^2}$$

$$= \frac{\alpha^{2n}(\alpha^2+1) + \beta^{2n}(\beta^2+1) - 2\alpha\beta(\alpha^n\beta^n) - 2(\alpha^n\beta^n)}{(\alpha-\beta)^2}$$

$$= \frac{\alpha^{2n}(\alpha^2+1) + \beta^{2n}(\beta^2+1)}{(\alpha-\beta)^2}$$

$$= \frac{\alpha^{2n+1}(\alpha + 1/\alpha) + \beta^{2n+1}(\beta + 1/\beta)}{(\alpha-\beta)^2}$$

$=$

$= F_{2n+1}$

Fermat Numbers

$f_n = 2^{2^n} + 1 \quad \forall\, n \geq 1$

$f_0 = 3$

$f_1 = 5$

$f_2 = 17$

$f_3 = 257$

$f_4 = 65537$, $f_5 = 4294967297$

- Prime numbers of the form $2^{2^n} + 1$ are called Fermat primes.
- Fact:

  Any prime divisor of f_n will have the form $k 2^{n+2} + 1 \quad \forall\, n \geq 2$

Eg: $f_4 = 65537$

$\sqrt{f_4} \leq 256$

Primes of read form $64k + 1$

$193 \nmid 65537$

$\therefore f_4$ is a prime.

Fermat numbers can also be defined recursively:

$$f_n = f_{n-1}^2 - 2f_{n-1} + 2$$
$$= (f_{n-1} - 1)^2 + 1$$

Greatest Common Divisor (GCD)

GCD of two integers a and b is defined to be the largest positive divisor of a and b. It is denoted by (a, b).

Facts:

$(a, -b) = (-a, b) = (a, b) = (-a, -b)$

We restrict ourselves to $\mathbb{W}$.

(a and b are not 0 simultaneously)

Note: $(a,0) = a$.

Symbolically,

$a, b \in \mathbb{N}$, $d \in \mathbb{N}$

Then $d = (a,b)$ if the following are satisfied.

(i) $d \mid a$ and $d \mid b$

(ii) $d' \mid a$ and $d' \mid b \Rightarrow d' \leq d$

Properties:

Suppose $d = (a,b)$. Then

(i) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (They are relatively prime).

(ii) $d = (a, a-b)$

Proof of (i)

Given $d = (a,b)$

Suppose $d' = \left(\frac{a}{d}, \frac{b}{d}\right)$

Then $d' \mid \frac{a}{d}$ and $d' \mid \frac{b}{d}$

$\Rightarrow dd' \mid a$ and $dd' \mid b$

But $d = (a,b)$

$\Rightarrow dd' \leq d$

$\therefore \boxed{d' \leq 1}$ d' can only be 1.

Proof of (ii)

Given $d = (a,b)$

Suppose $d' = (a, a-b)$

$\Rightarrow d' \mid a$ and $d' \mid a-b$

$\Rightarrow d' \mid a-(a-b)$

$\Rightarrow d' \mid b$

$\therefore d' \leq d \longrightarrow (1)$

Also

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid a$ and $d \mid a-b$

But $d' = (a, a-b)$

$\therefore d \leq d' \longrightarrow (2)$

$\therefore \boxed{d = d'}$

Results

① $\forall n \geq 2 \quad (F_n, F_{n+1}) = 1$

We can use the equation $F_{n-1} F_{n+1} - F_n^2 = (-1)^n$

Let $d = (F_n, F_{n+1})$

$\Rightarrow d \mid F_n, \; d \mid F_{n+1}$

$\Rightarrow d \mid F_n^2, \; d \mid F_{n-1} F_{n+1}$

$\Rightarrow d \mid (-1)^n$

$\therefore \boxed{d = 1}$

Method 2 : Induction

We proceed by induction :

$n = 2: \quad (F_2, F_3) = (1, 2) = 1$

Assume it is true for $n = k$:

$(F_k, F_{k+1}) = 1$

We show for $n = k+1$

$d = (F_{k+1}, F_{k+2})$

$= (F_{k+1}, F_k + F_{k+1})$

$= (F_{k+1}, -F_k)$ — ? $(a,b) = (a, a-b)$

$= (F_{k+1}, F_k)$

$= (F_k, F_{k+1})$

$= 1$.

GCD of Fermat numbers

① $(f_n, f_m) = 1$ if $m \neq n$. Ex: Induction

Use $f_0 f_1 \dots f_{n-1} = f_n - 2$

Proof:

, $m \neq n$

WLOG, let $m > n$.

$f_0 f_1 \dots f_n f_{n+1} \dots f_{m-1} = f_m - 2$

let $d = (f_n, f_m)$

Then $d \mid f_n$, $d \mid f_m$

$\Rightarrow d \mid 2$

$\therefore d = 1$ or 2.

But d has to be odd. (Cos f_n is odd)

A theorem of Euclid:

Let $a, b \in \mathbb{N}$, $d = (a,b)$.

Then $\exists \alpha, \beta \in \mathbb{Z}$ st $d = \alpha a + \beta b$

(GCD is a linear combination).

Proof:

$$S = \{ xa + yb : \begin{matrix} x, y \in \mathbb{Z} \\ xa + yb \in \mathbb{Z}_{>0} \end{matrix} \}$$

(i) $S \neq \phi$.

$a = 1 \cdot a + 0 \cdot b$

$\therefore a \in S$

$\Rightarrow S \neq \phi$

We can now use WOP:

$S \subseteq \mathbb{N}$, $S \neq \phi$.

By WOP, S has a least element d.

$d = \alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$.

Claim:

$d = (a, b)$

(i) $a = dq + r$, $0 \leq r < d$.

$r = a - dq$

$d = \alpha a + \beta b$

$\Rightarrow r = a - q(\alpha a + \beta b)$

$= a(1 - q\alpha) - q\beta b$

If $0 < r < d$, $r \in S$

$\rightarrow\leftarrow$

$\therefore r = 0$

$\Rightarrow d \mid a$

Ily, $d \mid b$.

(ii) To show:

$d' \mid a$ and $d' \mid b \Rightarrow d' \leq d$

$d' \mid a$ and $d' \mid b$

$\Rightarrow d' \mid \alpha a + \beta b$

$\Rightarrow d' \mid d$

$\Rightarrow \boxed{d' \leq d}$

Corollaries

① $(a,b) = 1 \iff \exists\ \alpha, \beta \in \mathbb{Z}$ st $1 = \alpha a + \beta b$

$\Rightarrow$ is trivial.

$\leftarrow$ Given $\alpha a + \beta b = 1$ To show: $(a,b) = 1$

Let $d = (a,b)$

$\Rightarrow d \mid a,\ d \mid b$

$\Rightarrow d \mid \alpha a + \beta b$

$\Rightarrow d \mid 1$

$\Rightarrow \boxed{d = 1}$

② $\gcd(a,b) = 1,\ \gcd(a,c) = 1 \Rightarrow \gcd(a, bc) = 1$

$\Rightarrow 1 = x_1 a + y_1 b \longrightarrow ①$

and $1 = x_2 a + y_2 c \longrightarrow ②$

$1 = x_1 x_2 a^2 + x_2 y_1 ab + x_1 y_2 ac + y_1 y_2 bc$

$1 = (x_1 x_2 a - x_2 y_1 b + x_1 y_2 c)\, a + (y_1 y_2)\, bc$

$\therefore (a, bc) = 1.$

2.01.24

③ $a|c$, $b|c$ and $(a,b)=1 \Rightarrow ab|c$

$a|c \Rightarrow c = k_1 a$

$b|c \Rightarrow c = k_2 b$

$(a,b) = 1$

$\Rightarrow ax + by = 1$

$\Rightarrow cax + cby = c$

$\Rightarrow ax(k_2 b) + by(k_1 a) = c$

$ab(k_2 x + k_1 y) = c$

$\Rightarrow ab|c$

④ $a|bc$ and $(a,b)=1 \Rightarrow a|c$

$a|bc \Rightarrow \exists\, r \in \mathbb{N}$ st $bc = ra$

$(a,b) = 1$

$ax + by = 1$

$acx + bcy = c$

$acx + bray = c$

$a(cx + bry) = c \rightarrow a|c$

5. p is a prime, $p|ab \Rightarrow p|a$ or $p|b$.

Proof:

p is a prime,

$p|ab$

If $p|a$, we are done.

If $p \nmid a$, $(p,a)=1$

$\Rightarrow p|b$

GCD of n integers

Suppose $a_1, a_2, \ldots, a_n \in \mathbb{N}$.

GCD of $\{a_i\}_{i=1}^{n}$ is defined as the largest positive integer such that $d \mid a_i \quad \forall\ i = 1:n$

Recursive relation

$$d = (a_1, a_2, \ldots, a_n)$$

$$= ((a_1, \ldots a_{n-1}), a_n)$$

$$d_1$$

$$\therefore d = (d_1, a_n)$$
$$d_2$$

To prove: $d_2 = d$

(i) $d_2 = (d_1, a_n)$

$\Rightarrow d_2 \mid d_1$ and $d_2 \mid a_n$

$\Rightarrow d_2 \mid a_i \quad \forall\ i = 1:n-1$

$\Rightarrow d_2 \mid d \longrightarrow (1)$

(ii) $d \mid a_i \quad \forall\ i = 1:n$

$\Rightarrow d \mid a_i \quad \forall\ i = 1:n-1, \quad d \mid a_n$

$\Rightarrow d \mid d_1, \quad d \mid a_n$

$\Rightarrow d \mid d_2$

Complete this :

5.02 . 24

Problems

① $(Ka, Kb) = K(a,b)$

② If $(a,b) = 1$, PT: $(a+2b, 2a+b) = 1$ or 3.

Proof:

$(a,b) = 1$

$\rightarrow \exists x, y \in N$ s.t. $ax + by = 1$

Suppose $d = (a+2b, 2a+b)$ $\rightarrow$ (i)

We show that $d=1$ or $d=3$

From (i),

$d \mid a+2b$, $d \mid 2a+b$

$\Rightarrow d \mid 2(a+2b) - (2a+b)$

$\Rightarrow d \mid 3b$

Ily $d \mid 3a$

$\Rightarrow d \mid (3a, 3b)$

$\Rightarrow d \mid 3(a,b)$

$\Rightarrow d \mid 3.$

If $d=1$, we are done.

If $d \neq 1$, $d \geq 2$

$\Rightarrow$ d has a prime divisor (say p)

$\Rightarrow p \mid d$ and $p \mid 3b$

$\Rightarrow p \mid 3$ or $p \mid b$.

③ If $(a,b) = 1$

$(a^2+b^2, a^2+2ab) = 1$ or 5

Suppose $d = (a^2+b^2, a^2+2ab)$

$(a,b) = 1$

$\Rightarrow ax + by = 1$

We show that $d=1$ or 5.

$\Rightarrow d \mid a^2+b^2$, $d \mid a^2+2ab$

$\Rightarrow d \mid b^2 - 2ab$

$\Rightarrow d \mid b(b-2a)$

Claim : $(d,a) = 1 = (d,b)$

Suppose $d_1 = (d,a)$

If $d_1 \geq 1 \Rightarrow p \mid d_1$

$d_1 \mid d$ and $d_1 \mid a$.

$\Rightarrow p \mid d$ and $p \mid a$

$\Rightarrow p \mid a^2+b^2$, $p \mid a$

$\Rightarrow p \mid b^2$, $p \mid a$

$\Rightarrow p \mid b$, $p \mid a$ $\rightarrow\leftarrow$

Now, $d \mid b(b-2a)$, $d \mid 2(a+2b)$

$\Rightarrow d \mid b-2a$, $d \mid a+2b$

$\Rightarrow d \mid 5b$

$\Rightarrow d \mid 5$

$\therefore d = 1, 5$

Check the argument.

Fundamental Theorem of Arithmetic

Any positive integer ≥ 2

① is either a prime

② can be expressed as a product of primes.

This representation is unique upto the order in which they occur.

(In other words, $\mathbb{Z}$ is a UFD!)

Proof

- $P(n)$ be the statement that n is a prime or can be expressed as a product of primes.
- $P(n)$ is true $\forall\ n \geq 2$.
- Clearly, $P(2)$ is true.

Let $P(2), P(3), \ldots, P(k)$ are true.

$P(k+1)$:

- If $(k+1)$ is a prime, we are done.
- $k+1$ is not a prime.

Then $\exists\ a, b$ st $k+1 = ab \quad 1 < a, b < k+1$.

Since $1 < a, b < k+1$

a and b are either primes or can be written as a product of primes.

By strong PMI, $P(n)$ is true $\forall\ n \geq 2$.

It remains to show that the factorization is unique.

Suppose $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$.

WLOG, let $r \leq s$

each p_i and q_i are primes.

also $p_1 \leq p_2 \leq \ldots \leq p_r$

$q_1 \leq q_2 \leq \ldots \leq q_s$.

We will show

① $r = s$

② $p_i = q_i \quad \forall i$

Suppose

$p_1 \mid q_1 \cdots q_s$

$\Rightarrow p_1 \mid q_k$ for some k.

$\therefore p_1 = q_k \geq q_1$

$\therefore p_1 \geq q_1$

By symmetry $q_1 \mid p_1 p_2 \cdots p_r$

$\Rightarrow q_1 \mid p_t$ for some t

$q_1 = p_t \geq p_1$

$\therefore q_1 \geq p_1$

$\therefore \boxed{p_1 = q_1}$

Now we have $p_2 \cdots p_r = q_2 \cdots q_s$

Proceed in a similar fashion.

We can cancel upto r terms.

We will be left with

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

This can't happen

$\therefore r = s$.

Canonical representation

$$\boxed{n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}, \quad n \geq 2$$

($p_1, p_2, \ldots, p_r$ distinct)

- p_i are primes
- $k_1, k_2, \ldots, k_r$ are positive integers.

$6 \times 5 \times 4$
$= 2^3 \times 3 \times 5$

Eg:

No. of divisors of 120 $= 2^3 \times 3^1 \times 5^1$

$= 4 \times 2 \times 2$

$= 16$

7.02.24

Problem

Find the number of trailing zeros of 234!

Soln:

$234! = 2^a 5^b c$

where $2, 5 \nmid c$

No. of trailing zeros $= \min(a, b)$

Multiples of $5 \leq 234 = \left\lfloor \frac{234}{5} \right\rfloor = 46$

Multiples of $2 \leq 234 = \left\lfloor \frac{234}{2} \right\rfloor = 117$

Multiples of $25 \leq 234 = 9$

Multiples of $125 \leq 234 = 1$

$b = 46 + 9 + 1 = 56$

Given $n \in \mathbb{N}$, highest power of a prime p dividing $n! = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$

Formula for GCD

Suppose

$a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ $\quad r_i, s_i \geq 0$

$b = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$

$\gcd(a, b) = \prod_{i=1}^{k} p_i^{\min(r_i, s_i)}$

Eg: (168, 180)

$168 = 2^3 \times 3^1 \times 5^0 \times 7^1$

$180 = 2^2 \times 3^2 \times 5^1 \times 7^0$

$(168, 180) = 2^2 \times 3^1 \times 5^0 \times 7^0$

$= 12$

Prop:

Given any prime $p > 2$, $p = 4k+1$ or $p = 4k+3$

Then there are infinitely many primes of the form $4k+3$.

Suppose $\exists$ only finitely many such primes : $p_0 (= 3), p_1, \ldots, p_k$. $N = 4p_1p_2 \cdots p_k + 3$ is also of this form.

Case-1 : N is not a prime. If so $N > p_k$, greatest such prime $\Rightarrow\Leftarrow$

Case-2: N is composite. N has to be odd. The factors of N are also odd: They have to be of the form $4n+1$ or $4n+3$

- Rule out $4n+1$ [product of any 2 integers of this form is of form $4n+1$]
- $\exists$ atleast one prime factor $p = 4k+3$

Case 2.1 : $p = p_0 = 3$

$\Rightarrow 3 \mid N$, $3 \nmid 3$

$\Rightarrow 3 \mid N-3 \Rightarrow 3 \mid 4p_1p_2 \cdots p_k$ $\Rightarrow\Leftarrow$

Case 2.2 : $p = p_i$, $1 \leq i \leq k$

$\Rightarrow p \mid N$ and $p \mid p_1 \cdots p_i p_{i+1} \cdots p_k$

$\Rightarrow p \mid 3$

$\Rightarrow\Leftarrow$

$\therefore$ There are inf many such primes.

Dirichlet's Theorem

Let $a, b \in \mathbb{N}$ and $(a,b) = 1$. Then the sequence $a, a+b, a+2b, \ldots$ contains infinitely many primes.

- If $a=1, b=4$ $\Big\}$ $\Rightarrow$ previous result.
  $a=3, b=4$
- $(a,b)=1$ is a necessary condition.

Least Common Multiple (LCM)

Let $a, b \in \mathbb{N}$. l is called lcm of a and b if

① $a \mid l$, $b \mid l$

② $a \mid l'$, $b \mid l' \Rightarrow l \leq l'$

Notation: $l = [a,b]$

Result:

Suppose $a \mid l'$, $b \mid l'$.

$\Rightarrow l \mid l'$

Let $l = [a,b]$.

Suppose $l' = lq + r \quad 0 \leq r < l$.

Enough to show $r = 0$.

We have $a \mid l'$, $a \mid l$

$\Rightarrow a \mid r$

Similarly, $b \mid r$. $\quad 0 < r < l$.

$\Rightarrow$ But $r = 0$.

$\Rightarrow l \mid l'$.

$$a = p_1^{r_1} \cdots p_k^{r_k}$$

$$b = p_1^{s_1} \cdots p_k^{s_k}$$

$$[a,b] = \prod_{i=1}^{k} p_i^{\max(r_i, s_i)}$$

$$[a,b] = \frac{ab}{(a,b)}$$

Proof

$$(a,b) = \prod_{i=1}^{k} p_i^{\min(r_i, s_i)}$$

$$[a,b] = \prod_{i=1}^{k} p_i^{\max(r_i, s_i)}$$

$$(a,b)[a,b] = \prod_{i=1}^{k} p_i^{r_i + s_i}$$

$$= \left[\prod_{i=1}^{k} p_i^{r_i}\right]\left[\prod_{i=1}^{k} p_i^{s_i}\right]$$

$$= ab$$

Result

① LCM of 2 distinct primes p, q is pq

② $[ka, kb] = k[a,b]$

Generalized LCM

Let $\{a_i\}_{i=1}^{n} \in \mathbb{N}$, $n \geq 3$

$$[a_1, \ldots a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$$

Problems

The sum of twin primes is divisible by 12. $p > 3$

$(p, p+2)$ are twin primes.

$p + (p+2) = 2(p+1)$

Sufficient to show $(p+1)$ is divisible by 6.

Consider p, $p+1$, $p+2$

We have either $3 \mid p$ or $3 \mid p+1$ or $3 \mid p+2$

$3 \mid p$ can't happen.

$3 \mid p+2$ can't happen as well

$\therefore$ $3 \mid p+1$

$\therefore$ Also p prime $\Rightarrow 4 \mid 2(p+1)$

$\Rightarrow 12 \mid 2(p+1)$

Done

9.02.24

Problems

① Find the smallest positive integer $n \geq 2$ st n is a square, cube and fifth power of some positive integers.

$$n = a^2 = b^3 = c^5.$$

$\text{lcm}(2,3,5) = 30$

Let $n = a^k$

$2 \mid k$, $3 \mid k$ and $5 \mid k$

Smallest such $k = 30$.

② Find the smallest positive integer st $\frac{n}{2}$ is a square, $\frac{n}{3}$ is a cube and $n/5$ is a 5^{th} power

$$n = 2a^2 = 3b^3 = 5c^5$$

Suppose $n = 2^a 3^b 5^c$, $a, b, c \neq 0$.

$\frac{n}{2}$ is a square $\Rightarrow 2 \mid a-1,\ 2 \mid b,\ 2 \mid c$

$\frac{n}{3}$ is a cube $\Rightarrow 3 \mid a,\ 3 \mid b-1,\ 3 \mid c$

$\Rightarrow 5 \mid a,\ 5 \mid b,\ 5 \mid c-1$

$\therefore a = 15$

$b = 10$

$c = 6$.

$$\boxed{n = 2^{15} 3^{10} 5^6.}$$

Diophantine Equations (LDEs)

Any equation of the type $ax + by = c$, $a, b \in \mathbb{Z}$ are called linear diophantine equation in 2 variable

- If $(x,y) \in \mathbb{R}^2$, we have inf. many solutions.
- We look for 'integral solutions'
  - → Existence
  - → If so, how many?
  - → Restrictions under which $\exists$ a soln.

Theorem:

- The LDE $ax+by=c$ is solvable $\Leftrightarrow \gcd(a,b) \mid c$.
- If (x_0, y_0) is a particular soln. of this LDE, then any other soln can be written as

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{Z}$$

d is gcd.

Digression

Lattices:

- Points on $\mathbb{R}^2$ (x,y) where $x, y \in \mathbb{Z}$ are lattice points
- When does a line have infinitely many lattice points?

Proof:

$\Rightarrow$ Suppose $ax+by=c$ has a soln. in $\mathbb{Z}$, say (x_0, y_0).

Then $ax_0 + by_0 = c$.

Since $d = (a,b)$

→ $d \mid a$, $d \mid b$

$\therefore$ $d \mid ax_0 + by_0$

$\Rightarrow$ $d \mid c$.

$\leftarrow$ Suppose $d \mid c$.

$\Rightarrow c = ed$, for some $e \in \mathbb{Z}$

We have to construct a soln for $ax + by = c$

$d = (a, b)$.

$\therefore \exists\, x_0, y_0 \in \mathbb{Z}$ st $ax_0 + by_0 = d$

$\Rightarrow aex_1 + bey_1 = ed$

$= c$

$\Rightarrow (ex_1, ey_1) \in \mathbb{Z}^2$ is soln

$\therefore ax + by = c$ is solvable.

② Suppose (x_0, y_0) is a particular soln. of $ax + by = c$. $\rightarrow$ ④

Suppose (x_1, y_1) is any other soln. of ④

We have

$ax_0 + by_0 = c \rightarrow ①$

$ax_1 + by_1 = c \rightarrow ②$

② - ① $\Rightarrow a(x_1 - x_0) + b(y_1 - y_0) = 0$

$a(x_1 - x_0) = b(y_0 - y_1)$

$d = (a, b)$ $\therefore$ $\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1)$

$\Rightarrow \frac{a}{d} \mid \frac{b}{d}(y_0 - y_1)$

But $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

$\Rightarrow \frac{a}{d} \mid y_0 - y_1$

Let $y_0 - y_1 = \frac{a}{d} t$ for some $t \in \mathbb{Z}$.

$y_1 = y_0 - \frac{a}{d} t$

But y_1 is arbitrary.

$$\therefore \boxed{y = y_0 - \frac{a}{d}t}$$

To find x

$$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_1 - y_0)$$

$$= \frac{b}{d}\left(\frac{a}{d}\right)t$$

$$\Rightarrow \boxed{x_1 = x_0 + \frac{b}{d}t}$$

Problems:

Find all solutions of LDE $15x + 21y = 39$.

$a = 15$

$b = 21$

$d = (15, 21) = 3$

$3 \mid 39 \Rightarrow$ solvable.

$\exists\, x, y$ st

$$3 = 15(3) + 21(-2)$$

$$39 = 15(39) + 21(-26)$$

$x_0 = 39$

$y_0 = -26$

$$\therefore x = 39 + \frac{21}{3}t = 39 + 7t$$

$$y = -26 - \frac{15}{3}t = -26 - 5t$$

$$\{(39 + 7t, -26 - 5t) \;,\; t \in \mathbb{Z}\}$$

$5x + 7y = 13$

$d = (5, 7) = 1 \mid 13$

$13 = 5(1) + 7(3)$

$(1, 3)$ is a soln

$$\boxed{x = 1 + 7t,\; y = 3 - 5t}$$

Example

$\mathbb{N}$

Divide 100 into two summands, where one is div by 7, and other is by 11

Find solutions for

$$7x + 11y = 100$$

$a = 7$

$b = 11$

$d = (7, 11) = 1$.

$1 \mid 100 \Rightarrow$ Solvable.

$$1 = 7(-3) + 11(2)$$

$$100 = 7(-300) + 11(200)$$

$$(x_0, y_0) = (-300, 200)$$

$$x = -300 + 11t$$

$$y = 200 - 7t$$

We need

$-300 + 11t \geq 0$ & $200 > 7t$

$t \geq \frac{300}{11}$ $\Rightarrow t < \frac{200}{7}$

$\geq 27. \ldots$ < 28.5

$\boxed{t = 28}$ $\boxed{t = 28}$

$\therefore x = -300 + 11(28)$

$= 8$

$y = 4$

Eg. 3

If a mango worth 5 coin and a pple worth 3 coins and $\frac{1}{3}$ orange worth 1 coin. How many mango, apple oranges totalling 100 can be bought with 100 coins?

$x \to$ mango

$y \to$ apple

$z \to$ orange

$$x + y + z = 100 \Rightarrow z = 100 - (x+y)$$

$$5x + y + \frac{z}{3} = 100$$

$$15x + 3y + z = 300$$

$$15x + 3y + 100 - x - y = 300$$

$$14x + 8y = 200$$

$$7x + 4y = 100$$

$$(x_0, y_0) = 100$$

$$x = 8 + 4t$$

$$y = 11 - 7t \quad \text{for some } t \in \mathbb{Z}.$$

$x \geq 1 \Rightarrow 8 + 4t \geq 1$

$$4t \geq -7$$

$$t \geq -7/4 = -1.75$$

$$\boxed{t \geq -1}$$

$y \geq 1 \Rightarrow 11 - 7t \geq 1$

$$-7t \geq -10$$

$$t \leq \frac{10}{7} = 1\ldots$$

$$\boxed{t \leq 1}$$

$$\boxed{t = -1, 0, 1}$$

Solns are $(12, 4, 84)$

$(8, 11, 81)$

$(4, 18, 78)$

Result.

$ax + by = c$ has a soln $\Leftrightarrow (a,b) \mid c$.

If it's solvable, then it has infinitely many solutions.

Euler's method

$$1076x + 2076y = 3076$$

$$(1076, 2076) = 4$$

So, soln's exist.

Use division algorithm:

$$x = \frac{-2076y + 3076}{1076}$$

$$x = -y + 2 + \underbrace{\left(\frac{-1000y + 924}{1076}\right)}_{u}$$

Say, $-1000y + 924 = 1076u$

$\Rightarrow 1076u + 1000y = 924$

$$y = \frac{924 - 1076u}{1000}$$

$$= -u + \underbrace{\left(\frac{924 - 76u}{1000}\right)}_{v}$$

$$\frac{924 - 76u}{1000} = v$$

$\Rightarrow 1000v = 924 - 76u$

$76u + 1000v = 924$

$$u = \frac{924 - 1000}{76}$$

$= -13V + 12 + \left(\frac{-12V+12}{76}\right)$

$w = \frac{-12V+12}{76}$

$12V + 76w = 12$

$V = 1 - 6w + \frac{w}{3}$

let $w = 3t$

Now back substitute.

$x = 519t - 1$

$y = -264t + 2 \quad , \quad t \in \mathbb{Z}$

LDE of the form

① $F_{n+1}\,x + F_n\,y = c$

Always $(F_{n+1}, F_n) = 1$

$\Rightarrow$ solvable.

$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$

Suppose n is even

$\Rightarrow F_{n+1}F_{n-1} - F_n^2 = 1$

$F_{n+1}(cF_{n-1}) + F_n(-cF_n) = c$

$x_0 = cF_{n-1}$

$y_0 = -cF_n$

is a particular soln.

Suppose n is odd.

$F_{n+1}F_{n-1} - F_n^2 = -1$

$F_{n+1}(-cF_{n-1}) + F_n(cF_n) = c$

$x_0 = -cF_{n-1}$

$y_0 = cF_n$

is a soln.

Eg: $34x + 21y = 17$

$F_9F_7 - F_8^2 = 34.13 - 21^2$

$= (-1)^8$

$c = 17$

$x_0 = cF_7$

$y_0 = -cF_8$

LDE in > 2 variables

The LDE $\sum_{i=1}^{n} a_i x_i = c$ has a soln iff $d = (a_1, \dots a_n) \mid c$.

When solvable, it has inf many solns.

Eg : Solve

$$6x + 8y + 12z = 10$$

$(6, 8, 12) = (6, 4) = 2 \mid 10 \Rightarrow$ inf many soln.

Let $8y + 12z = 4u$ (say)

$6x + 4u = 10$

$6x = -4u + 10$

$x = -\frac{4u}{6} + \frac{10}{6} = 1 + \underbrace{\frac{-4u+4}{6}}_{v}$ $\quad x = 1 + v$

$6v = -4u + 4$

$6v + 4u = 4$

$4u = 4 - 6v$

$u = 1 - \frac{6v}{4}$

$= 1 - \frac{3v}{2}$

Sub $v = 2t$

$u = 1 - \frac{3(2t)}{2}$

$\boxed{u = 1 - 3t}$ $\quad x = 1 + 2t$

Congruent Relation

Let A be a set. Any subset of $A \times A$ is called a relation.

Equivalence Relation

① $aRa \quad \forall a \in A$

② $aRb \Rightarrow bRa$

③ $aRb, bRc \Rightarrow aRc$

$a, b, c \in A$

Let $m \in \mathbb{Z}^+$. a is congruent to b modulo m if $m \mid a-b$.

Notation: $a \equiv b \pmod{m}$

Eg:

$12 \equiv 2 \pmod{5}$

$2 \equiv -3 \pmod{5}$

Define

$a \sim b \Leftrightarrow a \equiv b \pmod{m}$

(i) $a \sim a$

as $m \mid a-a$

(ii) $a \sim b \Rightarrow m \mid a-b$

$\Rightarrow m \mid b-a$

$\Rightarrow b \sim a$

(iii) $a \sim b \Rightarrow m \mid a-b$

$b \sim c \Rightarrow m \mid b-c$

$\Rightarrow m \mid a-b+b-c$

$\Rightarrow m \mid a-c$

$\Rightarrow a \sim c$

'$\sim$' is an eq. relation on $\mathbb{Z}$

$\sim$ induces m equivalence classes [partitions]

$$[i] = \{a \in \mathbb{Z} : a \sim i\}$$

$$= \{a \in \mathbb{Z} : a \equiv i \pmod m\}$$

Classes:

$$[0], [1], \ldots, [m-1]$$

$$\mathbb{Z} = \bigcup_{i=0}^{m-1} [i]$$

Note: ① $a \equiv b \pmod m \iff$ a and b leave same reminder on division by m.

② Suppose $a \equiv b \pmod m$

$c \equiv d \pmod m$

$e \in \mathbb{Z}$

Then $a+c \equiv b+d \pmod m$

$a-c \equiv b-d \pmod m$

$ac \equiv bd \pmod m$

$a+e \equiv b+e \pmod m$

$a^2 \equiv b^2 \pmod m$

$a^n \equiv b^n \pmod m$

Examples

Find the rem when 3^{247} is divided by 17.

$3^3 \equiv 10 \mod 17$

$3^4 \equiv 30 \mod 17$

$\equiv 13 \mod 17$

$3^5 \equiv 5 \mod 17$

$3^6 \equiv -2 \mod 17$

$3^7 \equiv -6 \mod 17$

$3^8 \equiv -8 \mod 17$

$\equiv -1 \mod 17$

$3^4 \equiv -4 \pmod{17}$

$3^8 \equiv -1 \pmod{17}$

$3^{240} \equiv 1 \pmod 7$

$3^{247} \equiv 3^7 \mod 17$

$\equiv -6 \pmod{17}$

$3^{247} \equiv (3^8)^{30} \cdot 3^7$

$\equiv (-1)^{30} 3^7$

$\equiv (-6) \mod 17$

Rem = 11

Prob-2 Finish

16^{53} divided by 7 $\quad 16^{53} = 2^{4\times 53} = 2^{212} \quad \frac{212}{3} = 70 + 2$

$2^3 \equiv 1 \pmod 7$

$(2^{70})^3 \cdot 2^2 \equiv 4 \pmod 7$

Prob-3

$10 \mid 9^{100} - 1$

$9^{100} - 1 \equiv (-1)^{100} - 1$

$\equiv 0 \pmod{10}$

T/F:

If $a \not\equiv 0 \pmod m$

$b \not\equiv 0 \pmod m$

then $ab \not\equiv 0 \pmod m$

is not true in general. But holds when m is a prime.

Result:

If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{\frac{m}{d}}$

where $d = (c, m)$

Proof:

$d = cx + my$

$m \mid ac - bc \Rightarrow m \mid (a-b)c$

$\Rightarrow \frac{m}{d} \mid (a-b)\frac{c}{d}$

$\Rightarrow \frac{m}{d} \mid (a-b)$ $\quad \left(\frac{m}{d}, \frac{c}{d}\right) = 1$

$\Rightarrow a \equiv b \pmod{\frac{m}{d}}$

PT:

$n^4 + 2n^3 + n^2 \equiv 0 \pmod 4 \quad \forall \ n \geq 1$

$n^2(n^2+2n+1) = n^2(n+1)^2$

$\equiv 0 \pmod 4$

As 2 always divides one of $n, n+1$.

No prime of the form $4n+3$ can be expressed as a sum of 2 squares.

Let $p = a^2 + b^2$

$a = 0, 1, 2, 3 \pmod 4$

$b = 0, 1, 2, 3 \pmod 4$

$a^2 = 0, 1$

$b^2 = 0, 1$

$a^2 + b^2 = 0, 1 \pmod 4$

But $p \equiv 3 \pmod 4$

Find unit digit in 1997^{1998} ← 1999.

$1997 \equiv 7 \pmod{10}$

1 2 3 0

7, 9, 3, 1,

$$7^a \equiv \begin{cases} 1 \pmod{10} & a \equiv 0 \pmod 4 \\ 7 & a \equiv 1 \pmod 4 \\ 3 & a \equiv 3 \pmod 4 \\ 9 & a \equiv 2 \pmod 4 \end{cases}$$

$1998 \equiv 2 \pmod 4$

$1998^{1999} \equiv 0 \pmod 4$

$1997^{1998^{1998}} \equiv 1 \pmod{10}$

16.02.24

Complete set of residues

A set of m integers is called complete set of residues modulo m if every integer is congruent modulo m to exactly one of them.

Example:

$S = \{0, 1, 2, \ldots, n-1\}$

Then S is a complete set of residues (modulo n)

$\tilde{S} = \{1, 2, \ldots, n-1, n\}$

is also a complete set of residues.

Equivalently, a set S of m integers is complete set of residues if no two of them are congruent modulo m.

Eg: $S := \{a_1, a_2, \ldots, a_m\}$

$\forall i, j \quad a_i \not\equiv a_j \pmod m$

PT: Any integer will be congruent to exactly one.

Let $a \in \mathbb{Z}$.

Suppose $a \equiv r \pmod{m}$ $\quad 0 \le r \le m-1$

$\exists\ j$ st $a_j \equiv r \pmod{m}$

$\Rightarrow a \equiv a_j \pmod{m}$

Suppose $(a, m) = 1$ and $\{a_1, \dots, a_m\}$ is a complete set of residues mod m. Then $\{aa_1, aa_2, \dots, aa_m\}$ is also a CSR modulo m.

Proof:

Claim: $aa_i \not\equiv aa_j \pmod{m}$

Suppose $aa_i \equiv aa_j \pmod{m}$

$\Rightarrow aa_i - aa_j \equiv 0 \pmod{m}$

$a(a_i - a_j) \equiv 0 \pmod{m}$

$\Rightarrow m \mid a(a_i - a_j)$ $\quad (a, m) = 1$

$\Rightarrow m \mid a_i - a_j$

$\Rightarrow\leftarrow$ (Complete set)

Fact:

$a \equiv b \mod (m_1)$

$a \equiv b \mod m_2$

Then $a \equiv b \mod [m_1, m_2]$

$\to m_1 \mid a-b$

$m_2 \mid a-b$

$\Rightarrow [m_1, m_2] \mid a-b$

$\Rightarrow a \equiv b \mod [m_1, m_2]$

$8 \equiv 2 \pmod 6$ $\quad (6,3) = 6$

$8 \equiv 2 \pmod 3$

Congruence Equations

$$x^2 + x + 1 = 0$$

$$x^2 + x + 1 \equiv 0 \pmod{m}$$

Congruence equations can have

① no soln

② inf many solns

Linear congruence equations

$$ax \equiv b \pmod{m}$$

$a, b \in \mathbb{Z}$.

$\Leftrightarrow ax = b + mk$

$\Leftrightarrow ax - mk = b$

$\Leftrightarrow (a, m) \mid b$

$ax = mk + b$

$ax - mk = b$

$\Rightarrow (a, m) \mid b$.

Problem:

The last $(n+1)$ digits of 5^{2^n} and $5^{2^{n-1}}$ are same, $n \geq 3$.

$$N = 5^{2^{n-1}}$$

$$N^2 = 5^{2^n}$$

To show: $N^2 \equiv N \pmod{10^{n+1}}$

$N^2 \equiv N \pmod{5^{n+1} 2^{n+1}}$

$\Leftrightarrow N^2 \equiv N \pmod{5^{n+1}} \rightarrow ①$

$N^2 \equiv N \pmod{2^{n+1}}$

$① \Rightarrow 5^{n+1} \mid N(N-1)$

Need to prove: $N^2 \equiv N \pmod{2^{n+1}} \quad \forall\ n \geq 3$

i.e., $N \equiv 1 \pmod{2^{n+1}}$

$\underline{n=3}$

$5^{2^{n-1}} = 5^{2^2} = 5^4 = 125$

We proceed by induction.

For $n=3$

$$5^{2^2} = 625$$

$$\equiv 1 \pmod{16}$$

Given: $5^{2^{k-1}} \equiv 1 \mod 2^{k+1}$

To show: $5^{2^k} \equiv 1 \mod 2^{k+2}$

Proof:

$$5^{2^{k-1}} = 1 + m\,2^{k+1}$$

$$5^{2^k} = (1 + m2^{k+1})^2$$

$$= 1 + m^2 2^{2k+2} + 2m\,2^{k+1}$$

$$= 1 + 2^{k+2}(m^2 + m)$$

$$\Rightarrow 5^{2^k} \equiv 1 \mod 2^{k+2}$$

21.02.24

Solving Linear Congruences

$$ax \equiv b \pmod{m}$$

has a soln $\Leftrightarrow (a,m) \mid b$.

Goal: Count # of distinct solutions

Eg:

$$2x \equiv 1 \pmod 3$$

$x=2$, $x=5$ are solns.

But both represent the 'same' thing.

Thm:

The linear congruence $ax \equiv b \pmod m$ is solvable $\Leftrightarrow (a,m) \mid b$. If so, then there are exactly d incongruent solutions.

Proof:

If $ax \equiv b \pmod{m}$ is solvable

$\Rightarrow \exists\, x_0$ s.t. $ax_0 - my = b$

$\Rightarrow (a, -m) \mid b$

$\Rightarrow (a, m) \mid b$

$\Leftarrow$

Second part:

Let x_0 be a solution to $ax \equiv b \pmod{m}$

Then $x = x_0 + \frac{m}{d}t$, $y = y_0 - \frac{a}{d}t$

where $ax_0 \equiv b \pmod{m}$, $b \in \mathbb{Z}$

Suppose $x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}$

$\Leftrightarrow \frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod{m}$

$\Leftrightarrow \frac{m}{d}(t_1 - t_2) = mk$, for some k.

$\Leftrightarrow t_1 = t_2 + dk$

$\Leftrightarrow \boxed{t_1 \equiv t_2 \pmod{d}}$

$\therefore$ choices for d are $\{0, 1, \ldots, d-1\}$

$x = x_0 + \frac{m}{d}t$; $\boxed{t = 0 \text{ to } d-1}$

Example:

$$12x \equiv 48 \pmod{18}$$

$(12, 18) = 6 \mid 48$

Given linear congruence is solvable

$x_0 = 4$ is a particular soln:

$$x = 4 + \frac{18}{6} t \qquad t = 0, 1, 2, 3, 4, 5$$

$$= 4 + 3t$$

$\therefore \quad x = 4, 7, 10, 13, 16, 19.$

Corollary:

If $(a, m) = 1$, then $ax \equiv b \pmod{m}$ has a unique soln (upto congruence)

Problem:

Show that $11 \cdot 14^n + 1$ is composite.

Proof:

$$\lambda = 1 + 11 \cdot 14^n \equiv 2(2^n) + 1 \pmod{3}$$

$$= 2^{n+1} + 1 \pmod{3}$$

$$= (-1)^{n+1} + 1 \pmod{3}$$

If n is even, $\lambda \equiv 0 \pmod{3}$

$$11 \cdot 14^n + 1 \equiv (-1)^n + 1 \pmod{5}$$

n is odd

$$\equiv 0$$

Modular inverse.

Consider $ax \equiv 1 \pmod{m}$

Let $(a,m) = 1$. Then soln of this congruence is called its modular inverse.

Let x_0 be the least residue modulo m st $ax_0 \equiv 1 \pmod{m}$.

Then $\boxed{x_0 = a^{-1}}$ is called the modular inverse

Consider $5x \equiv 1 \pmod{7}$

$x = \ldots, -11, -4, \textcircled{3}, 10, \ldots$.

③ is called modular inverse of a.

Diophantine Equation

We can solve diophantine equations using linear congruences.

Eg: $6x + 9y = 15 \rightarrow ①$

$6x \equiv 15 \pmod{9} \rightarrow ②$

Let's concentrate on ②.

$2x \equiv 5 \pmod{3}$ & $(2,3) = 1$

$x = 1$ is a soln.

$x = 1 + 3t$

$6(1+3t) + 9y = 15$

$9y = 15 - 6 - 18t$

$= 9 - 18t$

$\boxed{y = 1 - 2t}$

$(x,y) = (1+3t, 1-2t)$, $t \in \mathbb{Z}$.

Problem :

Find the smallest positive integer $a > 2$ st

$2 \mid a$, $3 \mid a+1$, $4 \mid a+2$, $5 \mid a+3$, $6 \mid a+4$

$\Rightarrow a = 2k$

$2k+1 \equiv 0 \pmod 3$

$2k \equiv -1 \mod 3$

$\equiv 2 \mod 3$

$\therefore \boxed{k \equiv 1 \mod 3}$

$\Rightarrow k = 1+3l$, for some $l \in \mathbb{Z}$.

$a = 2k = 2(1+3l)$

$\boxed{a = 2+6l}$

$4 \mid a+2$

$\Rightarrow 2+6l+2 \equiv 0 \pmod 4$

$\Rightarrow 6l \equiv 0 \pmod 4$

$\Rightarrow \boxed{l = 2s}$

$\therefore a = 2+6l = \boxed{2+12s}$

$5 \mid a+3$

$2+12s+3 \equiv 0 \pmod 5$

$12s \equiv -5 \pmod 5$

$12s \equiv 0 \pmod 5$

$\boxed{s = 5t}$

$a = 2+12s$

$\boxed{a = 2+6n}$

$6 \mid a+4$

$2+60n+4 \equiv 0 \pmod 6$

$60n \equiv 0 \pmod 6$

$\Rightarrow a = 2+60n$, $n \in \mathbb{Z}^+$ $\therefore \boxed{a = 62}$

Applications of congruences

① Consider $N = n_k n_{k-1} \dots n_0$

$$= n_k \times 10^k + n_{k-1} \times 10^{k-1} + \dots + n_1 \times 10 + n_0$$

$$= \sum_{i=0}^{k} n_i 10^i$$

We will discuss divisibility by 10.

Divisibility by 10

N is divisible by 10 $\Leftrightarrow$ $10 | n_0$

$\Leftrightarrow$ unit digit div. by 10.

- Same holds for 5, ie, (unit digit div by 5)

Div. by 2^i $(i \geq 1)$

N is divisible by 2^i $\Leftrightarrow$ iff the no. formed by last i digits is divisible by 2^i

Div by 3

N is divisible by 3 (9) iff sum of digits of N is divisible by 3 (9)

Div by 4

$$N = n_k \times (-1)^k + n_{k-1} (-1)^{k-1} + \dots \pmod{11}$$

$$\Rightarrow \sum_{2|i} n_i - \sum_{2 \nmid j} n_j \equiv 0 \pmod{11}$$

Problem:

Show that any number of the form abcabc is divisible by 7, 11 and 13.

$$abcabc = a(10^5 + 10^2) + b(10^4 + 10) + c(10^3 + 1)$$

$$= a(10^2)(1001) + b(10)(1001) + c(1001)$$

$$= (1001)(100a + 10b + c)$$

$$= (abc)(1001)$$

Now $1001 = 7 \times 143$

$= 7 \times 11 \times 13$

done.

Chinese Remainder Theorem

Consider the foll. system

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_n \pmod{m_n} \longrightarrow (1)$$

where $(m_i, m_j) = 1$, $i \neq j$

This system has a unique sol^n modulo $m_1 m_2 \ldots m_n$

Proof:

let $M = \prod_{i=1}^{n} m_i$

Define $M_i = \frac{M}{m_i}$

One can verify that $(M_i, m_i) = 1$. $\forall\ i = 1:n$

$\therefore \exists$ a soln to the eqn.

$$M_i y \equiv 1 \pmod{m_i} \longrightarrow (2)$$

Call this sol^n y_i

Now take $x = \sum_{i=1}^{n} a_i M_i y_i$

This x satisfies (1)

Consider

$$x = a_1 M_1 y_1 + \cdots + a_n M_n y_n \pmod{m_i}$$

$$\therefore \equiv a_i M_i y_i \pmod{m_i}$$

$$\equiv a_1 \pmod{m_i} \quad \text{(From ②)}$$

$\forall\ i = 1, 2, \ldots, n.$

Left to show: unique modulo $m_1 m_2 \ldots m_n$.

Suppose $\exists$ 2 solns: x_0, x_1 of ①

$$\therefore \quad x_0 \equiv a_i \pmod{m_i}$$

$$x_1 \equiv a_i \pmod{m_i} \qquad \forall\ i = 1, 2, \ldots, n.$$

$$\Rightarrow \quad x_0 \equiv x_1 \pmod{m_i} \qquad \forall\ i = 1, \ldots n$$

We have $(m_i, m_j) = 1$

$$\Rightarrow m_1 m_2 \ldots m_n \mid x_0 - x_1$$

$$\therefore \quad x_0 \equiv x_1 \pmod{\prod_{i=1}^{n} m_i}$$

Example

$$x \equiv 1 \pmod 3$$

$$x \equiv 2 \pmod 5$$

$$x \equiv 3 \pmod 7$$

Clearly $(m_i, m_j) = 1$

$M = 3 \times 5 \times 7 = 105$

$M_1 = 35 \qquad m_1 = 3$

$M_2 = 21 \qquad m_2 = 5$

$M_3 = 15 \qquad m_3 = 7$

Now Solve

$35y \equiv 1 \pmod 3$

$2y \equiv 1 \pmod 3$

$\boxed{y_1 = 2}$

$21y \equiv 1 \pmod 5$

$y \equiv 1 \pmod 5$

$\boxed{y_2 = 1}$

$15y \equiv 1 \pmod 7$

$y \equiv 1 \pmod 7$

$\boxed{y_3 = 1}$

$x = (1)(35)(2) + 3(21)(1) + 15(5)(1) \pmod{105}$

$\equiv 52 \pmod{105}$

Prob-2

Find the smallest positive integer n st $2^3 | n$, $3^3 | n+1$, $4^3 | n+2$

$n \equiv 0 \pmod 8$

$n \equiv 26 \pmod{27}$

$n \equiv 62 \pmod{64}$

$8 | n$

But $4^3 | n+2$

$\Rightarrow 8 | n+2$

$\Rightarrow\Leftarrow$

We cannot apply CRT when they are not coprime.

Consider

$$x \equiv a \pmod{m}$$

$$x \equiv b \pmod{n} \qquad (m,n) \neq 1$$

It has a soln iff $(m,n) \mid a-b$. It has a unique soln $[m,n]$

$\Rightarrow$

Let x_0 be a soln of the system.

$$x_0 = k_1 m + a$$

$$x_0 = k_2 n + b$$

$$\Rightarrow \quad 0 = k_1 m - k_2 n + a - b$$

$$k_1 m - k_2 n = b - a.$$

$$(m, -n) \mid b - a$$

$$\Leftrightarrow \boxed{(m,n) \mid a-b}$$

Unique soln.

Let $(m,n) \mid a-b$; Let x_0 be a soln. Let x_1 be an arbitrary soln.

To show:

$$x_1 \equiv x_0 \pmod{[m,n]}$$

$x_1 \equiv a \pmod{m}$ $\qquad$ $x_0 \equiv a \pmod{m}$

$x_1 \equiv b \pmod{n}$ $\qquad$ $y_0 \equiv b \pmod{n}$

$\therefore x_1 \equiv x_0 \pmod{m}$

$x_1 \equiv x_0 \pmod{n}$

$\Rightarrow m \mid x_1 - x_0$

$n \mid x_1 - x_0$

$\Rightarrow [m,n] \mid x_1 - x_0$

$\Rightarrow x_1 \equiv x_0 \mod [m,n]$

If we find a soln,

$$\boxed{x = x_0 + [m,n]t}$$

Solve:

① $x \equiv 4 \pmod 6$

$x \equiv 2 \pmod 8$

$x \equiv 1 \pmod 9$

$(6,8) = 2 \mid 4-2$ ✓

$(8,9) = 1 \mid 2-1$ ✓

$(6,9) = 3 \mid 4-1$ ✓

Soln.

Let $x = 6t+4$

$\Rightarrow 6t+4 \equiv 2 \pmod 8$

$6t \equiv -2 \pmod 8$

$3t \equiv -1 \pmod 4$

$\boxed{t \equiv 1 \pmod 4}$

$t = 4q+1$

$x = 6t+4 = 6(4q+1)+4 = 24q+10$

$\Rightarrow 24q+10 \equiv 1 \pmod 9$

$24q \equiv -9 \pmod 9$

$8q \equiv -3 \pmod 3$

$2q \equiv 0 \pmod 3$

$\Rightarrow q \equiv 0 \pmod 3$

$q = 3r$

$x = 24q+10$

$= 72r+10$

$x \equiv 10 \pmod{72}$

Solve the system

$$ax + by = r \pmod m$$
$$cx + dy = s \pmod m$$

has a unique soln mod $m \iff (ad-bc, m) = 1$

$$acx + bcy = rc \pmod m$$
$$acx + ady = as \pmod m$$
$$(ad-bc)y = (as-rc) \bmod m$$

$\Rightarrow$ Solve for y, then substitute

Eg

$$3x + 13y \equiv 8 \pmod{55}$$
$$5x + 21y \equiv 34 \pmod{55}$$

$\Rightarrow 15x + 65y \equiv 40$

$15x + 63y \equiv 102$

$ad - bc = 21(3) - 13(5)$

$= 63 - 65$

$= -2$

$$2y \equiv -62 \pmod{55}$$
$$\equiv -7 \pmod{55}$$
$$\equiv 48 \pmod{55}$$

$(-2, 55) = 1 \Rightarrow \exists$ a soln.

$y \equiv 24 \pmod{55}$

$\boxed{y = 55t + 24}$

$$3x + 13y \equiv 8 \pmod{55}$$
$$3x \equiv 8 - 13(24) \pmod{55}$$
$$\equiv -304 \pmod{55}$$

26.02.24

- $ax \equiv 1 \pmod m$ has a unique soln $\Leftrightarrow (a,m) = 1$.
- Solution is called an inverse of a mod m.
- Suppose $m = p$, a prime. Then $\{1, 2, \dots, p-1\}$ are invertible.

Lemma: $a \in \mathbb{N} \cup \{0\}$ is self invertible modulo $p \Leftrightarrow a \equiv \pm 1 \pmod p$

$\Rightarrow$ Suppose a is self invertible modulo p.

$a^2 \equiv 1 \pmod p$

$\Rightarrow p \mid a^2 - 1$

$\Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow p \mid a-1$ (or) $p \mid a+1$

$\Rightarrow a \equiv \pm 1 \pmod p$

$\Leftarrow a \equiv \pm 1 \pmod p$

$\Rightarrow p \mid a+1$ or $p \mid a-1$

$\Rightarrow a^2 \equiv 1 \pmod p$

$\therefore$ Exactly 2 residues are self invertible:
1 and $p-1$.

Take $a \in \{1, \dots, p-1\}$

Wilson's Theorem: If p is a prime

$$(p-1)! \equiv -1 \bmod p$$

When $p=2$ $1! \equiv -1 \pmod 2$ holds.

Let $p > 2$. Then the residues $\{1, 2, \dots, p-1\}$ are invertible modulo p. In particular, 1 and $p-1$ are self invertible. We group the rest into pairs (a,b) st

① $b = a^{-1}$

② $ab \equiv 1 \pmod p$

After grouping

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

$(p-2)! \equiv (p-1) \bmod p$

$\equiv -1 \pmod p$

Thm: Let $n \in \mathbb{N} \cup \{0\}$ st $(n-1)! \equiv -1 \pmod{n}$. Then n is prime. $\quad n \mid (n-1)! + 1$

Suppose $n = ab$, where $1 < a, b < n$.

We have $a \mid n$, and $a < n$

$\Rightarrow a \mid (n-1)!$

$\Rightarrow (n-1)! \equiv -1 \pmod{n}$

$\Rightarrow (n-1)! = qn - 1$ for some n

$\Rightarrow n \mid (n-1)! + 1$

$\Rightarrow a \mid (n-1)! + 1$ and $a \mid (n-1)!$

$\Rightarrow \Leftarrow$

n is a prime.

28.02.24

Wilson's Theorem

If p is prime,

$$(p-1)! \equiv -1 \pmod{p}$$

Qn:

PT: $\binom{np}{p} \equiv n \pmod{p}$, where p is odd prime

$$\binom{np}{p} = \frac{(np)!}{p!\,(n-p)!}$$

Let $k = {}^{np}C_p$

$$= \frac{(np)(np-1)!\,(np-2)!\cdots(np-(p-1))!}{p!}$$

$$k = \frac{n(np-1)\cdots(np-p+1)}{(p-1)!}$$

$$(p-1)!\,k = n(np-1)\cdots(np-p-1)$$

Taking LHS and RHS mod p

$$-k = n(-1)(-2)\cdots(-(p-1))$$

$$-k = n(-1)^{p-1}(p-1)! \pmod{p}$$

$$k = n(-1)^{p}(p-1)! \pmod{p}$$

If p is odd prime,

$$\boxed{k = n \pmod{p}}$$

Prove that if p and $p+2$ are twin primes, then we have

$$4[(p-1)!+1]+p \equiv 0 \mod (p^2+2p)$$

As $(p, p+2)=1$

$p+2$

$(p+1)! \equiv (-1) \mod (p+2)$

$p^2+2p = p(p+2)$

$$4[(p-1)!+1]+p = 4(p-1)!+4+p \equiv -4+4+p \pmod p$$
$$\equiv p \pmod p$$
$$\equiv 0 \pmod p \quad \rightarrow ①$$

$p+4 \equiv 2$

$$4[(p-1)!+1]+p \equiv 4(p-1)!+4+p \pmod{p+2}$$
$$= 2(-2)(-1)(p-1)!+(4+p) \mod (p+2)$$
$$= 2(p)(p+1)(p-1)!+2 \mod (p+2)$$
$$= 2(p+1)!+2 \mod (p+2)$$
$$= 2(-1)+2$$
$$= 0 \mod (p+2)$$

Fermat's Little Theorem

Let p be a prime, and $a \in \mathbb{Z}$ st $(a, p)=1$. Then

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

A consequence

$$7x \equiv 1 \pmod{101}$$

$(7, 101) = 1$

$x = 7^{101-2} = 7^{99}$.

Proof:

The least residues of $a, 2a, \ldots, (p-1)a$ modulo p are a permutation of $1, 2, \ldots, p-1$.

Step-1: $ia \not\equiv 0 \pmod p \quad \forall \quad 1 \le i \le p-1$

Suppose $ia \equiv 0 \pmod p$

$\Rightarrow p \mid ia$

But $(a, p) = 1$

$\Rightarrow p \mid i$

$\Rightarrow \leftarrow$ as $1 \le i \le p-1$

Step-2: If $ia \equiv ja \pmod p \quad 1 \le i, j \le p-1$, then $i = j$

Suppose $ia \equiv ja \pmod p$

$\rightarrow p \mid a(i-j)$

$(a, j) = 1$

$\rightarrow p \mid i-j$

$\Rightarrow i \equiv j \pmod p$

But $1 \le i, j \le p-1$

$\rightarrow i = j$

① $ia \not\equiv 0 \pmod p \quad 1 \le i \le p-1$

② If $ia \equiv r \pmod p$

$ja \equiv r \pmod p$

Then $ia \equiv ja \pmod p$

$\Rightarrow p \mid (i-j)(a), \quad i \neq j$

Proof.

$$a(2a)\cdots(p-1)(a) \equiv (p-1)! \pmod p$$

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

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

Remarks

① If $(a,p)=1$, then a^{p-2} is a soln of

$$ax \equiv 1 \bmod p$$

i.e., a^{p-2} is inverse of $a \bmod p$.

② If $(a,p)=1$, the congruence $ax \equiv b \pmod p$ has a sol^n $x \equiv a^{p-2}b \pmod p$

Eg:

$7x \equiv 1 \mod 29$

$(7,29)=1$

$7^{28} \equiv 1 \mod 29$

$7 \cdot 7^{27} \equiv 1 \mod 29$

$x = 7^{27} \mod 29$.

29, 58, 87, 116, 145

7, 49, 343.

③ If $a \in \mathbb{Z}$, and p is a prime,

$$a^p \equiv a \pmod p$$

- If $(a,p)=1$, Invoke fermat
- Sup $p \mid a$

$\Rightarrow a \equiv 0 \mod p$

$\Rightarrow a^p \equiv 0 \pmod p$

Also $p \equiv 0 \pmod p$

$\Rightarrow a^p \equiv a \pmod p$

$p \mid a^{p-1} - 1$

$p = a^{p-1} - 1$

$ap = a^p - p$

④ Let p, q are distinct primes

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

It is enough to show separately.

$p^{q-1} + q^{p-1} \equiv 0 + 1 \pmod p$

$p^{q-1} + q^{p-1} \equiv 1 + 0 \pmod q$

Find the remainder when 24^{1947} is div by 17.

$24 \equiv 7 \pmod{17}$

$24^{1947} \equiv 7^{1947} \pmod{17}$

$(7, 17) = 1$

By FLT

$7^{16} \equiv 1 \pmod{17}$

$7^{1947} \equiv (7^{16})^{121} \cdot 7^{11} \pmod{17}$

$\equiv 7^{11} \pmod{17}$

$7^2 \equiv -2 \pmod{17}$

$7^{10} \cdot 7^1 \equiv (-2)^5 \cdot 7 \pmod{17}$

$= -32 \times 7 \pmod{17}$

$= 2 \times 7 \pmod{17}$

$\boxed{7^{11} \equiv 14 \mod 17}$

$\therefore\ 24^{1947} \equiv 14 \pmod{17}$

Pf: $\forall n \in \mathbb{N} \quad n^5 \equiv n \pmod{30}$

$30 = 2 \times 3 \times 5$

To show: $n^5 \equiv n \pmod 2$

$n^5 \equiv n \pmod 3$

$n^5 \equiv n \pmod 5$

By corollary to Fermat,

$\forall a, p \quad a^p \equiv a \pmod p$

③ Pf $\forall a \in \mathbb{Z}$ st $(a, 561) = 1$ $\qquad 187 = 11 \times 17$

we have

$a^{560} \equiv 1 \pmod{561}$

$561 = 3 \times 11 \times 17$.

To show:

$a^2 \equiv 1 \pmod 3 \Rightarrow a^{560} \equiv 1 \pmod 3$

$a^{10} \equiv 1 \pmod{11} \quad a^{560} \equiv 1 \pmod{11}$

$a^{16} \equiv 1 \pmod{17} \quad a^{560} \equiv 1 \pmod{17}$

Converse of Fermat

If $\forall a \in \mathbb{N}, (a, n) = 1$, we have

$a^{n-1} \equiv 1 \pmod n$

Counterexample, $n = 561$

(not a prime)

④ Let $n = 2p$, $p \neq 2$. $\forall n \in \mathbb{N}$, $a^{n-1} \equiv a \pmod n$

$(2, p) = 1$

Enough to show:

① $a^{n-1} \equiv a \pmod 2$

② $a^{n-1} \equiv a \pmod p$

② $a^{n-1} \equiv a^{2p-1} \pmod p$

$\equiv (a^p)(a^{p-1}) \pmod p$

$\equiv a \pmod p$

① To show:

$a^{n-1} \equiv a \pmod 2$

$a^{n-1} = a^{2p-1}$

$2 \mid a^{n-1} - a$

$2 \mid a^{2p-1} - a$

$2 \mid a(a^{2p-2} - 1)$

Euler's Theorem

- generalized version of Fermat's Theorem.

Let $m \in \mathbb{N} \cup \{0\}$. Then

$$\phi(m) = \#\{a \in \mathbb{N} : (a, m) = 1,\ a \leq m\}$$

of +ve integers $\leq m$ and coprime to m.

18
1, 5, 7, 11, 13, 17

Eg: $\phi(11) = 10$

$\phi(p) = p - 1$, where p is a prime.

② $\phi(18) = 6$

③ $\phi(e) = p^e - p^{e-1}$

Consider $(a, p^e) = p, p^2, \ldots, p^e$

$1 \cdot 2 \cdots (p-1)\,(p)\,(p+1) \cdots 2p \cdots 3p \cdots p^{e-1}$

- Take multiples of p only.

Examples

① $35 \mid 18^{360}$

$(18)^{360} \equiv 1 \pmod{35}$

$(18)^{\phi(m)} \equiv 1 \pmod{35}$

② $18 \mid 245^{1040}$

$18 \times 3 = 54$

$245 \equiv 11 \pmod{18}$

$(245)^{1040} \equiv (11)^{1040} \pmod{18}$

$(11, 18) = 1$

$\{\phi(18)\} = 5, 7, 11, 13, 17, 1 = 6$

$\rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$

$\frac{1040}{6} = 173$

$11^6 \equiv 1 \pmod{18}$

$18 \times 6 = 108$

$18 \times 7 = 126$

$11^{1040} \equiv 121 \pmod{18}$

$\equiv 13 \pmod{18}$

4.3.24.

Euler's Phi function

Let $m \in \mathbb{Z}^+$. Then

$\phi(m) = \#\{a \in \mathbb{N}^+ : a \leq m \text{ and } (a, m) = 1\}$

Note:

$\phi(p^e) = p^e - p^{e-1}$, $e \in \mathbb{N} \cup \{0\}$.

(p is a prime)

Euler's Theorem

Let $a \in \mathbb{Z}$, $m \in \mathbb{N}$ st $(a, m) = 1$.

Then $\boxed{a^{\phi(m)} \equiv 1 \pmod{m}}$

Proof:

- Let $r_1, r_2, \ldots, r_{\phi(m)} \in \mathbb{N}$, st $1 \leq r_i \leq m$ $\forall\, i = 1$ to $\phi(m)$ and $(r_i, m) = 1$
- Let $(a, m) = 1$.

Claim:

The least residues of the integers $ar_1, ar_2, \ldots, ar_{\phi(m)}$ modulo m are a permutation of $r_1, \ldots, r_{\phi(m)}$.

Consider

ar_1
ar_2
$\vdots$
$ar_{\phi(m)}$.

$\xrightarrow[\text{residues mod } m]{\text{least}}$

r_1
r_2
$\vdots$
r_m

Proof:

Digress

$a \equiv r \pmod m$

$a = mk + r$.

$(a, m) = (r, m)$

(i) $(ar_i, m) = 1 \quad \forall\ 1 \le i \le \phi(m)$

Suppose $d = (ar_i, m)$ and $d \ge 1$.

d has a prime factor.

i.e., $d = px$ for some p, x.

$p \mid x$

Also $d \mid ar_i$ and $d \mid m$

$\Rightarrow p \mid ar_i$ and $p \mid m$

$p \mid a$ or $p \mid r_i$

If $p \mid a$ and $p \mid m$

$(a, m) \neq 1 \quad \rightarrow\leftarrow$

If $p \mid r_i$ and $p \mid m$

$(r_i, m) \neq 1 \quad \Rightarrow\Leftarrow$

$\therefore \boxed{d = 1}$

(2) $ar_i \not\equiv ar_j \pmod m \qquad 1 \le i \le j \le m$.

If not, $m \mid a(r_i - r_j)$

$\Rightarrow m \mid r_i - r_j$

$\rightarrow\leftarrow$

$\therefore ar_i \not\equiv ar_j$

Then

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1, r_2, \cdots r_{\phi(m)} \pmod m$$

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod m$$

$$\therefore \boxed{a^{\phi(m)} \equiv 1 \pmod m}$$

Problems

① $17x \equiv 20 \pmod{24}$

WKT $(17,24) = 1$ $\quad \phi(24) = 1,5,7,11,13,17,19,23$

$17^{\phi(24)} \equiv 1 \pmod{24}$

$17^8 \equiv 1 \pmod{24}$

$17^7 (17) \equiv 1 \pmod{24}$

$17 \underbrace{(17)^7 \times 20} \equiv 20 \pmod{24}$

$x \equiv (17)^7 \times (20) \pmod{24}$

$\equiv (-4)(-7)^7 \pmod{24}$

$\equiv 4(7)^7 \pmod{24}$

$\equiv 4(7^2)^3(7) \pmod{24}$

$\equiv 28 \pmod{24}$

$\boxed{x \equiv 4 \pmod{24}}$

② Let $(a,m) = 1 = (a-1, m)$

$a^{\phi(m)-1} + a^{\phi(m)-2} + \cdots + a + 1 \equiv 0 \pmod{m}$

$a^{\phi(m)} \equiv 1 \pmod{m}$

$m \mid a^{\phi(m)} - 1$

$m \mid (a-1)(a^{\phi(m)-1} + \cdots + a + 1)$

$\Rightarrow \quad m \mid a^{\phi(m)-1} + \cdots + a + 1$

③ $(a,b) = 1$

$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod (ab)$

Show

① $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod (a)$

② $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod b$.

① $a^{\phi(b)} + b^{\phi(a)} \equiv 0+1 \pmod{a}$

② $a^{\phi(b)} + b^{\phi(a)} \equiv 0+1 \pmod{b}$

④ Every $n \in \mathbb{Z}$ st $(n, 10) = 1$ divides some integer N consisting of all 1s.

k.

$(n, 10) = 1$

$(9, 10) = 1$

$\Downarrow$

$(9n, 10) = 1$

$10^{\phi(9n)} \equiv 1 \pmod{9n}$

$N = \dfrac{10^{\phi(9n)} - 1}{9}$.

Problems

Let $a_n = 2^n + 1$,

$m = n + k\phi(a_n)$, $k \in \mathbb{Z}$

PT: $a_n \mid a_m$

i.e., $a_m \equiv 0 \pmod{a_n}$

$$a_m = 2^m + 1$$
$$= 2^{n + k\phi(a_n)} + 1$$
$$= 2^n \cdot 2^{k\phi(a_n)} + 1$$

WRT

$(2, 2^n + 1) = 1$

$2^{\phi(a_n)} \equiv 1 \pmod{a_n}$

$\therefore a_m \equiv (-1)(1) + 1 \pmod{a_n}$

$\equiv 0 \pmod{a_n}$

② Find the primes p for which $\frac{2^{p-1} - 1}{p}$ is a perfect square

Soln:

p has to be odd.

Let $p = 2k + 1$

$\frac{2^{p-1}-1}{p} = n^2$ for some $n \in \mathbb{N}$

$\frac{2^{p-1}-1}{p} \in \mathbb{Z}$ (by Fermat's Thm) $\Rightarrow 2^{p-1} \equiv 1 \pmod{p}$ $(2,p)=1$

$2^{p-1} - 1 = pn^2$

$2^{2k} - 1 = (2k+1)n^2$

$\Rightarrow (2^k-1)(2^k+1) = pn^2$

Now $(2^k-1, 2^k+1) = 1$

Either 2^k-1 is a square or

2^k+1 is a square.

Case-1

$2^k - 1 = n^2$, n is odd

$= (2i+1)^2$

$2^k - 1 = 4i^2 + 1 + 4i$

$2^k = 4i^2 + 4i + 2$

$= 2(2i^2 + 2i + 1)$

$\Rightarrow i = 0$

$\Rightarrow 2^k = 2 \Rightarrow \boxed{k=1}$

$\Rightarrow \boxed{p = 2^k + 1 = 3}$

Case-2

$2^k + 1 = n^2$

$2^k = (2i+1)^2 - 1$

$2^k = 4i^2 + 4i$

$= 4(i^2 + i)$

$2^{k-2} = i^2 + i$

$= i(i+1)$

$\therefore i = 1$

$2^{k-2} = 2^1$

$\Rightarrow \boxed{k=3}$

$p = 2^3 - 1$

$= 7$

$\boxed{p=3 \text{ or } p=7}$

3. $a^2 + b^2 \equiv 0 \pmod p$

$p \equiv 3 \pmod 4$

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

Prove that p divides both a and b

To show: $a \equiv 0 \pmod p$

$b \equiv 0 \pmod p$

$a^2 \equiv -b^2 \pmod p$

It is enough to show $p \mid a$.

Suppose $p \nmid a$ and $p \nmid b$

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

$b^{p-1} \equiv 1 \pmod p$

$a^2 \equiv -b^2 \pmod p$

$+ (a)^{p-1} \equiv (-1)^{p-1/2}\ b^{p-1} \bmod p$

$1 \equiv (-1)^{p-1/2} \cdot 1 \pmod p$

$\Rightarrow 1 \equiv -1 \pmod p$

$p = 3 + 4k \Rightarrow p \mid 2$

$\Rightarrow \Leftarrow$

$\Rightarrow p - 1 = 4k + 2$

$\frac{p-1}{2} = 2k + 1 \Rightarrow$ odd.