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.

$(n, 10) = 1$

$(9, 10) = 1$

$\Downarrow$

$(9n, 10) = 1$

$10^{\phi(9n)} \equiv 1 \pmod{9n}$

$N = \dfrac{10^{\phi(9n)} - 1}{9}$.

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.

Multiplicative Functions

$f: \mathbb{N} \longrightarrow \mathbb{Z}$

↓

Number Theoretic Functions

$\phi: \mathbb{N} \to \mathbb{N}$

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

A number theoretic function is called a multiplicative function if

$f(mn) = f(m)\, f(n)$

if $(m,n) = 1$

$n = p_1^{e_1} \cdots p_k^{e_k}$

$f(n) = f(p_1^{e_1})\, f(p_2^{e_2}) \cdots f(p_k^{e_k})$

Eg: $n = 600$

$= 5^2 \times 2^3 \times 3^1$

$\phi(600) = \phi(2^3)\, \phi(3^1)\, \phi(5^2)$

$= (2^3 - 2^2)(3^1 - 3^0)(5^2 - 5^1)$

$= 4 \times 2 \times 20$

$= 160$

600

$= 6 \times (10)^2$

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

$= 2^3 \times 3^1 \times 5^2$

Theorem: ϕ is multiplicative

Let $m, n \in \mathbb{N}$, $(m,n) = 1$

Then $\phi(m \cdot n) = \phi(m)\, \phi(n)$

Consider

$1, \quad m+1, \quad 2m+1, \ldots, (n-1)m+1$

$2, \quad m+2, \quad 2m+2, \ldots, (n-1)m+2$

$\vdots$

$m, \quad 2m, \quad 3m, \ldots, \quad mn$

Among all rows, there will be exactly $\phi(m)$ rows which are coprime to m.

To prove:

In each row, there are $\phi(n)$ numbers coprime to n.

Suppose

$$r,\ m+r,\ 2m+r,\ \ldots,\ (n-1)m+r$$

are the integers coprime to m.

Any such

$$im+r \equiv jm+r \pmod{n}$$

$$\Rightarrow im \equiv jm \pmod{n}$$

$$\Rightarrow n \mid (i-j)(m)$$

$$\Rightarrow n \mid i-j$$

$$\therefore i=j$$

$$1, 2, \ldots, n$$

$\phi(n)$ integers are coprime to n.

$$\phi(n) = \phi(p_1^{e_1})\,\phi(p_2^{e_2}) \ldots \phi(p_k^{e_k})$$

$$= \prod_{j=1}^{k} \left(p_j^{e_j} - p_j^{e_j-1}\right)$$

$$= \prod_{i=1}^{n} p_i^{e_i} \prod_{j=1}^{n} \left(1 - \frac{1}{p_j}\right)$$

$$= n \prod_{j=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Problem

① Prove that $\phi(n)$ is even $\forall\ n \geq 3$

Proof:

Suppose $p \mid n$, where p is an odd prime.

$$\Rightarrow n = p^k m \text{ where } (p, m) = 1,\ k \geq 1$$

Then $\phi(n) = \phi(m)\,\phi(p^k)$

$$= (p^k - p^{k-1})\,\phi(m)$$

$$\Rightarrow 2 \mid \phi(n)$$

Suppose $n = 2^k$, $k \geq 2$

$\phi(n) = 2^k - 2^{k-1} = 2^{k-1}$

$\Rightarrow 2 \mid \phi(n)$

② If p and q are twin primes, with $p < q$, prove that

$\phi(q) = \phi(p) + 2$

wkt $q = p + 2$

$\phi(p) = p - 1$

$\phi(q) = q - 1$

$= p + 2 - 1$

$= p + 1$

$= \phi(p) + 2$

③ If $m \mid n$, then $\phi(m) \mid \phi(n)$

Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$

$m = \prod_{i=1}^{k} p_i^{\beta_i}$ $\quad 0 \leq \beta_i \leq \alpha_i$

$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$

$\phi(m) = \prod_{i=1}^{k} p_i^{\beta_i - 1}(p_i - 1)$

Now, $\forall i$, $\alpha_i - 1 \leq \beta_i - 1$

$\therefore \phi(m) \mid \phi(n)$

Tau and Sigma Function

$n \in \mathbb{N}$

$\tau(n)$ = # of positive divisors of n = $\sum_{d \mid n} 1$

$\sigma(n)$ = Sum of all positive divisors of n = $\sum_{d \mid n} d$

$\tau(18) = \#\{1, 2, 3, 6, 9, 18\} = 6$

$\sigma(18) = 19 + 11 + 9 = 39$

Let p be a prime

$\tau(p) = 2$

$\sigma(p) = 1+p$

$\tau(p^e) = e+1$

$\sigma(p^e) = 1+p+p^2+\cdots+p^e$

$= \frac{p^{e+1}-1}{p-1}$

Goal: Show that they are multiplicative.

Theorem: If $f(n)$ is multiplicative, then

$$F(n) = \sum_{d|n} f(d)$$

is also multiplicative.

Suppose we have $m, n \in \mathbb{Z}^+$, $(m,n) = 1$

Now

$$F(mn) = \sum_{d|mn} f(d)$$

- If $d|mn$, $d = d_1 d_2$, $d_1|m$, $d_2|n$, $(d_1, d_2) = 1$.

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n \\ (d_1,d_2)=1}} f(d) \quad \text{where } d = d_1 d_2$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2)$$

$$= \sum_{d_2|n} f(d_2) \sum_{d_1|m} f(d_1)$$

$$= F(n) F(m)$$

Key

① $(m,n) = 1$

② $f(mn) = f(m) f(n)$

- In particular, $\tau(n)$ and $\sigma(n)$ are multiplicative.
- $\tau(n) = \prod_{i=1}^{k} \tau(p_i^{e_i})$

$= \prod_{i=1}^{k} (e_i + 1)$

- $\sigma(n) = \prod_{i=1}^{k} \sigma(p_i^{e_i})$

$= \prod_{i=1}^{k} \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right)$

Problems

If $\tau(n)$ is odd, then n is a square.

Let $n = p_1^{e_1} \cdots p_k^{e_k}$

$\tau(n) = \prod_{i=1}^{k} (e_i + 1)$

$\Rightarrow \{e_i\}_{i=1}^{k}$ is even

$\therefore n = \left[\prod p_i^{e_i/2} \right]^2$

$\therefore n$ is a square.

② If $\sigma(n)$ is odd PT

① n is a square or

② $n = 2k^2$ for some k.

$n = p_1^{e_1} \cdots p_k^{e_k} = 2^k p_1^{e_1} \cdots p_k^{e_k}$

$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}$

for $n = 1 \Rightarrow$ holds

$\sigma(n) = (1 + p_1 + \cdots + p_1^{e_1}) \cdots (1 + p_k + \cdots + p_k^{e_k})$

e_i's are even $\forall\ 1 \le i \le k$

(p_i's are odd)

Problems

Let f and g be 2 multiplicative number theoretic functions.

Further,

$$F(1) = f(1)$$

$$F(p^e) = f(p^e) \quad \forall \text{ primes } p \text{ and } e \in \mathbb{N}$$

What can you say about $F(n)$ & $f(n)$?

Let $N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $N \geq 2$

$$F(N) = F(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k})$$

$$= f(p_1^{e_1}) F(p_2^{e_2}) \dots F(p_k^{e_k})$$

$$= f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_k^{e_k})$$

$$= f(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k})$$

$$= f(N)$$

To prove:

$$\sum_{d|n} \phi(d) = n$$

$f(n) = n$ is multiplicative.

$\sum_{d|n} \phi(d)$ is multiplicative.

as ϕ is multiplicative

$$F(n) = \sum_{d|n} \phi(d)$$

$$f(n) = n$$

$$F(1) = \sum_{d|1} \phi(d) = 1$$

$$f(1) = 1$$

Let p be any prime, $e \in \mathbb{N}$.

Consider $n = p^e$

$$F(p^e) \sum_{d|n} \phi(n) = \phi(1) + \phi(p) + \cdots + \phi(p^e)$$

$$= 1 + (p-1) + (p^2 - p) + \cdots + p^e - p^{e-1}$$

$$= p^e$$

$$= f(p^e)$$

$$\therefore F(p^e) = f(p^e)$$

$\Rightarrow F(n) = f(n) \quad \forall\ n \in \mathbb{N}$ (from last result)

$$\boxed{\sum_{d|n} \phi(d) = n}$$

Problem:

Prove that product of all positive divisors of $n \in \mathbb{Z}^+$ is $n^{\tau(n)/2}$

i.e., $\prod_{d|n} d = n^{\tau(n)/2}$

Let $d_1, d_2, \ldots, d_{\tau(n)}$ be positive divisors of n.

$\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_{\tau(n)}}$ are the same divisors but in some other order.

$$\prod_{d|n} n = d_1 d_2 \cdots d_{\tau(n)} = \frac{n}{d_1} \cdot \frac{n}{d_2} \cdots \frac{n}{d_{\tau(n)}}$$

$$\Rightarrow \left[\prod_{i=1}^{\tau(n)} d_i \right]^2 = n^{\tau(n)}$$

$$\boxed{\prod_{i=1}^{\tau(n)} d_i = n^{\tau(n)/2}}$$

Mobius Inversion Formula

$$f(n) = \sum_{d|n} f(d)$$

↓

an expression

$$\boxed{f(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right)}$$

Mobius Inversion fn

$$\tau(n) = \sum_{d|n} 1$$

$$1 = \sum_{d|n} \mu(d)\, \tau\left(\frac{n}{d}\right)$$

Mobius Fn

$$\mu(n) = \begin{cases} 1, & \text{if } n=1 \\ 0, & \text{if } p^2 \mid n, \ p \text{ is prime} \\ (-1)^k & \text{if } n = p_1 \cdots p_k \end{cases}$$

Eg

① $\mu(4) = 0 = \mu(12)$

② $\mu(6) = 1 = \mu(21)$

③ $\mu(p) = -1$

To show: μ is multiplicative

Claim: $\mu(n)$ is multiplicative

i.e., $\mu(mn) = \mu(m)\,\mu(n) \quad \forall\ m,n \in \mathbb{N}$

$(m,n) = 1$

Case-1 : $p^2 \mid mn$

$\mu(mn) = 0$

As $p^2 \mid mn$, $(m,n) = 1$

$\therefore p^2 \mid m$ or $p^2 \mid n$

$\Rightarrow \mu(m) = 0$ or $\mu(n) = 0$.

$\Rightarrow \mu(m)\,\mu(n) = 0$

$\therefore \mu(mn) = 0 = \mu(m)\,\mu(n)$

Case-2: If $p^2 \nmid mn$ for any prime p.

$m = p_1 \cdots p_r$

$n = q_1 \cdots q_s$

- $p_i \neq q_j \quad \forall$ pairs (i,j)
- p_i's and q_i's are distinct primes

$\mu(mn) = (-1)^{r+s}$

$= (-1)^r (-1)^s$

$= \mu(m)\,\mu(n)$

Lemma: $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{, ow.} \end{cases}$

$\mu(1) = 1$

Suppose $n \geq 2$

$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

What does d look like? Compact notation helps!

$$\sum_{d|n} \mu(d) = \prod_{i=1}^{k} \left(\sum_{d|p_i^{e_i}} (\mu(d)) \right)$$

$$= \prod_{i=1}^{k} \left(\mu(1) + \mu(p_i) + \mu(p_i^2) + \cdots + \mu(p_i^{e_i}) \right)$$

$$= \prod_{i=1}^{k} (1 - 1 + 0)$$

$$= 0$$

Let f and F be number theoretic functions and

$$F(n) = \sum_{d|n} f(d)$$

$$\boxed{f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)}$$

Proof:

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left(\sum_{d'|\frac{n}{d}} f(d') \right)$$

$d|n$ and $d'|n/d \iff d'|n$ and $d|n/d'$

$\mapsto$ $d|n$, $d'|n/d$

$\Rightarrow \frac{n}{d} = d'k$

$\Rightarrow n = dd'k$

$\Rightarrow d \mid \frac{n}{d'}$, $d'|n$

$\leftarrow\!\!\mapsto$ $d'|n$ and $d|n/d'$

$\frac{n}{d'} = dk$

$\Rightarrow n = dd'k$

$\therefore d|n$, $d'|\frac{n}{d}$.

Done.

$$\sum_{d' \mid n} \mu(d') \sum_{d \mid \frac{n}{d'}} f(d) = \sum_{d' \mid n} \sum_{d \mid \frac{n}{d'}} \mu(d) f(d')$$

$$= \sum_{d' \mid n} f(d') \sum_{d \mid \frac{n}{d'}} \mu(d) \qquad \left\{ \sum_{d \mid n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & \text{ow} \end{cases} \right.$$

$$= f(n) \cdot 1$$

Mobius Inversion formula.

$$F(n) = \sum_{d \mid n} f(d) \longrightarrow (1)$$

$$f(n) = \sum_{d \mid n} \mu(d) F(n/d) = \sum_{d \mid n} \mu(n/d) F(d)$$

Prove:

If F and f are related by (1), then

F is mult $\Leftrightarrow$ f is multip

Problem

PT: $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$

$$\sum_{d|n} \frac{1}{d} = \sum_{d|n} \frac{1}{n/d} = \sum_{d|n} \frac{d}{n}$$
$$= \frac{1}{n} \sum_{d|n} d$$
$$= \frac{\sigma(n)}{n}$$

If $m|n$, $\frac{\sigma(n)}{n} \geq \frac{\sigma(m)}{m}$

$m|n \Rightarrow n = mk$

$$\frac{\sigma(n)}{n} = \sum_{d|n} 1/d$$
$$= \sum_{d|m} 1/d + \sum_{\substack{d|n \\ d\nmid m}} \frac{1}{d}$$
$$= \frac{\sigma(m)}{m} + \text{extra}$$

$$\boxed{\frac{\sigma(n)}{n} \geq \frac{\sigma(m)}{m}}$$

② Let $n \geq 2$

$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$\sum_{d|n} \mu(d)\tau(d) = (-1)^k$

Since μ and τ are mult, so is $\mu\tau$

$$\sum_{d|n} \mu(d)\tau(d) = \prod_{i=1}^{k} \sum_{d|p^i} \mu(d)\tau(d)$$
$$= \prod_{i=1}^{k} \left\{ \mu(1)\tau(1) + \mu(p_i)\tau(p_i) + \mu(p_i^2)\tau(p_i^2) + \cdots \right\}$$

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

$$= (-1)^k$$

Perfect Numbers

A positive integer n is called perfect if sum of all proper positive divisors is equal to n.

$$n = \sum_{\substack{d \mid n \\ d \neq n}} d$$

$$= \sigma(n) - n$$

$$\Rightarrow \boxed{\sigma(n) = 2n}$$

Example

$P_1 = 6 = 1+2+3$

$P_2 = 28 = 1+2+4+7+14$

$P_3 = 496$

$P_4 = 8128$

Conjectures

① n^{th} perfect number has exactly n digits

② perfect numbers end in 6 or 8 alternating.

These are wrong!

$P_5 = 33550336$

$P_6 = 8598690 56$

Observation

① Is there an odd perfect number?

Has been verified that $\forall n \leq 10^{300}$, $\exists$ odd perfect number.

Theorem: Let n be an even integer. Then n is perfect $\iff$ $n = 2^{k-1}(2^k - 1)$ where $2^k - 1$ is prime, $k \geq 2$.

Proof:

$\Leftarrow$ Suppose

$$n = 2^{k-1}(2^k - 1), \text{ where } (2^k - 1) \text{ is prime.}$$

To show: $\sigma(n) = 2n$.

$$\begin{aligned}
\sigma(n) &= \sigma(2^{k-1}(2^k - 1)) \\
&= \sigma(2^k - 1)\,\sigma(2^{k-1}) \\
&= 2^k [2^k - 1] \\
&= 2[2^{k-1}(2^k - 1)] \\
&= 2n.
\end{aligned}$$

$\Rightarrow$ Suppose $\sigma(n) = 2n$.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

$$\sigma(n) = 2p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

WLOG, let $p_1 < p_2 < \cdots < p_k$, $p_1 = 2$

$$\sigma(n) = p_1^{e_1+1} p_2^{e_2} \cdots p_k^{e_k}$$

Alt:

n is even perfect

$$n = 2^{k-1} m, \text{ where } m \text{ is odd}$$

$$\begin{aligned}
\sigma(n) &= \sigma(2^{k-1})\,\sigma(m) \\
2n &= (2^k - 1)\,\sigma(m) \\
2 \cdot 2^{k-1} m &= (2^k - 1)\,\sigma(m)
\end{aligned}$$

$2^k m = (2^k - 1)\sigma(m) \rightarrow (1)$

But $2^k - 1$ is prime

$\rightarrow 2^k - 1 \mid m$

$\Rightarrow m = (2^k - 1)M \rightarrow (2)$

$(2^k)(2^k - 1)M = (2^k - 1)\sigma(m)$

$\Rightarrow \sigma(m) = 2^k M$

$= (2^k - 1)M + M$

$= m + M$

We can't afford $M > 1$. (write).

Suppose $M > 1$.

$\exists\ p \mid M$.

$\sigma(m) = m + M + p$

$> m + M$

$\Rightarrow\Leftarrow$

$\Rightarrow M = 1$, m is a prime

From (1),

$n = 2^{k-1} m$

$= 2^{k-1}(2^k)$, $(2^k - 1)$ prime

Can we say anything about k?

k should be a prime.

$\therefore$ n is even perfect $\Leftrightarrow$ $n = 2^{p-1}(2^p - 1)$, where p is a prime and $2^p - 1$ is also a prime.

Theorem :

If n is an even perfect number, $n \equiv 6$ or $8 \pmod{10}$

Proof :

$n = 2^{p-1}(2^p - 1)$, p is a prime

$2^p - 1$ is a prime.

If $p = 2$, $n = 6$ holds

Assume p is odd.

$\therefore$ $p = 4k+1$ or $p = 4k+3$

Case-1 : $p = 4k+1$

$$n = 2^{4k}(2^{4k+1} - 1)$$
$$\equiv 16^k [2 \cdot 16^k - 1] \pmod{10}$$
$$\equiv 6[2 \cdot 6 - 1] \pmod{10}$$
$$\equiv 6 \pmod{10}$$

Case-2 : $p = 4k+3$

$$n \equiv 2^{4k+2}[2^{4k+3} - 1] \pmod{10}$$
$$= (16^k)(4)[16^k \cdot 8 - 1] \pmod{10}$$
$$= (6)(4)[47] \pmod{10}$$
$$= (6)(4)(7) \pmod{10}$$
$$\equiv 8 \pmod{10}$$

Problems :

If $n = 2^{p-1}(2^p - 1)$ p, $2^p - 1$ are primes.

Prove that $\phi(n) = n - 2^{2p-2}$

$(2^{p-1}, 2^p - 1) = 1$

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

$\therefore$ $\phi(n) = \phi(2^{p-1})\,\phi(2^p - 1)$

$= (2^{p-1} - 2^{p-2})(2^p - 2)$

$= 2^{p-1}(1 - 1/2)(2)(2^p - 1)$

$= n - 2^{2p-2}$

② Prove that pq is not a perfect number if p, q are distinct odd primes.

$(p, q) = 1$

$$\sigma(pq) = \sigma(p)\,\sigma(q)$$
$$= (p+1)(q+1)$$
$$= 1 + p + q + pq$$

Suppose

$$1 + p + q + pq = 2pq$$
$$1 + p + q - pq = 0$$
$$1 = pq - q - p$$
$$2 = 1 - p - q + pq$$
$$= (1-p)(1-q)$$

$(1-p) = -1 \Rightarrow p = 2$
$1 - q = 2$ $\Rightarrow \leftarrow$

③ If n is a perfect number, PT:

$$\sum_{\substack{1 \le d < n \\ d \mid n}} \frac{d}{n} = 1$$

Recall $\frac{\sigma(n)}{n} = \sum_{d \mid n} \frac{1}{d}$

$$= \sum_{\substack{1 \le d < n \\ d \mid n}} \frac{d}{n} - 1$$

$$= \frac{1}{n} \sum_{d \mid n} d - 1$$

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

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

④ If $\frac{\sigma(n)}{n} = \frac{5}{3}$, then $5n$ is odd perfect number.

$$\sigma(n) = \frac{5n}{3}$$

Then $3 \mid n$.

Suppose $2 \mid n$. Then $6 \mid n$.

$$\frac{\sigma(n)}{n} = \frac{5}{3} \geq \frac{\sigma(6)}{6}$$

But $\frac{\sigma(6)}{6} = 2$. $\rightarrow\leftarrow$

$\therefore 2 \nmid n$.

$\therefore n$ is odd.

To show: $\sigma(5n) = 10n$.

Given $\sigma(n) = \frac{5n}{3}$

Then $\sigma(n)$ is always odd

$\Rightarrow n$ is a square.

$\therefore 3^2 \mid n$.

Claim : $(n, 5) = 1$.

Suppose $n = 5k$ for some k.

$3^2 \mid n$, $5 \mid n$

$\Rightarrow 45 \mid n$

$$\frac{\sigma(3^2 \cdot 5)}{3^2 \cdot 5} = \frac{13 \cdot 6}{9 \cdot 5} = \frac{78}{45} = \frac{26}{15} \geq 5 \mid 3$$

$\rightarrow\leftarrow$

Even perfect numbers

$$n = 2^{p-1}(2^p - 1)$$

where p, $2^p - 1$ are primes.

Mersenne number

- A number of the form $2^n - 1$ is called Mersenne number.
- If $M_p := 2^p - 1$ is a prime, called Mersenne prime.

Result [Primality test for Mersenne Primes]

If $p \equiv 3 \pmod 4$, $p > 3$, is a prime such that $2p+1$ is also a prime, then M_p is composite.

Example:

$p = 251$

$p \equiv 251 = 3 \pmod 4$

$2p+1 = 503$ is a prime.

$2^p - 1 = 2^{251} - 1$ is composite.

Chapter -10

Primitive Roots

Order of a positive integer modulo m

- Let $a \in \mathbb{N}$ st $(a, m) = 1$.
- Order of a modulo m is the smallest positive integer $e \in \mathbb{N}$ st $a^e \equiv 1 \pmod{m}$

  Notation: $\operatorname{ord}_m a = e$

- We can have an upper bound on e: $e \leq \phi(m)$ as $a^{\phi(m)} \equiv 1 \pmod{m}$

Example

① $\operatorname{ord}_7 5$

$\phi(7) = 6$

$5^2 \equiv 4 \pmod 7$

$5^3 \equiv 6 \pmod 7$

$5^6 \equiv 1 \pmod 7$

② $\operatorname{ord}_{13} 5 =$

$\phi(13) = 12$

$5^3 \equiv \pmod{13}$

$5^4 \equiv 1 \pmod{13}$

Theorem: Let $a, m \in \mathbb{N}$ st $(a, m) = 1$, and $\operatorname{ord}_m a = e$.

Then $a^n \equiv 1 \pmod m \leftrightarrow e \mid n$.

Proof:

$\leftarrow$ If $e \mid n \Rightarrow n = ek$

$a^n = a^{ek}$

$= (a^e)^k \equiv 1^k \equiv 1 \pmod m$

$\Rightarrow$ Suppose $a^n \equiv 1 \pmod m$

such that $(a, m) = 1$

Clearly, $e \leq n$.

$$n = qe + r, \quad 0 \leq r \leq e.$$

$$a^n = a^{qe+r}$$

$$= a^{qe} \cdot a^r$$

$$1 \equiv (1) \cdot a^r \pmod m$$

$$\Rightarrow a^r \equiv 1 \pmod m$$

$\Rightarrow$ r has to be 0.

as $\operatorname{ord}_m a = e$

$\Rightarrow r > e$ $\Rightarrow\Leftarrow$

In particular, $\boxed{\operatorname{ord}_m a \mid \phi(m)}$

Problem :

$\operatorname{ord}_{21} 5$

$\phi(21) = \phi(3)\phi(7)$

$= 2 \cdot 6$

$= 12$

$5 \equiv 5$

$5^2 \equiv 4$

$5^3 \equiv -1$

$5^6 \equiv 1$

$1, 2, 3, 4, 6, 12$

Check for $1, 2, 3, 4, 6, 12$

Notice $5^6 \equiv 1 \pmod{21}$

Corollary :

$$a^i \equiv a^j \pmod m \leftrightarrow i \equiv j \pmod e$$

where $\operatorname{ord}_m a = e$.

Proof :

$\rightarrow$ Let $a^i \equiv a^j \pmod m$ and $i \geq j$

$(a, m) = 1$

$\Rightarrow (a^j, m) = 1$

a^j has an inverse modulo m, call it a^{-j}

$$a^{i-j} \equiv 1 \pmod m$$

$$\Rightarrow e \mid i-j$$

$$\rightarrow i \equiv j \pmod e$$

$\Leftarrow$ Suppose $i \equiv j \pmod e$

$$\rightarrow e \mid i-j$$

$$\rightarrow i = j + ke, \quad k \in \mathbb{Z}$$

$$a^i = a^j \cdot a^{ke}$$

$$= a^j (a^e)^k \pmod m$$

$$\equiv a^j \pmod m$$

■

- $\operatorname{ord}_m a = e$

  $a, a^2, \ldots, a^e$ are incongruent to each other modulo m.

$$\operatorname{Ord}_m (a^k) = \frac{\operatorname{ord}_m a}{(k, \operatorname{ord}_m a)} = \frac{e}{(k,e)}$$

There are $\phi(\operatorname{ord}_m a)$ numbers that have same order as a^k.

$\phi^{11}(e)$

Proof:

Suppose $d = (k,e)$

$d \mid k \Rightarrow k = k_1 d$

$e = e_1 d$

$(k_1, e_1) = 1$.

To prove:

$$\operatorname{Ord}_m a^k = \frac{e}{d}$$

$$(a^k)^{e/d} = (a^e)^{k/d}$$

$$\equiv 1^{k/d}$$

$$\equiv 1 \pmod m$$

To show:

It is the smallest such

Suppose $\exists\ l$ st

$$a^{kl} \equiv 1 \pmod m$$

But $\text{ord}_m a = e$

$\Rightarrow e \mid kl$

$\rightarrow \frac{e}{d} \mid \frac{k}{d} l$

$\Rightarrow \frac{e}{d} \mid l$

$\Rightarrow \frac{e}{d} \leq l$

Problem

$\text{ord}_{13} 2 = 12$

$\text{ord}_{13} 2^3 = \frac{12}{(3,12)} = 4$

$\text{ord}_{13} 2^4 = \frac{12}{(4,12)} = 3$

$\phi(13) = 12$

$1, 2, 3, 4, 6, 12$

$2^{12} \equiv 1 \pmod{13}$

$\text{ord}_m a^r = \frac{e}{(k,e)}$

$\text{ord}_{13} 2$

$\varphi(13) = 12$

check $1, 2, 3, 4, 6, 12$

$2 \equiv 2$

$2^2 \equiv 4$

$2^3 \equiv -5$

$2^4 \equiv 16 \equiv 3$

$2^6 \equiv 25 \equiv -1 \pmod{13}$

$\boxed{2^{12} \equiv 1}$

Primitive root modulo m

- Let $a, m \in \mathbb{N}$, $(a,m) = 1$. Then a is called primitive root modulo m if $\operatorname{ord}_m a = \phi(m)$. (i.e., $e = \varphi(m)$)
- There is no guarantee of existence.

$a \equiv b \pmod m$ ↳ same order

Example:

- 2 is primitive root mod 13.
- # of primitive roots $= \phi(m)$

Argue:

$$\underbrace{a, a^2, \dots, a^{\phi(m)}}_{a_1, a_2, \dots, a_{\phi(m)}}$$

$\phi(\phi(m)) \longrightarrow$ redo.

Recall

$(a, m) = 1$

$\operatorname{ord}_m a$ = Smallest e such that $a^e \equiv 1 \pmod m$

- $\operatorname{ord}_m a \mid \phi(m)$
- If $a^i \equiv a^j \pmod m$
  $i \equiv j \pmod{\operatorname{ord}_m a}$
- $\operatorname{ord}_m a^k = \dfrac{\operatorname{ord}_m a}{(k, \operatorname{ord}_m a)}$
- a is called primitive root mod m if $\operatorname{ord}_m a = \phi(m)$

Result

If α is a primitive root modulo m, and $a_1, a_2, \ldots, a_{\phi(m)}$ are positive integers st $a_i \leq m$

and $(a_i, m) = 1$

then least residues $\alpha, \alpha^2, \ldots, \alpha^{\phi(m)} \bmod m$ is permutation of $a_1, a_2, \ldots, a_{\phi(m)}$.

Proof: (Redo from book)

Recall: $a \equiv r \pmod m$

$(a, m) = (r, m)$

$(\alpha^i, m) = 1$

$\forall \quad 1 \leq i \leq \phi(m)$

$\alpha^i \equiv a_j \pmod m$

$\{\alpha, \alpha^2, \ldots, \alpha^{\phi(m)}\}$

We want to count the # of primitive roots.

If a is a primitive root mod m, how many incongruent primitive roots are there?

Brute force: check for all $a_1, a_2, \ldots, a_{\phi(m)}$. Time consuming.

Problem:

Find all incongruent primitive roots modulo 19

- $\text{ord}_{19} 1 = 1$
  $\phi(19) = 18$
  $2^9 \equiv -1 \mod 19$
  $2^{18} \equiv 1 \pmod{19}$

Thus 2 is a primitive root.

$\{2^k : (k, 18) = 1\}$

$\{2, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}\}$

$\varphi(19) = 1$

$(k, 18) = 1$ $k = 1, 3, 5, 7, 11, 13, 17$

$\{a, , a^5, a^7, a^{11}, a^{13}, a^{17}\}$

mod 19

$\{8, 3, 10, 14, 13, 15\}$

Find a primitive root mod 8 $\qquad \varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$

$\phi(8) = \phi(2^3)$

$= 2^3 - 2^2$

$= 8 - 4$

$= 4$

$\{1, 3, 5, 7\}$

$\text{ord}_8 3 = 2$

$\text{ord}_8 5 = 2$

$\text{ord}_8 7 = 2$

$\therefore \nexists$ a primitive root.

Prime numbers have primitive roots (next class)

Primality test

Lucas primality Test

Let $n \in \mathbb{Z}^{>0}$. If $\exists$ a positive integer x such that $x^{n-1} \equiv 1 \pmod n$ and $x^{\frac{n-1}{q}} \not\equiv 1 \pmod n$ for any prime divisor q of $n-1$, then n is a prime.

Proof

$\text{ord}_n x = e$

Then $e \mid n-1$

$\Rightarrow n-1 = ek$

If $k > 1$, then k has a prime divisor, call it q.

$$x^{n-1/q} = x^{ek/q}$$

$$= (x^e)^{k/q} \pmod n$$

$$\equiv 1 \pmod n$$

But $x^{n-1/q} \not\equiv 1 \pmod n$

$\rightarrow\leftarrow$

$\therefore k = 1$

$\text{ord}_n x = n-1$

We are left to show n is a prime.

Recall that

$$\text{ord}_n x \mid \phi(n)$$

$\Rightarrow n-1 \mid \phi(n)$

$\Rightarrow \phi(n) = n-1$

$\Rightarrow n$ is a prime.

Problem:

If $p>3$ has a primitive root, then it has even number of primitive roots.

- $\phi(n)$ is even $\forall\ n \geq 3$
- $\phi(\phi(p)) = \phi(p-1)$ is even. Done.

If a^{-1} is the multiplicative inverse of $a \bmod m$, $(a,m)=1$, Then

$$\text{ord}_m a = \text{ord}_m a^{-1}$$

Note that $aa^{-1} \equiv 1 \pmod m$

Let $\operatorname{ord}_m a = e$.

$$a^e (a^{-1})^e \equiv 1 \pmod m$$
$$(a^{-1})^e \equiv 1 \pmod m.$$

To show: e is the smallest

Let $l < e$ st

$$(a^{-1})^l \equiv 1 \pmod m$$
$$a^l (a^{-1})^l \equiv a^l \pmod m$$
$$1 \equiv a^l \pmod m$$

$(a^2)^{-1} = (a^{-1})^2$?

$(a^n)^{-1} = (a^{-1})^n$?

Alt:

$$a^{-1} \equiv a^{e-1} \pmod m$$
$$\operatorname{ord}_m a^{e-1} = \frac{e}{(e-1, e)} = 1$$

In particular, if a is primitive root, so is its inverse.

Thm: For any prime p, $\exists$ an element of order $p-1$. ???

Lemma-1:

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree 'n' and $p \nmid a_n$ where a_n is the leading coefficient in $f(x)$.

Then $f(x) \equiv 0 \pmod p$ has atmost n incongruent solutions.

Proof:

We proceed by induction on n.

$n = 1$

$f(x) = a_1 x + a_0$, $p \nmid a_1$

$$a_1 x + a_0 \equiv 0 \pmod p$$

$$a_1 x \equiv -a_0 \pmod p$$

is the reqd soln.

$\therefore$ Holds for $n = 1$.

Suppose the result holds for $n = k$. Let $g(x)$ be a polynomial of degree $k+1$.

To solve:

$$g(x) \equiv 0 \pmod p \longrightarrow (1)$$

Case-1 : (1) has no soln

We have nothing to prove.

Case-2 : Suppose (1) has a soln, say α.

$$\Rightarrow g(\alpha) \equiv 0 \pmod p$$

$$\Rightarrow g(x) = (x-\alpha)\bar{g}(x) + r$$

$$g(\alpha) = (\alpha-\alpha)\bar{g}(\alpha) + r \pmod p$$

$$\Rightarrow r \equiv 0 \mod p$$

$$\Rightarrow g(x) = (x-\alpha)\bar{g}(x) \mod p$$

Suppose β is any other (incongruent) soln of (1):

$$\Rightarrow g(\beta) \equiv 0 \pmod p$$

$$g(\beta) = (\beta-\alpha)\bar{g}(\beta) \pmod p$$

$$\Rightarrow (\beta-\alpha)\bar{g}(\beta) \equiv 0 \pmod p$$

$$\Rightarrow \bar{g}(\beta) \equiv 0 \pmod p \qquad (\beta \not\equiv \alpha \mod p)$$

Corollary:

Let p be a prime, and $d \mid p-1$. Then

$x^d - 1 \equiv 0 \pmod p$ has exactly d solutions.

(*)

Proof

By FLT,

$$x^{p-1} \equiv 1 \pmod{p}$$

has exactly $p-1$ incongruent solns $(1, \ldots, p-1)$.

We have $d \mid p-1$

$$\rightarrow x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \ldots + x^d + 1)$$

$$= (x^d - 1)\, g(x)$$

where $g(x) = x^{p-1-d} + \ldots + x^d + 1$

By Lemma 1,

$$g(x) \equiv 0 \pmod{p}$$

has atmost $\deg(g(x)) = p-1-d$ solns modulo p.

Then $x^d - 1 \equiv 0 \pmod{p}$ has

atleast $(p-1) - (p-1-d) = d$ incongruent solns.

$$\therefore \#\text{Solutions} \geq d$$

Invoke lemma ① directly on ⊛,

$$\#\text{ solutions} \leq d$$

$$\Rightarrow \boxed{\#\text{ solutions} = d}$$

Lemma-3: Let p be a prime, and $d \mid p-1$. $\exists$ exactly $\phi(d)$ incongruent integers of order d modulo p.

Proof:

Notation:

$$\psi(d) = \#\{a \in \mathbb{N} : 1 \le a \le p-1 \text{ and } \operatorname{ord}_p a = d\}$$

$$\sum_{d \mid p-1} \psi(d) = p-1$$

Also $$\sum_{d \mid p-1} \phi(d) = p-1$$

Case-1:

If $\psi(d) = 0$, $\psi(d) \le \phi(d)$

Case-2:

If $\psi(d) \neq 0$

Let a be an element of order $d \pmod p$

Consider $a, a^2, \ldots, a^d$ are incongruent mod p.

There are exactly $\phi(d)$ integers.

Theorem

① Given a prime p, $\exists$ a primitive root of p.

② In fact, $\exists$ exactly $\phi(p-1)$ incongruent primitive roots.

Q: Let α be a primitive root modulo p. (p is odd prime). Find the remainder when $\alpha^{p-1/2}$ is divided by p.

Soln.

$$\alpha^{p-1} \equiv 1 \pmod p$$

$$\left(\alpha^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$$

$\Rightarrow p \mid \left(\alpha^{\frac{p-1}{2}}\right)^2 - 1$

$\Rightarrow p \mid \alpha^{p-1/2} - 1$ or $p \mid \alpha^{p-1/2} + 1$

$\Rightarrow \alpha^{p-1/2} \equiv -1 \pmod p$

$\Rightarrow \boxed{\alpha^{\frac{p-1}{2}} \equiv p-1 \mod p}$

Q: Let α be a primitive root modulo p, where $p \equiv 1 \pmod 4$

PT: $\alpha^{p-1/4}$ is a soln of $x^2+1 \equiv 0 \pmod p$

Same as above.

Q: Let α be a primitive root modulo p^j, $j \geq 1$, α odd, p odd. Then α is a primitive root modulo $2p^j$

$$\phi(2p^j) = \phi(2)\,\phi(p^j)$$

$$= \phi(p^j)$$

$$\alpha^{\phi(2p^j)} = \alpha^{\phi(p^j)} \equiv 1 \pmod{p^j} \quad \rightarrow ①$$

Also $\alpha \equiv 1 \pmod 2$ $\rightarrow ②$

$\Rightarrow \alpha^{\phi(2p^j)} \equiv 1 \pmod{2p^j}$

Verify order.

Q: Let α be a primitive root modulo p, and p is odd.

Then $\alpha^{p-2} + \alpha^{p-3} + \dots + \alpha + 1 \equiv 0 \pmod{p}$

$$1 + \alpha + \dots + \alpha^{p-2} = \frac{(1)(\alpha)^{p-1} - 1}{\alpha - 1}$$

$$= \frac{1 - \alpha^{p-1}}{1 - \alpha}$$

We have $\alpha^{p-1} \equiv 1 \pmod{p}$

$$\alpha^{p-1} - 1 \equiv 0 \pmod{p}$$

$$(\alpha - 1)(1 + \alpha + \dots + \alpha^{p-2}) \equiv 0 \pmod{p}$$

Now $\alpha \neq 1$.

Quadratic residues

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

where p is an odd prime.

Also, $p \nmid a$. If not, it becomes linear.

$$4A(Ax^2 + Bx + c) \equiv 0 \pmod{p}$$

$$(2Ax + B)^2 + 4AC - B^2 \equiv 0 \pmod{p}$$

$$(2Ax + B)^2 \equiv B^2 - 4AC \pmod{p}$$

We will consider the congruence of the type

$$x^2 \equiv a \pmod{p}$$

Eg:

$$3x^2 - 4x + 7 \equiv 0 \pmod{13}$$

$$(6x - 4)^2 \equiv 10 \pmod{13}$$

$$y = 6x - 4$$

$$y^2 \equiv 10 \pmod{13}$$

$$y = 6, 7$$

$6x \equiv y+4 \pmod{13}$

$x \equiv -2(y+4) \pmod{13}$

$x = 4, 6 \pmod{13}$

Quadratic Residues

$$x^2 \equiv a \pmod{m} \quad \text{—} (*)$$

Let $m \in \mathbb{Z}^{>0}$ and a be any integer st $(a,m) = 1$. Then a is called quadratic residue modulo m if $(*)$ is solvable. Otherwise a is called quadratic non-residue modulo m.

Eg:

$a = 5, \quad m = 13$.

$x^2 \equiv 5 \pmod{13}$

$\therefore$ 5 is quadratic non-residue mod 13.

Suppose $a \equiv b \pmod{m}$.

Then a is quadratic residue modulo $m \iff b$ is quadratic residue mod m.

List of quadratic residues mod 13.

$12^2 \equiv 1^2 \equiv 1 \pmod{13}$

$11^2 \equiv 2^2 \equiv 4$

$10^2 \equiv 3^2 \equiv 9$

$9^2 \equiv 4^2 \equiv 3$

$8^2 \equiv 5^2 \equiv 12$

$7^2 \equiv 6^2 \equiv 10$

Quadratic residues are 1, 4, 9, 3, 12, 10

Quadratic non-residues are 2, 5, 6, 7, 8, 11,

Result

Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues.

Proof:

Suppose p has k (incongruent) quadratic residues. Each congruence can yield 2 solutions $\Rightarrow 2k$ solutions. The squares of least residues are $1, 2, \ldots, p-1$ $\therefore p-1$ in number.

$$2k = p-1 \Rightarrow k = \frac{p-1}{2} \text{ quadratic residues}$$

$$\#\text{ of non residues} = p-1 - \left(\frac{p-1}{2}\right) = \frac{p-1}{2}$$

Suppose $x^2 \equiv a \pmod p \rightarrow ①$

p is an odd prime, $(a, p) = 1$.

- It can have atmost 2 incongruent solutions.
- ① has either 0 or 2 solutions.

If $x_0^2 \equiv a \pmod p$

Then $x_1 = p - x_0$

$$x_1^2 = (p - x_0)^2$$

$$\equiv x_0^2 \equiv a \pmod p$$

Euler's criterion

- Tells is 'a' quadratic residue?

Let $(a, p) = 1$, p is an odd prime. Then 'a' is quadratic residue modulo p

$$\leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Proof:

Suppose $x_0^2 \equiv a \pmod p$

$$x_0^{p-1} \equiv a^{p-1/2} \pmod p$$

$$\Rightarrow a^{p-1/2} \equiv 1 \pmod p \quad [FLT]$$

Conversely, assume $a^{p-1/2} \equiv 1 \pmod p$.

Since for any odd prime p, there exist primitive roots, say α.

Consider $\alpha, \alpha^2, \ldots, \alpha^{p-1}$.

$a \equiv \alpha^k \pmod p$ for some k; $1 \le k \le p-1$

$$a^{p-1/2} = (\alpha^k)^{p-1/2} \pmod p$$

$$\Rightarrow (\alpha^k)^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Claim: k has to be even.

As α is a primitive root, and p is a prime

$$\text{ord}_p \alpha = p-1$$

$$\Rightarrow p-1 \mid \frac{k(p-1)}{2}$$

$\Leftrightarrow$ k is an even integer, say $k = 2i$.

Then $a = \alpha^{2i} \equiv (\alpha^i)^2 \pmod p$

Let p be an odd prime, $a \in \mathbb{Z}^{\geq 0}$, and $(p,a) = 1$.

a is a quadratic non-residue $\Leftrightarrow a^{p-1/2} \equiv (-1) \bmod p$

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

$$a^{p-1} - 1 \equiv 0 \pmod p$$

$$\left(a^{p-1/2} - 1\right)\left(a^{p-1/2} + 1\right) \equiv 0 \pmod p$$

$$\therefore a^{p-1/2} \equiv -1 \pmod p$$

as other case is for quadratic residue.

$\Leftarrow$ Suppose $(p,a) = 1$ and $a^{p-1/2} \equiv -1 \pmod p$

If a is quadratic residue, $-1 \equiv 1 \pmod p$

$$\Rightarrow 2 \equiv 0 \pmod p$$

$$\Rightarrow p = 2$$

$\rightarrow\leftarrow$.

Legendre Symbol

Let p be an odd prime. Let $a \in \mathbb{Z}^{\geq 0}$ st $(p,a) = 1$.

The $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is quadratic residue of } p \\ -1, & \text{otherwise} \end{cases}$$

- Let p be an odd prime, $a \in \mathbb{Z}^{\geq 0}$ st $(a,p) = 1$. a is a quadratic residue of $p \Leftrightarrow \left(\frac{a}{p}\right) = 1$.

Note: $x^2 \equiv a \pmod p$ is solvable $\Leftrightarrow \left(\frac{a}{p}\right) = 1$.

Theorem:

Let p be an odd prime, $a, b \in \mathbb{Z}$ with $p \nmid ab$.

① If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Suppose $a \equiv b \pmod p$

$x^2 \equiv a \pmod p$ is solvable iff $x^2 \equiv b \pmod p$ is solvable

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

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

$\left(\frac{ab}{p}\right) \equiv (ab)^{p-1/2} \pmod p$

$\equiv (a^{p-1/2})(b^{p-1/2})$

$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$

③ $\left(\frac{a^2}{p}\right) = 1$

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

In each case evaluates to 1.

- If $a \equiv b \pmod p$, then either both are quadratic residues or both are quadratic nonresidues.
- The product of two quadratic residues is a quadratic residue.
- The product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.
- The product of two quadratic nonresidues is a quadratic residue.
- The square of every integer relatively prime to p is a quadratic residue.

Thm: Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = (-1)^{p-1/2}$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv -1 \pmod 4 \end{cases}$$

$\left(\frac{-1}{p}\right) = (-1)^{p-1/2} \pmod p$

$= \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$

Eg: $\left(\frac{-4}{41}\right) = \left(\frac{-1}{41}\right)\left(\frac{4}{41}\right)$

$= \left(\frac{4}{41}\right) = 1$

$\left(\frac{-9}{83}\right) = \left(\frac{-1}{83}\right)\left(\frac{3^2}{83}\right)$

$= -1$

Legendre's symbol

$(a, p) = 1$, p is prime

$$\left(\frac{a}{p}\right) = \left(a/p\right) = \begin{cases} 1 & a \text{ is quad residue} \\ -1 & a \text{ is quad residue} \end{cases}$$

Note:

$$\left(\frac{a^3}{p}\right) = \left(\frac{a}{p}\right)^3 = \left(\frac{a}{p}\right)$$

$(a, p) = 1$

$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

$$\left(a/p\right) = \left(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}/p\right)$$

$$= \left(p_1^{e_1}/p\right)\left(p_2^{e_2}/p\right)\cdots\left(p_k^{e_k}/p\right)$$

$$= \prod_{i=1}^{k} \left(p_i/p\right)^{e_i}$$

- $\left(ab/p\right) = \left(a/p\right)\left(b/p\right)$ given $a \equiv b \pmod p$
- $\left(p+2/p\right) = \left(2/p\right)$ Since $p+2 \equiv 2 \mod p$

Example.

$$\left(\frac{5000}{23}\right) = \left(2^3 \times 5^4/23\right)$$

$5000 = 5 \times (5\times 2)^3 = 5^4 \times 2^3$

$$= \left(5/23\right)^4 \times \left(2/23\right)^3$$

$$= \left(2/23\right)$$

$$= 1$$

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

$= \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$

② $\left(\frac{-9}{83}\right) = \left(\frac{-1}{83}\right)\left(\frac{9}{83}\right)$

$= -1$

Gauss Lemma

Let p be an odd prime, and $a \in \mathbb{Z}$ st $(a,p) = 1$. If n denotes the number of least residues modulo p of integers $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ that exceed $p/2$, then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Example:

$p = 13$

$a = 5$

$\frac{p-1}{2} = 6$

$\{a, 2a, \ldots, 6a\}$

$= \{5, 10, 15, 20, 25, 30\}$

mod p

$= \{5, 10, 2, 7, 12, 4\}$

$\frac{p}{2} = \frac{13}{2} = 6.5$

$n = 3$

$\left(\frac{a}{p}\right) = (-1)^3$

$= -1$

② $\left(\frac{10}{13}\right)$ $a = 10$

$p = 13$

$\frac{p-1}{2} = \frac{12}{2} = 6$

$a, 2a, \ldots, 6a$

$\{10, 20, 30, 40, 50, 60\}$

mod 13 $= \{\dot{10}, \dot{7}, 4, 1, \dot{11}, \dot{8}\}$

$\frac{p}{2} = \frac{13}{2} = 6.5$

$n = 4$

$\left(\frac{10}{13}\right) = 1$

③ $\left(\frac{7}{13}\right)$ $a = 7$

$p = 13$

$\frac{p-1}{2} = 6$

$7, 14, 21, 28, 35, 42$

mod 13 $= \{\dot{7}, 1, \dot{8}, 2, \dot{9}, 3\}$

$\frac{p}{2} = 6.5$ $n = 3$

$\left(\frac{7}{13}\right) = -1$

④ $\left(\frac{2}{13}\right)$ $a = 2$

$p = 13$

$\frac{p-1}{2} = 6$ $\{2, 4, 6, 8, 10, 12\}$

$\{2, 4, 6, \tilde{8}, \tilde{10}, \tilde{12}\}$

$p/2 = 6.5$

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

Using the lemma, find $\left(\frac{3}{23}\right)$

$a = 3$

$p = 23$

$\frac{p-1}{2} = 11$

$\{3, 6, 9, 12, 15, \ldots, 33\}$

mod 23 $= \{3, 6, 9, \underline{12}, \underline{15}, \underline{18}, \underline{21}, 1, 4, 7, 10\}$

$\frac{p}{2} = \frac{23}{2} = 11.5$

$n = 4$

$\left(\frac{3}{23}\right) = (-1)^4$

$= 1$

Other way

$3 \equiv 49 \pmod{23}$

$\equiv 7^2 \pmod{23}$

Recall

- Let p be an odd prime.
- Let $a \in \mathbb{Z}$ st $(a,p) = 1$
- If $x^2 \equiv a \pmod{p}$ has a soln, a is quadratic residue mod p.
- $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is quad} \\ -1 \end{cases}$
- $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ if $(a,p) = 1 = (b,p)$

Euler's Criterion.

$$\left(\frac{a}{p}\right) \equiv a^{p-1/2} \pmod{p}$$

Gauss Lemma

Let $(a,p) = 1$ and let n be the # of least residues of integers $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ that exceed $p/2$. Then $\left(\frac{a}{p}\right) = (-1)^n$.

Eg:

What is $\left(\frac{2}{p}\right)$

$S = \{2, 2\cdot 2, \ldots, \frac{p-1}{2}\cdot 2\}$ $\qquad 1 \le r \le \frac{p-1}{2}$

No need to reduce mod p.

n = # of integers in S that exceed $p/2$ $\qquad 2r < p/2$

$= \left(\frac{p-1}{2}\right) - \{\#$ of integers in S that are $\le p/2\}$ $\qquad r < p/4$

$= \left(\frac{p-1}{2}\right) - \{r : r < p/4\}$

$= \left(\frac{p-1}{2}\right) - \lfloor p/4 \rfloor$

$p = 4k+1$

$\frac{p-1}{2} = 2k$

$\left[\frac{p}{4}\right] = \left[\frac{4k+1}{4}\right]$

$= k$

$\Rightarrow$ can't conclude anything.

Case-1 :

$p \equiv 1 \pmod 8$

$p = 8k+1$

$n = 4k - 2k = 2k$

even

Case-2 :

$p \equiv 3 \pmod 8$

$p = 8k+3$

$n = 4k+1-2k = 2k+1$

odd

Case-3

$p \equiv 5 \pmod 8$

$p = 5 + 8k$

$n = 4k+2-(2k+1) = 2k+1$

Case-4

$p \equiv 7 \pmod 8$

$p = 7 + 8k$

$n = 4k+3-2k-1$

$= 2k+2$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8 \end{cases}$$

Problems

① $\left(\frac{8}{19}\right) = \left(\frac{2}{19}\right)^3 = \left(\frac{2}{19}\right) = -1$

② $\left(\frac{13}{31}\right) = \left(\frac{-18}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{9}{31}\right)\left(\frac{2}{31}\right)$

$= (-1)(1) = -1$

Note:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Eg: $\left(\frac{7}{43}\right)$

- Motivation for quadratic reciprocity

$$\left(\frac{7}{43}\right) = \left(\frac{43}{7}\right) ?$$

$a \equiv b \pmod p$

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

Quadratic Reciprocity Laws:

Suppose p and q are distinct odd primes.

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

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

Eg: $\left(\frac{7}{43}\right)$

$p = 7$

$q = 43$

$$\left(\frac{7}{43}\right) = (-1)\left(\frac{43}{7}\right)$$

$$= (-1)\left(\frac{1}{7}\right) \rightarrow \text{Square}$$

$$= -1$$

When is $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$?

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$

$= -\left(\frac{q}{p}\right)$ if $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$

(Eg): $\left(\frac{3}{101}\right)$ $p = 3$, $q = 101$

$= \left(\frac{101}{3}\right)$

$= \left(\frac{2}{3}\right)$

$= -1$

Eg: $\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0$

Eg: $\left(\frac{153}{43}\right) = \left(\frac{24}{43}\right) = -\left(\frac{43}{24}\right) = -\left(\frac{2}{43}\right)\left(\frac{3}{43}\right)$ <Redo>

$p = 27$

$q = 43$

$= (-1)(1)$

$= (+1)$

Eg: Let $p = 4a + q$, p, q are distinct odd primes. PT:

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

Case-1: $q \equiv 1 \pmod 4$

$$\left(\frac{a}{p}\right) = \left(\frac{a}{4a+q}\right) = \left(\frac{4a+q}{a}\right) = \left(\frac{q}{a}\right) = \left(\frac{a}{q}\right)$$

Case-2: $q \equiv 3 \pmod 4$ {Then $p \equiv 3 \pmod 4$ as well}

$$\left(\frac{a}{p}\right) = \left(\frac{a}{4a+q}\right) = -\left(\frac{4a+q}{a}\right) = -\left(\frac{q}{a}\right) = \left(\frac{a}{q}\right)$$

Alt:

$$\left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$$

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

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

If $p \equiv 1 \pmod 4$

$$= (1)\left(\frac{a}{a}\right)$$

If $p \equiv 3 \pmod 4$

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

Problems

$(3, p) = 1$, p is a prime.

$$\left(\frac{3}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)}\left(\frac{p}{3}\right)$$

$$= \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) & \text{if } p \equiv 1 \pmod 3 \\ \left(\frac{2}{3}\right) & \text{if } p \equiv 2 \pmod 3 \end{cases} \qquad a/p$$

$$= \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

mod 12
1, 5, 7, 11

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & p \equiv 1, 11 \pmod{12} \\ -1, & p \equiv 5, 7 \pmod{12} \end{cases}$$

$p \equiv 7 \pmod{12}$

Eg:

$$\left(\frac{3}{71}\right) = 1$$

Similary can do for $\left(\frac{3}{p}\right)$

Ex: Derive for $\left(\frac{5}{p}\right)$ where $p \to$ odd prime

$(5, p) = 1$

$(5, p) = 1$

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\left(\frac{5}{2}\right)\left(\frac{p-1}{2}\right)}$$

$$= \left(\frac{p}{5}\right)(-1)^{p-1}$$

As p is odd prime,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

$$\left(\frac{p}{5}\right) = \begin{cases} \left(\frac{1}{5}\right) & p \equiv 1 \pmod 5 \\ \left(\frac{2}{5}\right) & p \equiv 2 \pmod 5 \\ \left(\frac{3}{5}\right) & p \equiv 3 \pmod 5 \\ 1 & p \equiv 4 \pmod 5 \end{cases}$$

$\frac{1}{5}$ $1^2 \equiv 1 \pmod p$

$\left(\frac{2}{5}\right)$ $2^2 \equiv -1 \pmod 5$

$\left(\frac{3}{5}\right)$ $3^2 \equiv -1$

$$= \begin{cases} 1 & p \equiv \pm 1 \pmod 5 \\ -1 & p \equiv \pm 2 \pmod 5 \end{cases}$$

Problem

Let p be an odd prime, $(p,5) = 1$.

Prove that

$$\left(\frac{5^{-1}}{p}\right) = \left(\frac{p^{-1}}{5}\right)$$

Let $a = 5^{-1}$

$b = p^{-1}$

$5a \equiv 1 \pmod{p}$

$bp \equiv 1 \pmod{5}$

To show: $\left(\frac{a}{p}\right) = \left(\frac{b}{5}\right)$

$$\left(\frac{5a}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{a}{p}\right)$$

$$1 = \left(\frac{5}{p}\right)\left(\frac{a}{p}\right) \longrightarrow (1)$$

Ily

$$1 = \left(\frac{b}{5}\right)\left(\frac{p}{5}\right) \longrightarrow (2)$$

By QRT,

$$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) \longrightarrow (3)$$

From (1), (2), (3)

$$\left(\frac{a}{p}\right) = \left(\frac{b}{5}\right)$$

Jacobi Symbol

Let m be an odd positive integer, and $(a, m) = 1$.

Suppose $m = p_1^{e_1} \cdots p_k^{e_k}$

$$\left(\frac{a}{m}\right) = \left(\frac{a}{\prod_{i=1}^{k} p_i^{e_i}}\right)$$

$$= \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

When m is a prime, Jacobi symbol is same as Legendre symbol.

Eg

$$\left(\frac{55}{273}\right)_J = \left(\frac{55}{3}\right)\left(\frac{55}{7}\right)\left(\frac{55}{13}\right)$$

$273 = 3 \cdot 7 \cdot 13$

$$= \left(\frac{1}{3}\right)\left(\frac{-1}{7}\right)\left(\frac{3}{13}\right)$$

$$= 1 \cdot -1 \cdot 1$$

$$= -1$$

- Whenever Jacobi symbol is -1, it is not quadratic residue

Otherwise, cant say anything.

If a is quadratic residue mod m,

$$x^2 \equiv a \pmod{m}$$

has a soln, then $\left(\frac{a}{m}\right) = 1$

$\rightarrow$ $x^2 \equiv a \pmod{p_i}$

$\Downarrow$

$\left(\frac{a}{p_i}\right) = 1$

Suppose $m = \prod_{i=1}^{k} p_i^{e_i}$

$$\left(\frac{a}{m}\right) = \left(\frac{a}{\prod p_i^{e_i}}\right) = \prod \left(\frac{a}{p_i}\right)^{e_i} = 1$$

Eg:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)$$
$$= (-1)(-1)$$
$$= 1.$$

$\exists x$ st $x^2 \equiv 2 \pmod{15}$

Theorem:

Let m be an odd integer, and $(a, m) = (b, m) = 1$. Then

① If $a \equiv b \pmod{m}$, then $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

② $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$

③ $\left(\frac{a^2}{m}\right) = 1.$

Generalised Quadratic Reciprocity Law.

Let m and n be odd integers st $(m, n) = 1$

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1/2)(n-1/2)}$$

$$m = \prod_{j=1}^{k} p_i^{e_i}$$
$$n = \prod_{i=1}^{l} q_i^{s_i}$$

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{l} \left(\frac{m}{q_i}\right)^{s_i}$$

$$= \prod_{j=1}^{l} \prod_{j=1}^{k} \left(\frac{p_i}{q_i}\right)^{e_i s_j}$$

Find the value of

$$\left(\frac{411}{2587}\right) = \left(\frac{3}{2587}\right)\left(\frac{137}{2587}\right)$$

$411 = 3 \cdot 137$

$2587 =$

$$= -\left(\frac{2587}{3}\right)\left(\frac{2587}{137}\right)$$

$$= -\left(\frac{1}{3}\right)\left(\frac{121}{137}\right)$$

$$= -(1)(1)$$

$$= -1$$

411 is not quadratic residue modulo 2587.

Continued Fractions

Suppose $r \in \mathbb{R}$, $r \in \mathbb{Q}$.

- $\exists$ a sequence in $\mathbb{Q}$ that converges to r.
- Goal: construct such a sequence.

Finite Continued Fractions

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{\ddots}{a_{n-1} + \cfrac{1}{a_n}}}}$$

where $\{a_i\}_{i=0}^{n} \in \mathbb{R}$, $\{a_i\}_{i=1}^{n} > 0$

- a_0 can be ≥ 0 or < 0.

$a_1, a_2, \ldots, a_n$ are called partial quotients.

- If $a_i \in \mathbb{Z}$ $\forall$ $0 \leq i \leq n$, this expression is called finite simple continued fractions.

Eg: $\frac{15}{11} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + 1/3}}$

Notation: $x = [a_0; a_1, \ldots, a_n]$

In the above example,

$\frac{15}{11} = [1; 2, 1, 3]$.

Theorem: Every finite simple continued fraction represents a rational number.

Proof:

Let $x = [a_0; a_1, a_2, \ldots a_n]$

Base case: $n = 0$

$x = a_0 \in \mathbb{Q}$

Holds true for $n = 0$

Suppose the result holds for any simple finite c.f with $\leq k \left\{ x = [a_0; a_1, \ldots, a_{k-1}] \in \mathbb{Q} \right\}$

$x = [a_0; a_1, \ldots, a_k] \in \mathbb{Q}$

$= a_0 + \cfrac{1}{[a_1; \ldots, a_k]}$

$= a_0 + \frac{1}{r}$, $r \in \mathbb{Q}$

$\in \mathbb{Q}$

Theorem:

Any rational number can be expressed as a simple finite continued fraction.

Proof:

Let $r \in \mathbb{Q}$

$r = \frac{a}{b}$, $(a, b) = 1$, $a, b \in \mathbb{Z}$, $b > 0$.

Suppose $a = q_1 b + r$

$$\frac{a}{b} = q_1 + \frac{r}{b}$$

$$= q_1 + \frac{1}{\frac{b}{r_1}}$$

$b = q_2 r_1 + r_2 \qquad 0 \le r_2 < r_1$

$$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1}$$

$$\therefore \frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}}$$

$$= q_1 + \frac{1}{q_2 + \frac{1}{\left(\frac{r_1}{r_2}\right)}}$$

- Continuing like this, we get $r_i = 0$ after some iterations (at most b many)
- $r = \frac{a}{b} = [q_1; q_2, q_3, \ldots q_i]$

Example :

$$\frac{23}{13} = 1 + \frac{10}{13}$$

$$= 1 + \frac{1}{\left(\frac{13}{10}\right)}$$

$$= 1 + \frac{1}{1 + \frac{3}{10}}$$

$$= 1 + \frac{1}{1 + \frac{1}{\left(\frac{10}{3}\right)}}$$

$$= 1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{3}}}$$

$$= [1; 1, 3, 3]$$

Convergent of x

Let $x = [a_0; a_1, \ldots, a_n]$ → $n+1$ partial quotients

k^{th} convergent $c_k = [a_0; a_1, \ldots, a_k]$

$0 \le k \le n$

- n^{th} convergent $= x$.

Eg:

$\frac{21}{13} = [1; 1, 1, 1, 1, 1, 1]$

$c_0 = [1] = 1$

$c_1 = [1; 1] = 1 + \frac{1}{1} = 2$

$c_2 = [1; 1, 1] = 1 + \frac{1}{1 + \frac{1}{1}} = 1 + \frac{1}{2} = 3/2 \approx 1.5$

$c_3 = [1; 1, 1, 1,] = 5/3 \approx 1.66$

$c_4 = [1; 1, 1, 1, 1] = 8/5 \approx 1.60$

$c_5 \approx 1.625$

$c_6 \approx 1.615$

$c_0 < c_2 < c_4 < c_6 < c_5 < c_3 < c_1$

- c_{2i} is an increasing seq (approaching c_n)
- c_{2i+1} is a decreasing seq (approaching c_n)
- Both are monotonic sequences.

Recurrences

Thm: Let $c_k = \frac{p_k}{q_k}$ be the k^{th} convergent of the simple continued fraction $[a_0; a_1, \ldots, a_n]$, where $0 \le k \le n$. Define them as follows.

$p_0 = a_0$ $\quad$ $q_0 = 1$

$p_1 = a_0 a_1 + 1$ $\quad$ $q_1 = a_1$

$p_k = a_k p_{k-1} + p_{k-2}$ $\quad$ $q_k = a_k q_{k-1} + q_{k-2}$

Proof

$$c_0 = [a_0] = \frac{a_0}{1} = a_0$$

$$c_1 = [a_0; a_1] = a_0 + \frac{1}{a_1 + 1} =$$

We shall use induction.

Suppose, this result holds for any finite simple continued fraction having m partial quotients.

$$c_{m+1} = [a_0; a_1, \ldots, a_{m+1}]$$

$$= \left[a_0; a_1, \ldots, a_m + \frac{1}{a_{m+1}}\right]$$

$$= \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}}$$

$$= \frac{(a_m a_{m+1}) p_{m-1} + p_{m-1} + a_{m+1} p_{m-2}}{(a_m a_{m+1}) q_{m-1} + a_{m+1} q_{m-2} + q_{m-1}}$$

$$= \frac{(a_{m+1})(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{(a_{m+1})(a_m q_{m-1} + q_{m-2}) + q_{m-1}}$$

$$= \frac{(a_{m+1}) p_m + p_{m-1}}{(a_{m+1}) q_m + q_{m-1}}$$

$$= \frac{(a_{m+1}) p_{(m+1)-1} + p_{(m+1)-2}}{(a_{m+1}) q_{(m+1)-1} + q_{(m+1)-2}}$$

$$= \frac{p_{m+1}}{q_{m+1}}$$

Thm: Let $c_k = \frac{p_k}{q_k}$ as defined earlier, $1 \le k \le n$.

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$$

$ax + by = 1$

Proof (by induction)

Corollary: $(p_k, q_k) = 1$

Theorem:

$$c_k = \frac{p_k}{q_k} \qquad 0 \le k \le n$$

We have $c_{2i} < c_{2j+2}$

$c_{2i+1} > c_{2i+3}$

$c_{2i} < c_{2j+1} \qquad i, j \ge 0$

$$-(c_{2i} - c_{2i+2}) = -\left(\frac{p_{2i}}{q_{2i}} - \frac{p_{2i+2}}{q_{2i+2}}\right)$$

$$= -\frac{p_{2i} q_{2i+2} + p_{2i+2} q_{2i}}{q_{2i} q_{2i+2}}$$

$$= \frac{p_{2i+2}}{q_{2i+2}} - \frac{p_{2i+1}}{q_{2i+1}} + \frac{p_{2i+1}}{q_{2i+1}} - \frac{p_{2i}}{q_{2i}}$$

$$= \frac{p_{2i+2} q_{2i+1} - p_{2i+1} q_{2i+2}}{q_{2i+2} q_{2i+1}} + \frac{p_{2i+1} q_{2i} - p_{2i} q_{2i+1}}{q_{2i} q_{2i+1}}$$

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

$$= \frac{1}{q_{2i} q_{2i+1}} - \frac{1}{q_{2i+2} q_{2i+1}}$$

$$= \frac{q_{2i+2} - q_{2i}}{q_{2i} q_{2i+1} q_{2i+2}}$$

> 0

Solving LDE using finite simple continued fractions:

$$ax + by = c$$

is solvable $\Leftrightarrow$ $(a,b) \mid c$.

$$\frac{a}{d} + \frac{b}{d} y = \frac{c}{d}, \quad \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

We consider $ax + by = 1$ $\quad (a,b) = 1$

$$\frac{a}{b} \in \mathbb{Q}$$

$$\frac{a}{b} = [a_0; a_1, \ldots, a_n]$$

$$C_{n-1} = \frac{P_{n-1}}{q_{n-1}}$$

$$C_n = \frac{P_n}{q_n} = \frac{a}{b} \qquad P_n = a, \quad q_n = b$$

$$P_n q_{n-1} - P_{n-1} q_n = (-1)^{n-1}$$

$$a q_{n-1} - P_{n-1} b = (-1)^{n-1}$$

If n is odd,

$$x_0 = q_{n-1}$$

$$y_0 = P_{n-1}$$

is a solution.

If n is even,

$$x_0 = -q_{n-1}$$

$$y_0 = P_{n-1}$$

is a soln.

Example

$$172x + 20y = 1000$$

$$43x + 5y = 250 \longrightarrow (1)$$

We consider the LDE

$$43x + 5y = 1 \longrightarrow (2)$$

$$\frac{43}{5} = 8 + \frac{3}{5} = 8 + \frac{1}{5/3} = 8 + \frac{1}{1 + \frac{2}{3}} = 8 + \frac{1}{1 + \frac{1}{(3/2)}} = 8 + \frac{1}{1 + \frac{1}{1 + 1/2}}$$

$$a_0 \; a_1 \; a_2 \; a_3$$

$$= [8; 1, 1, 2]$$

$n = 3$, odd

$x_0 = q_2$

$y_0 = -p_2$

is a soln of (2),

$p_0 = a_0 = 8$ $\qquad$ $q_0 = 1$

$p_1 = a_0 a_1 + 1 = 8(1) + 1 = 9$ $\qquad$ $q_1 = a_1 = 1$

$p_2 = a_2 p_1 + p_0$ $\qquad$ $q_2 = a_2 q_1 + q_0$

$= (1)(9) + 8 = 17$ $\qquad$ $= 1(1) + 1$

$= 2$

$x_0 = q_2 = 2$

$y_0 = -p_2 = -17$

$(2, -17)$ is a soln of (2).

$43 \times 2 + 5 \times -17 = 1$

$43 \times (2 \times 250) + 5 \times (-17 \times 250) = 250$

$(500, -4250)$ is soln of (1).

All soln of (1) are

$x = 500 + 5t$

$y = -4250 - 43t$

Infinite Continued Fraction

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cdots}}}$$

$a_i, b_i \in \mathbb{R} \quad \forall i$

is called infinite continued fraction.

We discuss only infinite continued fractions of the type

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

i.e., $b_i = 1 \quad \forall i$

Moreover, if $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$, then we call it a simple infinite continued fraction.

We can associate this with a sequence:

$$C_n = [a_0, a_1, \ldots, a_n]$$

$\{C_{2n}\}$ is an increasing sequence bounded above and $\{C_{2n+1}\}$ is a decreasing sequence bounded below.

$$\lim_{n\to\infty} C_{2n} = l \qquad \lim_{n\to\infty} C_{2n+1} = l'$$

$$C_{2n+1} - C_{2n} = \frac{(-1)^{2n}}{q_{2n+1}\, q_{2n}} = \frac{1}{q_{2n+1}\, q_{2n}}$$

$$< \frac{1}{q_n^2}$$

When $n \to \infty$

$$\lim_{n\to\infty} C_{2n+1} = \lim_{n\to\infty} C_{2n}$$

$$\Rightarrow l = l'$$

$[a_0; a_1, a_2, \dots] = \lim_{n\to\infty} C_n$

$= \lim_{n\to\infty} [a_0; a_1, \dots, a_n]$

Thm.

① Infinite simple continued fraction $[a_0; a_1, \dots]$ represents an irrational number

② Let $x = x_0$ is an irrational number. ⊃

Define a sequence $a_k = \lfloor x_k \rfloor$

$$x_{k+1} = \frac{1}{x_k - a_k}, \quad k \geq 0 \qquad x_1 = \frac{1}{x_0 - a_0}$$

Then $x = [a_0; a_1, a_2, \dots]$

If $[a_0; a_1, \dots]$ and $[b_0; b_1, \dots]$ represent the same irrational number, we have $a_i = b_i \ \forall i$.

① Find the irrat^l represented by $[1; 1, \dots, 1]$

$$x = [1; 1, 1, \dots]$$

$$= 1 + \frac{1}{[1; \dots, 1]}$$

$$x = 1 + \frac{1}{x}$$

$$x^2 = x + 1$$

$$x^2 - x - 1 = 0$$

$$x = \frac{1 \pm \sqrt{5}}{2}$$

Choose $x = \frac{1+\sqrt{5}}{2}$

② Find the irrat^l rep by $[3; 6, 1, 4, 1, 4, 1, 4]$

$y = [1; 4, 1, 4, \dots]$

$$[3; 6, 1, 4, 1, 4, \dots]$$

$$x = 3 + \frac{1}{6 + \frac{1}{y}}$$

$$= 3 + \frac{y}{6y+1} =$$

$$x(6y+1) = 18y + 3 + y$$

$$6xy + x = 19y + 3$$

$$y = [1; 4, 1, 4, \ldots]$$

$$= 1 + \frac{1}{4 + \frac{1}{y}}$$

$$= 1 + \frac{y}{4y+1}$$

$$y(4y+1) = 4y + 1 + y$$

$$4y^2 + y = 5y + 1$$

$$4y^2 - 4y - 1 = 0$$

$$y = \frac{4 \pm \sqrt{16+16}}{8}$$

$$= \frac{4 \pm 4\sqrt{2}}{8} = \frac{1 \pm \sqrt{2}}{2}$$

$$y = \frac{1+\sqrt{2}}{2}$$

$$x(6y+1) = 19y$$

$$x = \frac{19y}{6y+1}$$

$$= \frac{19\left(1+\sqrt{2}\right) + 3 \times 2}{2\left\{6\left(\frac{1+\sqrt{2}}{2}\right)+1\right\}}$$

$$= \frac{19}{2}\left\{\frac{1+\sqrt{2}}{3(1+\sqrt{2})+1}\right\}$$

$$= \frac{19\left(1+\sqrt{2}\right) + 6}{2\left\{4 + 3\sqrt{2}\right\}}$$

$$x = \frac{25 + 19\sqrt{2}}{}$$

$a + b\sqrt{2}$

Eg: $\sqrt{13}$

$x = x_0 = \sqrt{13}$

$a_0 = \lfloor x_0 \rfloor = \lfloor \sqrt{13} \rfloor = 3$

$x_1 = \dfrac{1}{\sqrt{13} - 3} = \dfrac{\sqrt{13} + 3}{4}$

$a_1 = \left\lfloor \dfrac{\sqrt{13} + 3}{4} \right\rfloor$