Number Theory

Fermat's little thm.,
If p is a prime, and p ∤ a, then $a^{p-1} \equiv 1 \pmod{p}$.

Result: (Wilson's Th.)

If p is prime, $(p-1)! \equiv -1 \pmod{p}$.

Consider $(\mathbb{Z}_p)^*$ $1 \le x \le p-1$

$(\bar{1}, \bar{2}, \bar{3}, \bar{4}, \ldots \overline{p-1})$

$\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$
$\bar{1}\ \bar{4}\ \bar{5}\quad \bar{2}\ \bar{3}\ \bar{6}$

$[x]^2 = [1]$

$x^2 \equiv 1 \pmod{p}$
$\Rightarrow p \mid (x-1)(x+1)$
$\Rightarrow p \mid (x-1)$ or $p \mid (x+1)$

Hence, $x \equiv 1 \pmod{p}$ or
$x \equiv (p-1) \pmod{p}$

$\bar{1} \times \bar{2} \times \bar{3} \cdots \times \overline{(p-1)}$
$= \bar{1} \times \overline{(p-1)}$

Now, $(p-1)! \equiv (p-1) \pmod{p}$
$\therefore (p-1)! \equiv -1 \pmod{p}$

Excercise

For $n>1$,

If $(n-1)! \equiv -1 \pmod n$,

then n is a prime.

Def: function from $\mathbb{N}$ to $\mathbb{R}$ or $\mathbb{C}$ is called an arithmatic function or number theoretic function.

Mobius function

defined by $M(1) = 1$.

For $n>1$,

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

$$M(n) = \begin{cases} (-1)^k & \text{if } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 1 \\ 0 & \text{else.} \end{cases}$$

Remark: If n has sq. factor then

$M(n) = 0$.

Result: For $n \geq 1$

$$\sum_{d|n} M(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

$(d \in \mathbb{N})$

For $n=1$, clear.

For $n>1$,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_K^{\alpha_K}$$

$$\sum_{d|n} \mu(d) = 1 + M(p_1) + \cdots + M(p_K) + M(p_1 p_2) + \cdots M(p_{K-1} p_K) + \cdots + (-1)^K$$

$$= 1 + {}^K C_1 (-1) + \binom{K}{2}(-1)^2 \cdots + \binom{K}{K}(-1)^K$$

$$= (1-1)^K = 0$$

Def: For f, g two arithmetic func., define

$$h(n) = \sum_{d|n} f(d)\, g(n/d)$$

denote: $h = f * g$, called dirichilet product.

Remark: (1) $*$ is comm.

(2) $*$ is associative.

$$f * I = f$$

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

we can observe

$$I(n) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

$$f^{-1}(1) = \frac{1}{f(1)} \qquad f * f^{-1} = I$$

($f(1)$ is non-zero)

For $n > 1$

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d>1}} f\left(\frac{n}{d}\right) f^{-1}(d)$$

with $f(1) \neq 0$.

Conc: The set of arithmetic funcs is an abl. group.

s.t. $G-F$ is disconnected.

Then, $G-\{e_1, e_2, \ldots, e_{r-1}\}$ has a bridge. e_r, let $e_r = uv$.

Let S be a set of $r+1$ vertices

Number Theory

Prime field:

A field is called prime if it has no proper subfield.

Remark: Every field contains a prime field, that is the intersection of all subfields.

Prime field of F is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p.

Consider $f: \mathbb{Z} \to F$

$f(n) = n.1$

If $\ker f = \{0\}$. $\ker f = \langle m \rangle$

$\mathbb{Z}/\langle m \rangle \cong \text{Im} f \Rightarrow m$ is prime

Result: The no. of elt. of a finite field is p^n for some prime p and $n \in \mathbb{N}$.

$\mathbb{Z}_p \hookrightarrow F$

$[F : \mathbb{Z}_p] = n$. let $v_1, v_2, \ldots, v_n$ be a

Every $a \in F$ is a linear combination

$a = c_1 v_1 + c_2 v_2 \cdots + c_n v_n$.

$|F| = p^n$.

Cor: A addition group $(F, +)$ is isomorphic to

$\underbrace{Z_p \oplus Z_p \oplus Z_p \cdots \oplus Z_p}_{n\text{-times}}$.

Result: The multiplication group of non-zero elements of $F = GF(p^n)$ is cyclic.

$GF(p^n)^*$ is abelian group.

There exist $\alpha \in F^*$ such that $O(\alpha) = lcm(O(\alpha))$

$a^{\gamma} = 1, \forall a \in F^*$

As $x^r - 1$ has atmost r-zeroes in F,

$|F^*| < \gamma$

$1, \alpha, \alpha^2, \ldots \alpha^{r-1}$ are distinct.

Hence, $|F^*| = \gamma$, $\langle a \rangle = F^*$

Note:

$O(a,b) = lcm(O(a), O(b))$

Corollary

$GF(p^n)^* \cong Z_{p^n - 1}$

Cor:
Any 2 fields of order p^n are isomorph

Result:

Any field F of order p^n is the splitting field of $x^{p^n} - x \in Z_p[x]$

Proof:
Note that $|F^*| = p^n - 1$.
$\forall\ a \in F^*$, $a^{p^n - 1} = 1$ and if $a = 0$,
$a^{p^n} - a = 0$
Every element of F is a zero of $x^{p^n} - x$
$x^{p^n} - x \in Z_p[x]$ has only p^n zeroes

Result:

If $m \mid n$, then $GF(p^n)$ has a unique subfield of p^m.

Euler's theorem:

If $n \geq 1$, and $\gcd(a, n) = 1$,

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

$a \in U(\mathbb{Z}_n) = \{a \mid (a, n) = 1\}$

$|U(\mathbb{Z}_n)| = \phi(n)$

Hence, $a^{\phi(n)} = 1$ in $\mathbb{Z}_n$.

$$a^{\phi(n)} \equiv 1 \mod n.$$

Fermat's little theorem:

If p is a prime and $p \nmid a$,

Then $a^{p-1} \equiv 1 \mod p$.

10

1, 3, 9, 7

(1, 3, 7, 9)

multi

Let $A = \{ f \mid f$ an arbitrary fn. such that $f(1) \neq 0 \}$.

Result: $(A, *)$ is an abelian group, where $*$ is the dirichilet product.

identity elt $I = \begin{bmatrix} 1 \\ n \end{bmatrix}$

For $f \in A$, $\begin{cases} f^{-1}(1) = \dfrac{1}{f(1)} \\ f^{-1}(n) = -\dfrac{1}{f(1)} \sum\limits_{\substack{d \mid n \\ d<n}} f\left(\dfrac{n}{d}\right) f^{-1}(d) \end{cases}$ for $n \geq 1$,

$f * f^{-1} = I$

for $n > 1$, $\sum\limits_{d \mid n} f(d)\, f^{-1}\left(\dfrac{n}{d}\right) = 0$

$$f(1)\, f^{-1}(n) + \sum_{\substack{d \mid n \\ d>1}} f(d)\, f^{-1}\left(\frac{n}{d}\right) = 0$$

μ^{-1} ? $f_0(n) = 1 \ \forall\ n \geq 1$ is the inverse of μ.

$\sum\limits_{d \mid n} \mu(d) = I$ $\quad M * f_0 = I$, $\quad f_0(n) = 1 \ \forall\ n \geq 1$

Result: (Mobius inversion formula)

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

$$\Leftrightarrow \quad g(n) = \sum_{d|n} f(d)\, \mu\left(\frac{n}{d}\right)$$

Proof:

$$f = g * f_0$$

$$\Leftrightarrow \quad f * \mu = g * f_0 * \mu = g * I = g$$

* **Result 1** For $n \geq 1$, $\sum_{d|n} \phi(d) = n$.

when ϕ is the Euler function denoted by $\phi(n)$ is the no. of the int. relatively prime to n and less than or equal to n.

* **Result 2:** For $n \geq 1$, $\phi(n) = \sum \mu(d)\left(\frac{n}{d}\right)$

(Result 1 $\Leftrightarrow$ Result 2 from Mobius inversion formula)

Defs An arithmatic fn. f which is not identically zero is called multiplicative

if $f(mn) = f(m) \cdot f(n)$, whenever $(m,n) = 1$.

Multiplicative

If $f(m)f(n) = f(mn)$ $\forall$ m, n, then we call f is completely multiplicative

$\mu(4) = 0$

$\mu(2)\mu(2) = 1$

$\phi(4) = 2$

$\phi(2)\phi(2) = 1$

} completely not multiplicative

Remark: If f is multiplicative, $f(1) = 1$

Result: If f and g are multiplicative, so is $f * g = h$.

$$(m,n) = 1$$

$$h(mn) = \sum_{d \mid mn} f(d)\, g\left(\frac{mn}{d}\right)$$

$$h(mn) = \sum_{d \mid mn} f(d)\, g\left(\frac{mn}{d}\right)$$

$d = ab$ $\quad$ $\gcd(m,n) = 1$

$a \mid m$ $\gcd(a,b) = 1$

$b \mid n$ $\quad \left(\frac{m}{a}, \frac{n}{b}\right) = 1$

$$= \sum_{a \mid m} f(a)\, g\left(\frac{m}{a}\right) \sum_{b \mid n} f(b)\, g\left(\frac{n}{b}\right)$$

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

Result: If $f * g$ and g are multiplicative then so is f.

Proof: Suppose f is not multiplicative.

Let $(m,n) = 1$, with mn is smallest possible such that $f(mn) \neq f(m) f(n)$.

If $mn = 1$, then $f(1) \neq 1$,

Hence, $h(1) \neq 1$ contradiction.

If $mn > 1$, then $f(ab) = f(a) f(b)$ $\forall$ a, b with $(a,b) = 1$.

$ab < mn$.

$$h(mn) = \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)\, g\left(\frac{mn}{ab}\right) + f(mn)\, g(1)$$

$$h(mn) = \sum_{a|m} f(a)\, g\left(\frac{m}{a}\right) \sum_{b|n} f(b)\, g\left(\frac{n}{b}\right) - f(m)\, f(n) + f(mn)$$

As, $f(mn) \neq f(m)\, f(n)$,

we have $h(mn) \neq h(m) h(n)$

a contradiction.

f is multiplicative.

Cor: If f is multiplicative, so is f^{-1},

$M_0 \leq A$

↳ The set of all multiplicative fns.

Exercise

Result: Let f be a multiplicative function,

f is completely multiplicative $\iff f^{-1} = \mu f$

Refer to Maths stack exchange where $\mu f(n) = \mu(n) f(n)$ $\forall n \geq 1$

For any α,

① Consider f_α defined by

$$f_\alpha(n) = n^\alpha \quad \forall \quad n \geq 1.$$

$f_0 = 1$

$f_1 = n$.

Note that f_α is completely multiplicative

② $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$, If $\alpha = 0$, $\sigma_\alpha = \sigma_0$ count the no. of divisors.

If $\alpha = 1$, $\sigma_\alpha = \sigma_1$ count the sum of divisors

Note that σ_α is multiplicative (not completely)

Remark:

① $\mu * f_0 = I \Rightarrow \mu$ is multiplicative

multiplicative

② ϕ is multiplicative

Proof:
If f is multiplicative,

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

is multiplicative.

For $n \geq 1$

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

$$\phi(n) = \sum_{K=1}^{n} \left[\frac{1}{n, (K)} \right]$$

$$= \sum_{U=1}^{n} \sum_{d|(n,K)} \mu(d) = \sum_{K=1}^{n} \sum_{\substack{d|n \\ d|K}} \mu(d)$$

$$= \sum_{d|n} \sum_{q=1}^{n/d} \mu(d)$$

$$= \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1$$

$K = qd.$

$$= \sum_{d|n} \mu(d) \frac{n}{d}.$$

$1 \leq K \leq n$

$1 \leq q \leq n/d.$

Result:

For $n \geq 1$,

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{P}\right)$$

↳ prime divisor.

Proof: Let $p_1, p_2, p_3 \cdots p_k$ be distinct prime factors of n.

$$\prod_{p \mid n} \left(1 - 1/p\right) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= 1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i,j} \frac{1}{p_i p_j} - \sum_{i,j,l} \frac{1}{p_i p_j p_l} + \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}$$

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

(Proved).

Quick Results

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

② $\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)}$ $\quad d = (m,n)$

Proof: Let $p_1, p_2, p_3 \cdots p_k$ be distinct prime factors of n.

$$\prod_{p|n}\left(1-\frac{1}{p}\right) = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$$= 1 - \sum_{i=1}^{k}\frac{1}{p_i} + \sum_{i,j}\frac{1}{p_i p_j} - \sum_{i,j,l}\frac{1}{p_i p_j p_l} + \cdots + \sum_{i}\frac{(-1)^k}{p_1 p_2 \cdots p_k}$$

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

(Proved).

Quick Results

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

(2) $\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)}$ $\quad d = (m,n)$

(3) $a \mid b \Rightarrow \phi(a) \mid \phi(b)$

(4) $\phi(n)$ is even $\forall n \geq 3$.

$\mathbb{Z}_n$.

$(a, n) = 1 \qquad |U(\mathbb{Z}_n)| = \phi(n)$.

Euler

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

$U_n \overset{?}{=} \langle a \rangle$

For what n, U_n is cyclic.

generated by $\langle a \rangle$.

If U_n is cyclic, then the no. of generators is $\phi(\phi(n))$.

Then, the set of generators.

$$= \{a^K \in U \mid (K, \phi(n)) = 1\}.$$

$$\{a^1, a^2, a^3, \ldots a^{\phi(n)}\}$$

Basically we have to find an element whose order is $\phi(n)$.

★ Let $(a, n) = 1$

smallest k such that $a^k \equiv 1 \pmod{n}$ is called the exponent of a mod n.

order(a)

$exp_n(a) = k$,

If $exp_n(a) = \phi(n)$, then a is called primitive roots mod n.

* 9 has primitive roots 285.
* 8 has no primitive roots.

→ Result:

Let α be an odd number,

If $\alpha \geq 3$,

$$x^{\phi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$$

Cor: 2^α $(\alpha \geq 3)$ has no primitive roots.

Proof: By induc.

$\alpha = 3$ ✓

$$x^{\phi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha}$$

$$x^{\phi(2^\alpha)/2} = 1 + t \cdot 2^\alpha$$

$$x^{\phi(2^\alpha)} = 1 + t^2 2^{2\alpha} + 2^{\alpha+1} \cdot t \equiv 1 \bmod 2^{\alpha+1}$$

$$x^{\phi(2^\alpha)} \equiv 1 \bmod 2^{\alpha+1}$$

$$x^{\phi(2^{\alpha+1})/2} \equiv 1 \pmod{2^{\alpha+1}}$$

Result: For $n > 1$,
n has primitive roots iff.

$x = 2, 4, p^\alpha$ or $2p^\alpha$ for odd prime p.

Result: If $(m,n) = 1$, $m > 2$ & $n > 2$ then (mn) has no primitive root.

Proof: Let $(a, mn) = 1$, Then $(a,n) = 1$ and $(a,m) = 1$.
We know that $a^{\phi(m)} \equiv 1 \pmod m$ (Euler)
Let $d = \gcd(\phi(m), \phi(n))$
$\Rightarrow (a^{\phi(m)})^{\phi(n)/d} \equiv 1 \pmod m$

$k = \text{lcm}(\phi(m), \phi(n)) \Rightarrow a^k \equiv 1 \pmod{m}$

Similarly, $a^k \equiv 1 \pmod{n}$

As $(m,n) = 1$, $a^k \equiv 1 \pmod{mn}$

$$k = \frac{\phi(m)\,\phi(n)}{d} = \frac{\phi(mn)}{d} \leq \frac{\phi(mn)}{2}$$

Result1: For odd prime p,

p^α has primitive roots.

Result2: For odd prime, $2p^\alpha$ has primitive ro

Let a be a primitive root of p

Excercise

If a is even,

$a + p^\alpha$ is a primitive root of p

Suppose a is odd.

Then $(a, 2p^\alpha) = 1$.

Let k be ~~the~~ $\exp_{2p^\alpha}(a)$.

Then, $a^k \equiv 1 \pmod{2p^\alpha}$

$\Rightarrow a^k \equiv 1 \pmod{p^\alpha}$

$\Rightarrow \phi(p^\alpha) \mid k.$

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

But $k \mid \phi(2p^\alpha)$

$\Rightarrow k = \phi(2p^\alpha)$

Let a be a primitive root of n.
For $(b,n)=1$, there exists a unique K such that $b = a^K \pmod n$.
We call K is the index of b to the base a, written.

$$ind_a(b) = K.$$

Example

$n = 9$

$a = 5$

$\text{mod}_5\ 7 = 2.$

(1) $ind_a(xy) = ind_a(x) + ind_a(y) \pmod{\phi(n)}$

(2) $ind_a(x^K) = K\, ind_a(x) \pmod{\phi(n)}$

(3) $ind_a(1) \equiv 0 \pmod{\phi(n)}$

(4) $ind_a(a) \equiv 1 \pmod{\phi(n)}$

* p odd prime, p^α has a primitive root
$\alpha = 1$, Z_p^* is cyclic
Let a be a primitive root mod p.
$\Rightarrow a^{p-1} \equiv 1 \pmod p$
If $a^{p-1} \equiv 1 \pmod{p^2}$
then clearly a is not a p.r. mod p^2
So, if a pr. of p is a p.r. of p^2 then $a^{p-1} \not\equiv 1 \pmod{p^2}$. Hence, * is necessary to have a p.r. of p^2.

Result: Let a be a p.r. of p, a is a p.r. of $p^\alpha \ \forall\ \alpha > 1$ iff $a^{p-1} \not\equiv 1 \pmod{p^2}$.

⇒ For $\alpha = 2$,

as $p-1 < \phi(p^2)$

$$a^{p-1} \not\equiv 1 \pmod{p^2}$$

Suppose $a^{p-1} \not\equiv 1 \pmod{p^2}$ (★)

There is at least one p.r. of p satisfying ★.

The p.r. a satisfies then we are done.

If not, $a + p$ should satisfy ★

Let $a_1 = a + p$.

$$a_1^{p-1} = (a+p)^{p-1} = a^{p-1} + (p-1)a^{p-2}p + \cdots + p^2$$

$$= a^{p-1} - pa^{p-2} \pmod{p^2}$$

So $a_1^{p-1} \not\equiv 1 \pmod{p^2}$

$a^{p-2} \not\equiv 0 \pmod{p}$ ↗

But this is ~~not possible~~.

Hence, $\beta = \alpha - 1$

So that $t = \phi(p^\alpha)$

By ind. on α, you can conclude that $\forall \alpha \geq 2$,

$$a^{\phi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}$$

$f(d)\ f^{-1}\left(\frac{n}{d}\right)$

$= I(n)$

Let a be a pr. mod p s.t. $a^{p-1} \not\equiv 1 \pmod{p^2}$

Let $t = o(a) \pmod{p^\alpha}$

$\exp(a)$.

claim $t = \phi(p^\alpha)$

As $a^t \equiv 1 \pmod{p^\alpha} \Rightarrow a^t \equiv 1 \pmod{p}$

$\Rightarrow \phi(p) \mid t$

$\Rightarrow t = q\,\phi(p)$

As $t \mid \phi(p^\alpha)$, $q\phi(p) \mid \phi(p^\alpha)$

$\Rightarrow q(p-1) \mid p^{\alpha-1}(p-1)$

$\Rightarrow q \mid p^{\alpha-1}$

$\Rightarrow q = p^\beta$ $\quad \beta \leq \alpha - 1$.

So, $t = p^\beta(p-1)$

Claim: $\beta = \alpha - 1$

Suppose $\beta < \alpha - 1 \Rightarrow \beta \leq \alpha - 2$

$t = p^\beta(p-1) \mid p^{\alpha-2}(p-1) = \phi(p^{\alpha-1})$

So, $\phi(p^{\alpha-1})$ is a multiple of t. $a^{\phi(p^{\alpha-1})} \equiv 1 \pmod{p^\alpha}$ ✓