Introductory Number Theory

Yashas.N

yn37git.github.io/blog/2025/Short-Notes

Contents

0 Symbols used

$s|t$ $\to$ such that.
iff $\to$ if and only if.
$a|b$ $\to$ a divides b .
$\exists!$ $\to$ there exists unique.

1 Preliminaries

Principle of Mathematical induction

■ First principle : If S is a subset of positive integers ($\mathbb{Z}^+$) with the following :
- $1 \in S$.
- $k \in S \implies k+1 \in S$.

then S is the whole set of positive integers i.e. $S = \mathbb{Z}^+$.

■ Second principle (strong induction): if $S \subseteq \mathbb{Z}^+$ $s|t$
- $1 \in S$ and
- $1, 2, .., k \in S \implies k+1 \in S$

then $S = \mathbb{Z}^+$.

2 Divisibility in $\mathbb{Z}^+$

■ for every $a, b \in \mathbb{Z}, \exists($ unique $)q \in \mathbb{Z}, r \in \mathbb{Z}^+$ $s|t$ $a = qb + r$ and $0 \leqslant r \leqslant |b|$.
■ $a|b$ (a divides b) iff $a = qb$ for some (unique) $q \in \mathbb{Z}$
■ $a|b$ then $|a| \leqslant |b|$.

let $d = \gcd(a, b)$ denote greatest common divisor of a and b then
■ $\exists! x, y \in \mathbb{Z}$ $s|t$ $d = xa + yb$
■ $d =$ least element of $S = \{xa + yb | xa + yb > 0, x, y \in \mathbb{Z}\}$.
■ set $\{xa + yb | x, y \in \mathbb{Z}\}$ contains precisely multiples of d.
■ if $a|c$ and $b|c$ then $ab|c$ if $\gcd(a, b) = 1$.
■ Euclid's lemma : $a|bc$ and $\gcd(a, b) = 1$ then $a|c$.

■ a and b are relatively primes if $\gcd(a,b) = 1$ iff $1 = xa + yb$ for some $x, y \in \mathbb{Z}$.
■ if $a = qb + r$ then $\gcd(a,b) = \gcd(b,r)$. thus $\gcd(a,b)$ is the last remainder in the euclidean algorithm
■ $\gcd(ka,kb) = |k| \gcd(a,b)$ (here $k \neq 0$) thus prime factorisation of a ad b comes into play here.
■ if $d = \gcd(a,b)$ then there are relatively prime integers r, s such that $a = rd$ and $b = sd$.
■ $\gcd(a,bc) = 1$ iff $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$.
■ $\gcd(a,n) = \gcd(kn \pm a, n)$ for all $k \in \mathbb{Z}^+$.
■ if $\gcd(a,b) = d$ then there exist $a_1, b_1\ _s|_t\ a = a_1 d, b = b_1 d$ and $\gcd(a_1,b_1) = 1$.

let $l = \text{lcm}(a,b)$ denote the lowest common multiple of a and b. then
■ $\gcd(a,b)\,\text{lcm}(a,b) = ab$.
■ $\text{lcm}(a,b) = ab$ iff $\gcd(a,b) = 1$.

Diophantine equations

Equations in one or more variable that is to be solved in integers is called a Diophantine equation.
■ The linear diophantine equation $ax + by = c$ for given $a, b, c \in \mathbb{Z}$ has a solution iff $\gcd(a,b)|c$. (if so then as $d|c \implies c = dt = t(x_0 a + y_0 b) \implies x = x_0 t, y = y_0 t$.)
■ all solutions of the above linear diophantine equation is of form

$$x = x_0 + \left(\frac{b}{d}\right) t \quad y = y_0 + \left(\frac{a}{d}\right) t.$$

for some solution x_0, y_0 and arbitrary $t \in \mathbb{Z}$ i.e. there are infinitely many solutions for the linear diophatine equation $ax + by = c$.

3 Congruences

$a \equiv b \pmod{n}$

is defined as true if $n|(a-b)$ (note $a, b \in Z$ and $1 < n \in \mathbb{Z}^+$) otherwise $a \not\equiv b \pmod{n}$.

properties

■ $\equiv$ mod n is a equivalence relation on $\mathbb{Z}$ for any $n > 1$.
if $a \equiv b \pmod{n}$ and $c \equiv b \pmod{n}$ then
■ $a + c \equiv b + d \pmod{n}$.
■ $ac \equiv bd \pmod{n}$.
■ $a^k \equiv b^k \pmod{n}$ for $k \in \mathbb{Z}^+$.
■ it is not true that $ca \equiv cb \pmod{n} \implies a \equiv b \pmod{n}$.
■ $ca \equiv cb \pmod{n} \implies a \equiv b \pmod{n/d}$ where $d = \gcd(c,n)$.
■ if $a \equiv b \pmod{n}$ and $m|n$ then $a \equiv b \pmod{m}$.
■ if $\gcd(n,m) = 1$, $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$ then $a \equiv b \pmod{mn}$
■ if $a \equiv b \pmod{n}$ and $d|n, a, b$ then $a/d \equiv b/d \pmod{n}/d$.
■$\star$ if $a \equiv b \pmod{n}$ then $\gcd(a,n) = \gcd(b,n)$.
■ if $ac \equiv bd \pmod{n}$. and $b \equiv d \pmod{n}$ with $\gcd(b,n) = 1$ then $a \equiv c \pmod{n}$.

3.1 Linear congruences

equation $ax \equiv b \pmod{n}$ has a solution iff $d|b$ for $d = \gcd(a,n)$. if so the this equation has d mutually incongruent solutions mod n. (use : this is same as solutions for diophantine equation $ax - ny = b$).

from above point $ax \equiv b \pmod{n}$. has a unique solution mod n iff $\gcd(a,n) = 1$.

system of linear congruence equations

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1},\\ a_2x &\equiv b_2 \pmod{m_2},\\ &\vdots\\ a_kx &\equiv b_k \pmod{m_k}. \end{aligned}$$

where m_i's are relatively prime pairs is equivalent to solving system

$$\begin{aligned} x &\equiv c_1 \pmod{n_1},\\ x &\equiv c_2 \pmod{n_2},\\ &\vdots\\ x &\equiv c_k \pmod{n_k}. \end{aligned}$$

where $n_i = m_i/d_i$, $d_i = \gcd(a_i, m_i)$ and $c_i = (b_i/d_i)(a_i')$ for $a_i'(a_i/d_i) \equiv 1 \pmod{n_i}$ (use system is solvable iff each equation is solvable i.e. $d_i|b_i$, $\gcd(a_i/d_i, n_i) = 1$ so $\exists! a_i' \ {}_s|_t\ a_i'a_i/d_i \equiv 1 \pmod{n_i}$.)

Chinese Remainder Theorem

for $n_i \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$ the system of linear congruence equations

$$\begin{aligned} x &\equiv a_1 \pmod{n_1},\\ x &\equiv a_2 \pmod{n_2},\\ &\vdots\\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

has a simultaneous solution. This solution is unique upto mod $n = n_1n_2..n_k$.
And this solution is given by $x = a_1N_1x_1 + a_2N_2x_2..a_kN_kx_k$ where $N_i = n/n_i = n_1..n_{i-1}n_{i+1}..n_k$, for $N_ix_i \equiv 1 \pmod{n_i}$.

The system of linear congruences

$$\begin{aligned} ax + by &\equiv r \pmod{n}\\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

has a unique solution mod n whenever $\gcd(ad - bc, n) = 1$.

Fermat's Little Theorem

for a prime p and $p \not| a$ we have $a^{p-1} \equiv 1 \pmod{p}$. (use as $\{a, 2a, .., (p-1)a\}$ forms complete congruence residue of p so $a.2a..(p-1)a \equiv 1.2..(p-1) \pmod{p} \implies (p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$.)

Wilson's Theorem

p is a prime iff $p|(p-1)! + 1$ i.e. $(p-1)! \equiv -1 \pmod{p}$ (use for $1 < a < p-1, a \ /|p$ so $\exists! a' \in \{2, 3, ..p-2\}\ {}_s|_t\ aa' \equiv 1 \pmod{p}$ so $2.3..p-2 = (p-2)! \equiv 1 \pmod{p}$.)

4 Primes: Properties, Theorems and Conjectures.

let $p, q \in \mathbb{Z}^+$ be primes ($p > 1$ is prime in $\mathbb{Z}^+$ if only divisors of p are 1 and p.) and $\forall ab \in \mathbb{Z}$.then

- $p|ab \implies p|a$ or $p|b$
- $p|a^k \implies p|a$ or $p|a^k$.

Fundamental Theorem of Arithmetic

Every positive integer $n > 1$ is a prime or product of primes such that its representation of the form

$$n = p_1^{l_1}p_2^{l_2}..p_k^{l_k}.$$

for primes $p_1 < p_2 < .. < p_k$ and $l_i \in \mathbb{Z}^+$ is unique.

- there exists prime p appearing in prime factorization of a i.e. $a = pm\ {}_s|_t\ p \leqslant \sqrt{a}$.
- if $a > 1$ is not divisible by any prime $p \leqslant \sqrt{a}$ then a is a prime (simple restatement of above point.)
- There are an Infinite number of primes in $\mathbb{Z}^+$
- let p_n denote the n^{th} prime in ascending order of primes then $p_n < 2^n$.
- for $n > 2$ there exists a prime such that $n < p < n!$ (use: if not then $n! - 1$ is not prime and all its prime divisors are $p \leqslant n \implies p|n!$ thus $p \leqslant n$

leading to contradiction $p|1$.)

■ **Goldbach conjecture** : every even integer is sum of two numbers that are either prime or 1.
■ *twin prime* question : are there infinitely many twin prime pairs (primes with a gap of 2 integers between them).
■ for $n \in \mathbb{Z}^+$ there are n consecutive integers all of them composite ($(n+1)!+2, (n+1)!+3, .., (n+1)!+(n+1)$).

Dirichlet theorem

If a and b are relatively prime positive integers, then the arithmetic progression $a, a+b, a+2b, a+3b, ..$ contains infinitely many primes.

Fermat Kraitchik Factorisation method

■ for odd integer n if $n = x^2 - y^2$ then clearly $n = (x+y)(x-y)$ or if n is composite i.e. $n = ab$ then $n = (\frac{a+b}{2})^2 - (\frac{a-b}{2})^2$ holds as both a, b are odd.
■ So rearranging we get $x^2 - n = y^2$ now search for smallest integers $k\ {}_s|_t\ k^2 \geqslant n$ and look at numbers $k^2 - n, (k+1)^2 - n, (k+2)^2 - n, ..$ until a value $m \geqslant \sqrt{n}$ is found making $m^2 - n$ a square to give a factorisation of $n = ml$.
■ this process cannot go indefinitely as $(\frac{n+1}{2})^2 - n = (\frac{n-1}{2})^2$ gives trivial factorisation $n = n.1$.
■ thus this process terminates for some m and n is composite if not then clearly n is a prime.

4.1 Divisibility by Small primes

let $a = a_m 10^m + a_{m-1} 10m - 1 + .. + a_1 10 + a_0$ be the decimal representation of a then

$2|a$ iff unit digits of $a = a_0 = 2, 4, 8$ or 0.

$3, 9|a$ iff $3, 9|a_m + a_{m-1} .. + a_1 + a_0$ i.e. iff sum of the digits in decimal representation of a is divisible by 3 or 9 (use $10 \equiv 1 \pmod 9 \equiv 1 \pmod 3$).)

$4|a$ iff $4|10a_1 + a_0$ i.e. iff 4 divides the number formed by tens and units digits of a. (use $10^k \equiv 0 \pmod 4$ if $k \geqslant 2$).

$5|a$ iff $a_0 = 0$ or 5.

$11|a$ iff $11|a_0 - a_1 + a_2 .. + (-1)^m a_m$ (use $10 \equiv -1 \pmod{11}$).

$7, 11, 13|a$ iff $7, 11, 13|[(100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6)..]$ i.e. 7, 11, 13 divides a iff alternating sum of 3 digits taken at a time in digits of a is divisible by 7, 11, 13 (use $7.11.13 = 1001$ and if n is even $10^{3n} = 1, 10^{3n+1} = 10, 10^{3n+2} = 100 \pmod{1001}$. of if n is odd $10^{3n} = -1, 10^{3n+1} = -10, 10^{3n+2} = -100 \pmod{1001}$).

5 Number theoretic functions

Any function whose domain is the set of positive integers ($\mathbb{Z}^+$) is called a number theoretic function or arithmetic function.

let $\sum_{d|n} f(d)$ sum over all divisors of n i.e. for eg: $\sum_{d|6} f(d) = f(1) + f(2) + f(3) + f(6)$.

Multiplicative Function

a number theoretic function $f(k)$ is called a multiplicative function if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

if $f(d)$ is multiplicative then $F(n) = \sum_{d|n} f(d)$ is also a multiplicative function.

Mobius inversion Formula

■ Define Mobius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } p^2|n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1p_2..p_r \text{ where } p_i's \\ & \quad \text{are distint primes.} \end{cases}$$

■ let $\mathbb{F}(n) = \sum_{d|n} \mu(d)$ then

$$\mathbb{F}(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

■ clearly $\mu(n)$ and $\mathbb{F}(n)$ are multiplicative.
■ **The Formula** : if f, F are two number theoretic functions such that

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

then

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

Clearly from above we get if $F(n) = \sum_{d|n} f(d)$ is multiplicative then $f(n)$ is also multiplicative.

Positive Divisors function

for a given integer n let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of these divisors then

■ $\tau(n) = \sum_{d|n} 1.$

■ $\sigma(n) = \sum_{d|n} d.$

Now if $n = p_1^{k_1}p_2^{k_2}..p_r^{k_r}$ is prime factorisation of n then

■

$$\tau(n) = (k_1+1)(k_2+1)..(k_r+1) = \prod_{1\leqslant i\leqslant r}(k_1+1).$$

(use for each p_i there are k_i+1 choices for divisors of n given by $d = p_1^{a_1}p_2^{a_2}..p_r^{a_r}$ for $0 \leqslant a_i \leqslant k_i$ respectively).

■

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1}\frac{p_2^{k_2+1}-1}{p_2-1}..\frac{p_r^{k_r+1}-1}{p_r-1} = \prod_{1\leqslant i\leqslant r}\frac{p_i^{k_i+1}-1}{p_i-1}.$$

(use the factors in the product $(1+p_1+p_1^2+..+p_1^{k_1})(1+p_2+p_2^2+..+p_2^{k_2})..(1+p_r+p_r^2+..+p_r^{k_r})$ are the only values d can take if $d|n$).

■ $\tau(n)$ and $\sigma(n)$ are multiplicative functions.

■ $n^{\tau(n)/2} = \prod_{d|n} d.$

■ $\tau(n)$ is odd iff n is a perfect square.

■ $\sigma(n)$ is odd iff n is a perfect square of twice a perfect square (use : for odd prime p, $1+p+p^2+..+p^k$ is odd iff k is even).

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

■ $\sum_{d|n}\sigma(d) = \sum_{n|d}\frac{n}{d}\tau(d).$

Greatest integer function

Let $[x]$ for real number x denote the largest integer less than or equal to x i.e. $[x]$ is a unique integer satisfying $x-1<[x]\leqslant x$

■ every $x=[x]+\theta$ for $0\leqslant\theta<1$.

■ if p appears in the prime factorisation of n then the highest exponent of p dividing $n!$ is given by

$$\sum_{k=1}^{\infty}\left[\frac{n}{d}\right].$$

clearly this series converges as $[n/p^k]=0$ for $p^k>n$.

■ if f,F are two number theoretic functions such that

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

then for $N\in\mathbb{Z}^+$

$$\sum_{n=1}^{N}F(n)=\sum_{k=1}^{N}f(k)\left[\frac{N}{k}\right].$$

Euler's ϕ function

Define $\phi(n)$ as the number of positive integers$\leqslant n$ that are relatively prime to n.

■ $\phi(p)=p-1$ for a prime p.

■ $\phi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)=p^k(1-\frac{1}{p})$ (use: there are $p,2p,..,p^2,..p^{k-1}p$ integers that are not co-prime $\leqslant p^k$).

■ ϕ is a multiplicative function.

if $n=p_1^{k_1}p_2^{k_2}..p_r^{k_r}$ is its prime factorisation then

■

$$\begin{aligned}\phi(n)&=p_1^{k_1-1}(p_1-1)..p_2^{k_2-1}(p_2-1)\\&\quad..p_r^{k_r-1}(p_r-1)\\&=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})..(1-\frac{1}{p_r}).\end{aligned}$$

■ $\phi(2^k)=2^{k-1}$.

■ $\phi(n)$ is even $\forall n>2$.

■ $\frac{\sqrt{n}}{2}\leqslant\phi(n)\leqslant n$ (use $p-1>\sqrt{p}$ and $k-1/2\geqslant k/2$).

■ if n has r distinct primes in its prime factorisation then $2^r|\phi(n)$.

■ if $d|n$ then $\phi(d)|\phi(n)$.

6 More on Congruences

for $n>1$ and $\gcd(a,n)=1$. If $a_1,a_2,..,a_{\phi(n)}$ are positive integers less than n and relatively prime to n then $aa_1,aa_2,..,aa_{\phi(n)}$ is also congruent to $a_1,a_2,..,a_{\phi(n)}$ modulo n in some order.

Euler's Theorem

for $n\in\mathbb{Z}^+$ and $\gcd(a,n)=1$ we have

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

(use above point or induction on power of p by fermat's and binomial theorem.)

■ if $\gcd(m,n)=1$ then $m^{\phi(n)}+n^{\phi(m)}\equiv 1\pmod{mn}$

■

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

(use if $n=p^k$ then $\sum_{d|n=p^k}\phi(n)=1+(p-1)+(p^2-p)+..+(p^k-p^{k-1})=p^k$ and multiplicity of ϕ for multiplicity of $\sum_{d|n}\phi(d)$). ■ sum of positive integers less than n and relatively prime to n is equal to $\frac{n\phi(n)}{2}$ (use $\gcd(a,n)=\gcd(n-a,n)$ so $\{n-a_1,n-a_2,..n-a_{\phi(n)}\}=\{a_1,a_2,..,a_{\phi(n)}\}$ integers relatively prime to n so the set sum is also equal).

7 Primitive roots

for $n > 1$ and $\gcd(a, n) = 1$, define **Order** of a modulo n as the smallest +ve integer $k\ {}_s|_t\ a^k \equiv 1 \pmod{n}$.

if a has order k modulo n
■ then $a^h \equiv 1 \pmod{n}$ iff $k|h$, in particular $k|\phi(n)$.
■ $a^i \equiv a^j \pmod{n}$ iff $i \equiv j \pmod{k}$.
■ integers $a, a^2, .., a^k$ are incongruent modulo n.
■ a^h has order $\frac{k}{\gcd(k,h)}$

primitive root

for $\gcd(a, n) = 1$ if a has order $\phi(n)$ (maximum order) then a is called primitive root of n.

if a is primitive root of n then
■ $\{a, a^2, .. a^{\phi(n)}\} = \{a_1, a_2, .., a_{\phi(n)}\}$ which is the set of relative primes less than n.
■ if n has primitive roots then there are $\phi(\phi(n))$ of them (use order argument).

7.1 existence of primitive roots

Lagrange Theorem

for a prime p and integral coefficient polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} .. a_1 x + a_0$ with $a_n \not\equiv 0 \pmod{n}$ has at most n incongruent solutions modulo p for equation $f(x) \equiv 0 \pmod{p}$ (use induction).

for a prime p if $d|p-1$ then ■ $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions incongruent modulo p.
■ there are exactly $\phi(d)$ incongruent integers having order d modulo p.
■ in particular there are $\phi(p-1)$ primitive roots modulo p.

for $k \geqslant 3$ the integer 2^k has no primitive roots (use induction to prove $a^{2^{k-2}} \equiv 1 \pmod{2^k} \forall a$).

for $m, n > 2$ if $\gcd(m, n) = 1$ then integer mn doesn't have a primitive root (use both $\phi(n), \phi(m)$ are even so $h = \operatorname{lcm}(\phi(n), \phi(m)) = \phi(n)\phi(m)/\gcd(m, n) \leqslant \phi(n)\phi(m)/2$ so by euler's theorem $a^h \equiv 1 \pmod{n}$ and $\equiv 1 \pmod{m}$ so $a^h \equiv 1 \pmod{mn} \forall a$).

from above we get n doesn't have a primitive root if
■ 2 odd primes divide n
■ $n = 2^k p$ for $k \geqslant 2$ and $2 \nmid p$

if p is an odd prime and r a primitive root of p then
■ $r^p - 1 \not\equiv 1 \pmod{p^2}$ or $r' = r + p$, $r'^{p-1} \not\equiv 1 \pmod{p^2}$
■ from above point we get r or r' is a primitive root of p^2
let r be a primitve root of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$ then
■ for each $k \geqslant 2$

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

(use induction). ■ r is a primitive root of p^k (use all above points).

Integer of form $2p^k$ for odd prime p has a primitive root (use $\phi(2p^k) = \phi(p^k)$ so any odd primitive root r of p^k is a primitive root of $2p^k$ (this exists as : if primitive root of p^k r' is even then $r = r' + p^k$ is odd)).

Summary

An integer $n > 1$ has a primitive root iff

$$n = 2, 4, p^k \text{ or } 2p^k$$

for odd prime p and $k \in \mathbb{Z}^+$.

7.2 Indices

Relative Index

If for a given $n \in \mathbb{Z}^+$ has a primitive root r then for a s|t $\gcd(a,n) = 1$
the smallest integer k s|t $a \equiv r^k \pmod{n}$ is called the index of a relative to r denoted by $k = \operatorname{ind}_r a$ (i.e. $r^{\operatorname{ind}_r a} \equiv a \pmod{n}$).

let n have a primitive root r and $\gcd(a,n) = \gcd(b,n) = 1$ then

- $0 \leqslant \operatorname{ind}_r a \leqslant \phi(a)$.
- $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\phi(n)}$.
- $\operatorname{ind}_r a^k \equiv k \operatorname{ind}_r a \pmod{\phi(n)}$.
- $\operatorname{ind}_r 1 \equiv 0 \pmod{\phi(n)}$

Binomial Congruence

for $n \in \mathbb{Z}^+$ having a primitive root (any) r and $\gcd(a,n) = 1$, the binomial congruence

$$x^k \equiv a \pmod{n} \quad k \geqslant 2$$

is equivalent to the linear congruence

$$k \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(a)}$$

thus the binomial congruence has a solution x_0 iff for $d = \gcd(a, \phi(n))$, $d | \operatorname{ind}_r a$. If so then there are exactly d incongruent solutions.

eg: if $n = p$ an odd prime and $k = 2$ then $\phi(p) = p - 1$ and as $d = \gcd(2, p-1) = 2$ we have

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

has a solution iff $2 | \operatorname{ind}_r a$, if s exactly 2 solutions. Now as r^k runs through $p - 1$ values ($k = \operatorname{ind}_r a$), we get this binomial congruence has solution for precisely $p - 1/2$ values of a.

Improving above arguments we have the binomial congruence

$$x^k \equiv a \pmod{n} \quad k \geqslant 2$$

has a solution iff

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

for $d = \gcd(k, \phi(n))$ (use this is equivalent to $\frac{\phi(n)}{d} \operatorname{ind}_r a \equiv 0 \pmod{\phi(a)}$ which has a solution iff $d | \operatorname{ind}_r a$).

thus

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

has solution iff

$$a^{p-1/d} \equiv 1 \pmod{p}.$$

for $d = \gcd(k, p-1)$.

Exponential Congruence

for an odd prime p with primitive root r, the exponential congruence

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

has a solution iff for $d = \gcd(\operatorname{ind}_r a, p-1)$, $d | i \operatorname{ind}_r b$. If then there are d incongruent solutions modulo $p - 1$.

7.3 Quadratic Congruence and residue

main problem

■ for a given off prime p the quadratic congruence

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

where $a \not\equiv 0 \pmod{p}$ hold iff

$$(2ax+b)^2 \equiv b^2-4ac \pmod{p}.$$

(use $\gcd(a,p)=1$ so $\gcd(4a,p)=1$ so the congruence is equivalent to $4a(ax^2+bx+c) \equiv (2ax+b)^2-(b^2-4ac) \equiv 0 \pmod{p}$)

■ so solving this quadratic congruence is equivalent to solving $y^2 \equiv d \pmod{p}$ and $y \equiv 2ax+b \pmod{p}$ where $d=b^2-4ac$.

■ So this problem boils down to solving quadratic congruence of form $x^2 \equiv a \pmod{p}$.

■ if x_0 is solution of the above congruence then $p-x_0$ is also another $\not\equiv \pmod{p}$ solution given $a \neq 0 \pmod{p}$.

■ thus by lagrange theorem these exhaust incongruent solutions modulo p.

Quadratic residue

for an odd prime p and $\gcd(a,p)=1$ is the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution the a is said to be quadratic residue of p otherwise a is quadratic nonresidue of p.

Euler's criterion

a is quadratic residue of p (an odd prime) iff

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

(use if r is primitive root of p then $a \equiv r^k \pmod{p}$ and $a^{(p-1)/2} \equiv r^{k(p-1)/2} \equiv 1 \pmod{p}$ so $p-1 | k(p-1)/2$ or $k=2j$).

now $(a^{(p-1)/2}-1)(a^{(p-1)/2}+1) \equiv a^{p-1}-1 \equiv 0 \pmod{p}$ so either $a^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$

Thus if $a^{(p-1)/2} \equiv -1 \pmod{p}$ then a is quadratic nonresidue of p.

Legendre symbol

for an odd prime p and $\gcd(a,p)=1$ define

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

if a and b are relatively prime to odd prime p then

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

■ $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

■ $\left(\frac{a^2}{p}\right) = 1$

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

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

for off prime p

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0.$$

Hence there are precisely $(p-1)/2$ quadratic residue and $(p-1)/2$ quadratic nonresidue of p (use if r is primitive root of p then $x^2 \equiv r \pmod{p}$ has no solution so $r^{(p-1)/2} \equiv -1 \pmod{p}$ so $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = \sum_{k=1}^{p-1}$)

Thus from above point we have for an odd prime p having primitive root r : quadratic residue of p are congruent to even powers of r modulo p and quadratic nonresidues congruent of p to odd powers of r modulo p.

Gauss's Lemma

for an odd prime p and $\gcd(a,p)=1$ if there are n integers in the set $\{a, 2a, 3a, .., \frac{p-1}{2}a\}$ whose remainder upon division by p exceeds $p/2$ then

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

.

$$(\frac{2}{p}) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \end{cases}.$$

(use gauss's lemma)

From above point and similarities of $(p^2-1)/8$ we get if p is an odd prime then

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}.$$

if p is an odd prime and a an odd integer with $\gcd(a,p) =$ then

$$(\frac{a}{p}) = (-1)^{\sum_{k=1}^{(p-1)/2}[ka/p]}$$

where $[\cdot]$ denotes the greatest integer function.

Quadratic Reciprocity Law

if p and q are distinct odd primes then

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Consequences : if p and q are distinct odd primes then

■

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

■

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

Calculation of $(\frac{a}{p})$

if $a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ is its prime factorisation then

$$(\frac{a}{p}) = (\frac{\pm 1}{p})(\frac{2}{p})^{k_0}(\frac{p_1}{p})^{k_1}(\frac{p_2}{p})^{k_2}\ldots(\frac{p_r}{p})^{k_r}.$$

Thus we can invert above for odd primes p_i to get a smaller denominator by above point and continue this process until we end up with blocks only of form $(\frac{\pm 1}{q_i})$ and $(\frac{2}{q_i})$ for odd primes $q_i \leqslant p$ which can be easily calculated by $(\frac{-1}{q_i}) = (-1)^{(q_i-1)/2}$ and $(\frac{2}{q_i}) = (-1)^{(q_i^2-1)/8}$.

for odd prime p and $\gcd(a,p) = 1$

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

is solvable iff $(\frac{a}{p}) = 1$.

for odd integer a

■ $x^2 \equiv a \pmod 2$ is always solvable.

■ $x^2 \equiv a \pmod 4$ is solvable iff $a \equiv 1 \pmod 4$.

■ $x^2 \equiv a \pmod{2^n}$ for $n \geqslant 3$ is solvable iff $a \equiv 1 \pmod 8$.

From above points we have if $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ for odd primes p_i and $\gcd(a,n) = 1$ then $x^2 \equiv a \pmod n$ is solvable iff

■ $(\frac{a}{p_i}) = 1$

■ $a \equiv 1 \pmod 4$ if $4|n$ but $8 \not| n$ or $a \equiv 1 \pmod 8$ if $8|n$.

7 References

[1] David M. Burton : Elementary number theory, McGraw·Hill, 7, (2010).