$e = \mathrm{ord}_p(n) \iff p^e \mid n \;\&\; p^{e+1} \nmid n$

① Prove that $\mathrm{ord}_p(mn) = \mathrm{ord}_p(m) + \mathrm{ord}_p(n)$.

Congruences

① $ax \equiv ay \pmod m$, then

$$x \equiv y \left(\mathrm{mod}\ \frac{m}{\gcd(a,m)}\right)$$

② $ax \equiv b \pmod m$ has a solution $x \in \mathbb{Z}$ iff $\gcd(a,m) \mid b$.

Unique solution modulo $\frac{m}{\gcd(a,m)}$.

③ $ax + by = c$ has integer solutions iff $\gcd(a,b) \mid c$.

$$x = x_1 + \frac{b}{\gcd(a,b)}n \;;\; y = y_1 - \frac{a}{\gcd(a,b)}n \;;\; n \in \mathbb{Z}$$

④ If $ax + by = c$ is solvable, then there is a solution (x,y) s.t

$$0 \le x < \frac{b}{\gcd(a,b)} - 1$$

⑤ $a_1x_1 + \cdots + a_nx_n = c$

sol^n iff $\gcd(a_1, \ldots, a_n) \mid c$.

$$6x + 10y + 15z = 5$$

⑥ Residue class

$a \in \mathbb{Z}$

Residue class $\bar{a} = \{x \in \mathbb{Z} : x \equiv a \bmod m\}$

m distinct congruence classes modulo m.

$\bar{0}, \bar{1}, \ldots, \overline{m-1}$.

"Complete residue system" modulo m. $\{1, 7, 8\}$ mod 5

distinct x_i from each residue class mod m

$x_1, x_2 \ldots, x_m$

"Reduced residue system" modulo m:

distinct x_i from each residue class relatively prime to m.

$(x_i, m) = 1$.

$x, y \in \bar{a} \bmod m$ iff $(x, m) = (y, m)$

$\{x_1, x_2 \ldots, x_{\phi(m)}\}$ reduced residue system iff pairwise incongruent & $(x_i, m) = 1$.

$\{ax_1, ax_2 \ldots, ax_m\}$ is a complete &

$\{as_1, as_2 \ldots, as_{\phi(m)}\}$ is a reduced residue system.

$(a, m) = 1$

Euler's thm.

$(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \bmod m$

Fermat's thms

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

$a^{p-1} \equiv 1 \bmod p$. → Fermat's Little thm.

for every integer a, $a^p \equiv a \bmod p$. → Fermat's thm.

Chinese Remainder thm.

The system $x \equiv a_i \mod m_i$; $1 \le i \le k$
m_i are paircise relatively prime, has a unique solution modulo $m_1 m_2 \dots m_k$.

Remark: Read the proof carefully to solve problems.

Polynomial congruences

I $\begin{cases} f_1(x) \equiv 0 \mod m_1 \\ \vdots \\ f_2(x) \equiv 0 \mod m_2 \end{cases}$; X_j complete set of incongruent solutions mod m_j.

$n_j = |X_j|$

$\begin{cases} x \equiv a_1 \mod m_1 \\ \vdots \\ x \equiv a_2 \mod m_2 \end{cases}$

$(a_1, \dots, a_2) \in X_1 \times X_2 \dots \times X_2$

# of solution $n_1 n_2 \dots n_2$.

Ex. $x^2 + x + 1 \equiv 0 \mod 7$

Solutions $2, -3$ $\quad n_1 = 2$

$2x - 4 \equiv 0 \mod 6$ $\quad n_2 = 2$

" $\rightarrow 2, 2-1$

System will have 4 incongruent solutions

$\begin{cases} x \equiv 2 \mod 7 \\ x \equiv 2 \mod 6 \end{cases}$ $\quad \begin{cases} x \equiv -3 \mod 7 \\ x \equiv 2 \mod 6 \end{cases}$

$\begin{cases} x \equiv 2 \mod 7 \\ x \equiv -1 \mod 6 \end{cases}$ $\quad \begin{cases} x \equiv -3 \mod 7 \\ x \equiv -1 \mod 6 \end{cases}$

II $f(x) \in \mathbb{Z}[x]$.

Solution set $X(m)$ of $f(x) \equiv 0 \mod m$.

$N(m) = \#\, X(m)$

Let $m = m_1 \dots m_2$ $\quad (m_i, m_j) = 1$ $\quad i \neq j$

$N(m) = N(m_1) \times \dots \times N(m_2)$

$(a_1, a_2 \cdots, a_r) \in X(m_1) \times \cdots \times X(m_r)$, then corresponds a unique solution $a \in X(m)$ s.t $a \equiv a_i \bmod m_i$ for each i.

Ex. $x^2 + x + 9 \equiv 0 \bmod 63$

$\Updownarrow$

$x^2 + x + 9 \equiv 0 \bmod 9$

$x^2 + x + 9 \equiv 0 \bmod 7$

↳ Solve

III Modulo prime p.

p is prime, then every polynomial congruence

$f(x) \equiv 0 \bmod p$

$\Leftrightarrow r(x) \equiv 0 \bmod p$, $\deg r(x) < p$.

$f(x) = x^{11} + 2x^8 + x^5 + 3x^4 + 4x^3 + 1 \equiv 0 \bmod 5$

Assume $n \geq p$,

$n \equiv r \bmod p-1$,

$1 \leq r < p-1$,

$x^n \equiv x^r \bmod p \quad \forall x$.

Use Fermat's thm.

$x^p - x$

Obtain $r(x)$ by dividing $f(x)$ by $x^5 - x$.

$5x^4 + 5x^3 + x + 1$

Consequence of this analysis

Wilson's thm. p prime, then

$(p-1)! \equiv -1 \bmod p$

Number of roots: $\deg f(x) = n$

① Almost n roots $f(x) \equiv 0 \bmod p$.

If not all coefficients of $f(x)$ are divisible by p

② Exactly n roots $f(x) \equiv 0 \bmod p$

If every coefficient of $r(x)$ is divisible by p.

where $r(x)$ is

$$x^p - x = q(x) f(x) + r(x) \; ; \; \deg r(x) < \deg f(x)$$

Ex. $d \mid p-1$,

No. of roots of $x^d - 1 \equiv 0 \bmod p$

IV Modulo prime powers p^k.

p prime, $f(x) \in \mathbb{Z}[x]$.

a is a root of $f(x) \equiv 0 \bmod p^k$.

Then, the solutions b of $f(x) \equiv 0 \bmod p^{k+1}$ with $b \equiv a \bmod p^k$ are as follows.

(i) $(p, f'(a)) = 1$, then ∃ a unique solution b,

$$b = a + p^k t \; ; \; t \text{ is the unique}$$

solution to $f'(a)\, t \equiv -\frac{f(a)}{p^k} \bmod p$

(ii) $(p, f'(a)) \neq 1$ & $p^{k+1} \mid f(a)$, then

p solutions

$f(x) \equiv 0 \bmod p^{k+1}$ that are

congruent to $a \bmod p^k$.

$a + p^k t \quad ; \quad t = 0, 1, 2, \ldots, p-1$

(iii) $(p, f'(a)) \neq 1, \quad p^{k+1} \nmid f(a)$.

No solutions to

$f(x) \equiv 0 \bmod p^{k+1}$

that are congruent to $a \bmod p^k$.

Remark:

p prime, $k \in \mathbb{Z}^+$,

$f(a) \equiv 0 \bmod p$; $(p, f'(a)) \neq 1$,

then there exist precisely

1 sol^n b of

$f(x) \equiv 0 \bmod p^k$ s.t

$b \equiv a \bmod p$.

Ex. $7x^6 + 4x + 12 \equiv 0 \bmod 135$

$135 = 3^3 \cdot 5$

Quadratic Residues

Suppose $(a, m) = 1$. Then, a is called a quadratic residue mod m if $x^2 \equiv a \bmod m$ has a sol.^{n}.

quadratic non residue mod m : no sol.^{n}.

Thm. If $p > 2$, $(a, p) = 1$, then

$x^2 \equiv a \bmod p^k$ has exactly 2 roots if a is a quadratic residue mod p, & no solutions if a is a quadratic non residue mod p. ($x^2 \equiv a \bmod p$)

$p = 2$

Thm. Suppose a is odd.

(i) $x^2 \equiv a \bmod 2$ always solvable & has exactly 1 sol.^{n}.

(ii) $x^2 \equiv a \bmod 4$ is always solvable iff $a \equiv 1 \bmod 4$,

in which case there are precisely 2 solutions

(iii) $x^2 \equiv a \bmod 2^k$; $k \geq 3$ is solvable iff $a \equiv 1 \bmod 8$, in this case there are exactly 4 solutions.

$$\{ x_0, -x_0, x_0 + 2^{k-1}, -x_0 + 2^{k-1} \}$$

Thm. $x^2 \equiv a \bmod m$ is solvable iff $x^2 \equiv a \bmod p_i$ is (a is a quadratic residue mod p_i)

($m = 2^k p_1^{k_1} \cdots p_r^{k_r}$ $(p_i, 2) = 1$ distinct)

and $a \equiv 1 \bmod 4$

$a \equiv 1 \bmod 8$

Euler's Criterion

$(p, 2) = 1$, $(a, p) = 1$

a is a quadratic residue mod p iff

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

a is a quadratic non residue mod p

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

Legendre Symbol

$(p, 2) = 1$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & " \quad " \quad " \quad \text{non } " \text{ mod } p. \\ 0 & p \mid a \end{cases}$$

Euler's criterion in terms of Legendre Symbol.

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

Properties of Legendre Symbol

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

Law of quadratic reciprocity

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