Chap 23 elements of number theory

$a, b \in \mathbb{Z}$ Def: a is congruent to b, modulo n, if a and b, when they are divided by n, leave the same remainder r: $a = nq_1 + r$ and $b = nq_2 + r$.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a-b \Leftrightarrow \bar{a} = \bar{b} \text{ in } \mathbb{Z}_n$$

Thm: $\bar{a}$ is invertible in $\mathbb{Z}_n$ iff a and n are relatively prime.

Pf: $\gcd(a,n)=1 \Leftrightarrow \exists\, u, v \in \mathbb{Z}$ s.t. $au + nv = 1 \Leftrightarrow au \equiv 1 \bmod n$ for some $u \in \mathbb{Z}$

$$\Updownarrow$$

$$\bar{a} \cdot \bar{u} = \bar{1} \text{ in } \mathbb{Z}_n$$

Cor: $\mathbb{Z}_p$ is a field for every prime number p.

$\mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \cdots, \overline{p-1}\}$ is a group of order $p-1$.

Little Theorem of Fermat: Let p be a prime. Then

$$a^{p-1} \equiv 1 \bmod p \quad \text{for every } a \not\equiv 0 \bmod (p)$$

Pf: $|\mathbb{Z}_p^*| = p-1$, $|\langle a \rangle| \,\big|\, |\mathbb{Z}_p^*| \Rightarrow \mathrm{ord}(a)$ in $\mathbb{Z}_p^*$ divides $p-1$.

$(a \not\equiv 0 \bmod p)$ $a^{p-1} \equiv 1 \bmod p \Leftarrow \bar{a}^{p-1} = \bar{1}$ in $\mathbb{Z}_p^*$

Cor: $a^p \equiv a \pmod{p}$ for every integer a.

For any positive integer n, Let $\phi(n) = \#\{m \in \mathbb{Z};\ 0 < m < n,\ \gcd(m,n) = 1\}$.

For any integer n, let V_n denote the set of all the invertible elements in $\mathbb{Z}_n$

Then V_n is a group w.r.t. multiplication. $|V_n| = \phi(n)$

Euler's Thm: If a and n are relatively prime, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Pf: $\gcd(a,n) = 1 \Rightarrow \bar{a} \in V_n \Rightarrow \mathrm{ord}(\bar{a}) \,\big|\, |V_n| \Rightarrow \bar{a}^{\phi(n)} = \bar{1}$ in V_n

$$\Updownarrow$$

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

Solve linear Diophantine equations is equivalent to solving linear congruences:

$$ax+by=c \Leftrightarrow by=c-ax \Leftrightarrow ax\equiv c \pmod b \qquad (a,b,c,x,y\in\mathbb{Z})$$

<u>Thm</u>: The congruence $ax\equiv b \pmod n$ has a solution iff $\gcd(a,n)\mid b$

<u>Pf</u>: $ax\equiv b \pmod n$ has a solution $\Leftrightarrow \exists\, y\in\mathbb{Z}$, s.t. $\underbrace{b-ax=ny}_{\Updownarrow\ ax+ny=b}$

$$\Leftrightarrow b\in \underset{\gcd(a,n)}{\overset{\parallel}{(a,n)}} \Leftrightarrow \gcd(a,n)\mid b$$

We want to find all solutions to $ax\equiv b \pmod n$

<u>Thm</u>: If the congruence $ax\equiv b \pmod n$ has a solution, then it has a solution modulo m, where $m=\frac{n}{\gcd(a,n)}$

<u>Pf</u>: $ax\equiv b \pmod n$ has a solution $\Leftrightarrow \overset{c}{\overset{\parallel}{\gcd(a,n)}}\mid b$

$\exists\, y, y'\in\mathbb{Z}$

x is a solution $\Leftrightarrow b-ax=ny$ for some $y\in\mathbb{Z}$ $\Leftrightarrow a(x'-x)=n(y-y')$

x' any solution $\Leftrightarrow b-ax'=ny'$ $\quad y'\in\mathbb{Z}$ $\quad \Updownarrow\ a'=\frac{a}{c},\ n'=\frac{n}{c}$

$$\frac{n}{\gcd(a,n)}\mid x-x' \Leftrightarrow n'\mid x-x' \Leftrightarrow n'\mid a'(x-x) \Leftrightarrow a'(x-x)=n'(y-y')$$

$\gcd(a',n')=1$

Alternatively, $ax\equiv b \pmod n$ has a solution $x \Leftrightarrow n\mid (ax-b)$ and $c=\gcd(a,n)\mid b$

$\Leftrightarrow n'\mid a'x-b' \Leftrightarrow a'x\equiv b' \pmod{n'}$ has a solution $(a',n')=1$.

$a'=\frac{a}{c},\ n'=\frac{n}{c},\ b'=\frac{b}{c}$

$\Leftrightarrow \bar{x}=(\bar{a}')^{-1}\bar{b}'$ in $\mathbb{Z}_{n'}$

all solutions to $ax\equiv b \pmod n$ are congruent to n'.

Exer: 1.(a) $60x = 12 \pmod{24}$

$\cdot \gcd(60, 24) = 12$, $12 \mid 12 \Rightarrow \exists$ solution.

$\cdot$ $\frac{60}{12}x = \frac{12}{12} \left(\bmod \frac{24}{12}\right) \Leftrightarrow 5x = 1 \pmod 2 \Leftrightarrow \bar{5}\bar{x} = \bar{1}$ in $\mathbb{Z}_2$

$\Updownarrow$

x is odd $\Leftrightarrow x \equiv 1 \pmod 2 \Leftrightarrow \bar{x} = \bar{1}$ in $\mathbb{Z}_2$

1.(e) $147x \equiv 47 \pmod{98}$

$\cdot \gcd(\underset{7^2\times 3}{\overset{\shortparallel}{147}}, \underset{7^2\times 2}{\overset{\shortparallel}{98}}) = 49$ $\quad 49 \nmid 47 \Rightarrow$ no solutions.

4.(c) $30x^2 \equiv 18 \pmod{24}$: $\left(\gcd(\underset{6\times 5}{\overset{\shortparallel}{30}}, \underset{6\times 4}{\overset{\shortparallel}{24}}) = 6 \quad 6 \mid 18\right) \Leftrightarrow \frac{30}{6}x^2 \equiv \frac{18}{6} \bmod \left(\frac{24}{6}\right)$

$5x^2 \equiv 3 \pmod 6$

$\Leftrightarrow \bar{5}\,\overline{x^2} = \bar{3}$ in $\mathbb{Z}_6$ $\Leftrightarrow \overline{x^2} = \bar{5}^{-1} \cdot \bar{3} = \bar{5}\cdot\bar{3} = \overline{15} = \bar{3}$ in $\mathbb{Z}_6$

$(\bar{5}^2 = \overline{25} = \bar{1} \Rightarrow \bar{5}^{-1} = \bar{5})$

$\Leftrightarrow \bar{x} = \bar{3}$ in $\mathbb{Z}_6$ $\quad (\bar{1}^2 = \bar{1},\ \bar{2}^2 = \bar{4},\ \bar{3}^2 = \bar{9} = \bar{3},\ \bar{4}^2 = \overline{16} = \bar{4},\ \bar{5}^2 = \overline{25} = \bar{1}$

$\Leftrightarrow x \equiv 3 \pmod 6$

4.(f) $\underset{3(x^2-2x+1)+3 = 3(x-1)^2+3}{\overset{\shortparallel}{3x^2-6x+6}} \equiv 0 \pmod{15} \Leftrightarrow 3(x-1)^2 \equiv -3 \pmod{15}$

$\Updownarrow$

$(x-1)^2 \equiv -1 \pmod 5 \Leftrightarrow (x-1)^2 \equiv 4 \pmod 5$

$\Leftrightarrow \underset{(\overline{x-1})^2}{\overset{\shortparallel}{\overline{(x-1)^2}}} = \bar{4}$ in $\mathbb{Z}_5$ $\Leftrightarrow \underset{\bar{x}-\bar{1}}{\overset{\shortparallel}{\overline{x-1}}} = \bar{2}$ or $\bar{3}$ in $\mathbb{Z}_5$

$\Leftrightarrow \bar{x} = \bar{3}$ or $\bar{4}$ in $\mathbb{Z}_5$ $\Leftrightarrow x \equiv 3 \pmod 5$ or $x \equiv 4 \pmod 5$

A.6 (d) $30x^2 + 24y = 18 \Rightarrow \underset{6\times 5}{\overset{\shortparallel}{30}}x^2 \equiv \underset{6\times 3}{\overset{\shortparallel}{18}} \pmod{24} \Leftrightarrow 5x^2 \equiv 3 \pmod 4$

$\Leftrightarrow \bar{5}\underset{\overline{x^2}}{\overset{\shortparallel}{\bar{x}^2}} = \bar{3}$ in $\mathbb{Z}_4$ $\quad \bar{1}^2 = \bar{1},\ \bar{2}^2 = \bar{4} = \bar{0},\ \bar{3}^2 = \bar{9} = \bar{1}$. So no solution

$\bar{3}$ is not a square in $\mathbb{Z}_4$

Exer: 1. (b) $42x \equiv 24 \pmod{30}$

- $\gcd(42,30)=6$ $\quad 6 \mid 24 \Rightarrow \exists$ solution
- $7x \equiv 4 \pmod 5 \Leftrightarrow \underset{\underset{\bar{2}\cdot\bar{x}}{\parallel}}{\bar{7}\cdot\bar{x}} = \bar{4}$ in $\mathbb{Z}_5 \Leftrightarrow \bar{x} = \bar{2}^{-1}\cdot\bar{4} = \bar{3}\cdot\bar{4}$
$= \overline{12} = \bar{2}$ in $\mathbb{Z}_5$

$\Leftrightarrow x \equiv 2 \pmod 5$

1.(c) $49x \equiv 30 \pmod{25}$

- $\gcd(49,25)=1$ $\quad 1 \mid 30 \Rightarrow \exists$ solution
- $\overline{49}\,\bar{x} \equiv \overline{30}$ in $\mathbb{Z}_{25} \Leftrightarrow -\bar{x} = \bar{5}$ in $\mathbb{Z}_{25} \Leftrightarrow \bar{x} = -\bar{5}$ $\mathbb{Z}_{25}$

$\Leftrightarrow x \equiv -5 \pmod{25} \Leftrightarrow x \equiv 20 \pmod{25}$

1(d) $39x \equiv 14 \pmod{52}$

- $\gcd(39,52)=13$ $\quad 13 \nmid 14 \Rightarrow$ no solutions.

4. (a) $6x^2 \equiv 9 \pmod{15}$

- $\gcd(6,15)=3 \Rightarrow \frac{6}{3}x^2 \equiv \frac{9}{3} \left(\mathrm{mod}\ \frac{15}{3}\right)$

$\Leftrightarrow 2x^2 \equiv 3 \pmod 5 \Leftrightarrow \bar{2}\,\overline{x^2} = \bar{3}$ in $\mathbb{Z}_5 \Leftrightarrow \overline{x^2} = \underset{\underset{\bar{3}}{\parallel}}{\bar{2}^{-1}}\cdot\bar{3} = \underset{\underset{\bar{9}}{\parallel}}{\bar{4}}$ in $\mathbb{Z}_5$

a: $\bar{0}\ \bar{1}\ \bar{2}\ \bar{3}\ \bar{4}$ $\Rightarrow \bar{x} = \bar{2}$ or $\bar{x} = \bar{3}$

a^2: $\bar{0}\ \bar{1}\ \bar{4}\ \underset{\underset{\bar{4}}{\parallel}}{\bar{9}}\ \underset{\underset{\bar{1}}{\parallel}}{\overline{16}}$

$\Leftrightarrow x \equiv 2 \pmod 5$ or $x \equiv 3 \pmod 5$

4.(b) $60x^2 \equiv 18 \pmod{24}$

$\gcd(60,24)=12$. $\quad 12 \nmid 18 \Rightarrow$ no solution

4. (d) $4(x+1)^2 \equiv 14 \pmod{10}$

$(\gcd(4,10) = 2 \quad 2 \mid 14)$ $\Leftrightarrow$ $\frac{4}{2}(x+1)^2 \equiv \frac{14}{2} \left(\bmod \frac{10}{2}\right)$

$\Leftrightarrow 2(x+1)^2 \equiv 7 \pmod{5} \Leftrightarrow \bar{2} \cdot \overline{(x+1)^2} = \bar{7} = \bar{2}$ (mod 5) in $\mathbb{Z}_5$

$\Leftrightarrow \overline{(x+1)^2} = \bar{2}^{-1} \bar{2} = \bar{1} \Leftrightarrow \overline{(x+1)}^2 = \bar{1}$ in $\mathbb{Z}_5$.

$\bar{0}\ \bar{1}\ \bar{2}\ \bar{3}\ \bar{4}$

$\bar{0}\ \bar{1}\ \bar{4}\ \bar{9}\ \overline{16}$, $\bar{9} = \bar{4}$, $\overline{16} = \bar{1}$

$\Leftrightarrow \overline{x+1} = \bar{1}$ or $\overline{x+1} = \bar{4}$

$\Leftrightarrow \bar{x} = \bar{0}$ or $\bar{x} = \bar{3}$ in $\mathbb{Z}_5$

$\Leftrightarrow x \equiv 0 \pmod{5}$ or $x \equiv 3 \pmod{5}$.

4. (e) $4x^2 - 2x + 2 \equiv 0 \pmod{6}$

$\Updownarrow$

$4x^2 + 4x \equiv -2 \pmod{6} \Leftrightarrow 4x^2 + 4x + 1 \equiv -2 + 1 \pmod{6}$

$4(x+1)^2 \equiv -1 \pmod{6}$

$\gcd(4,6) = 2 \quad 2 \nmid -1 \Rightarrow$ no solutions.

E.4 Let p and q be distinct primes. Then $p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}$

Fermat's little thm $\Rightarrow$ $p^{q-1} \equiv 1 \pmod q$ =

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

$\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$

$\overline{m}_{(pq)} \mapsto (\overline{m}_{(p)}, \overline{m}_{(q)})$

$\overline{p}_{(pq)} \mapsto (0, \overline{p}_{(q)})$

$\overline{q}_{(pq)} \mapsto (\overline{q}_{(p)}, 0)$

$$\overline{p}_{(pq)}^{\,q-1} + \overline{q}_{(pq)}^{\,p-1} \mapsto (0, \overline{p}_{(q)}^{\,q-1}) + (\overline{q}_{(p)}^{\,p-1}, 0)$$

$$= (0, \overline{1}_{(q)}) + (\overline{1}_{(p)}, 0) = (\overline{1}_{(p)}, \overline{1}_{(q)})$$

$$\Rightarrow \overline{p}_{(pq)}^{\,q-1} + \overline{q}_{(pq)}^{\,p-1} = \overline{1}_{(pq)}$$

$$\Leftrightarrow p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}$$

OR consider $(p^{q-1}-1)(q^{p-1}-1) = p^{q-1}q^{p-1} - p^{q-1} - q^{p-1} + 1$

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

$pq \mid p^{q-1}q^{p-1} (= p \cdot q\,(p^{q-2}q^{p-2}))$

$\Rightarrow pq \mid p^{q-1}+q^{p-1}-1 \Leftrightarrow p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}$

E.6 Let p and q be distinct primes.

(a) If $p-1 \mid m$ and $q-1 \mid m$, then $a^m \equiv 1 \pmod{pq}$ for any a s.t. $p \nmid a$ and $q \nmid a$

Pf. $p \nmid a \Rightarrow a^{p-1} \equiv 1 \bmod p \overset{p-1\mid m}{\Longrightarrow} a^m \equiv 1 \bmod p \Leftrightarrow p \mid a^m - 1$

$q \nmid a \Rightarrow a^{q-1} \equiv 1 \bmod q \overset{q-1\mid m}{\Longrightarrow} a^m \equiv 1 \bmod q \Leftrightarrow q \mid a^m - 1$

$\Rightarrow (pq) \mid a^m - 1$

$\Updownarrow$

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

(b) If $(p-1) \mid m$ and $(q-1) \mid m$, then $a^{m+1} \equiv a \pmod{pq}$ $\forall a \in \mathbb{Z}$

Pf: $(p \mid a,\ q \nmid a)$ $q \nmid a \Rightarrow a^{q-1} \equiv 1 \pmod q \overset{q-1\mid m}{\Longrightarrow} a^m \equiv 1 \pmod q \Rightarrow q \mid a^m - 1$

$\Rightarrow q \mid a^{m+1} - a$

If $p \mid a$, then $p \mid a^{m+1} - a$ $\Big\} \overset{p \neq q}{\Rightarrow} pq \mid a^{m+1} - a \Leftrightarrow a^{m+1} \equiv a \pmod{pq}$

Similarly for $p \nmid a,\ q \mid a$

If $p \mid a,\ q \mid a$, then $pq \mid a \Rightarrow pq \mid a^{m+1} - a \Leftrightarrow a^{m+1} \equiv a \pmod{pq}$

If $p \nmid a,\ q \nmid a$ then E.6(a) implies