Linear congruences

Thm: The eqn $\boxed{ax \equiv b \mod n}$ has a soln if & only if $\gcd(a,n) \mid b$.

Proof: if: $\gcd(a,n)\, b_1 = b$ for some $b_1 \in \mathbb{Z}$.

$d = \gcd(a,n)$

Set $a = a_1 \gcd(a,n)$ & $n = n_1 \underbrace{\gcd(a,n)}$

Then $a_1 x \equiv b_1 \mod n_1$

$a_1 d\, x = b_1 d \mod n_1 d$

$n_1 d \mid (a_1 x - b_1) d$

$\Rightarrow n_1 \mid a_1 x - b_1$

Since $a_1$ & $n_1$ are coprime,

$\exists\, s, t$ s.t. $s a_1 + t n_1 = 1$

$\iff s a_1 \equiv 1 \mod n_1$

$\therefore a_1$ has an inverse modulo $n$.

$x \equiv s b_1 \mod n_1$

only if: if $\alpha$ is a soln, $a_1 d \alpha = b \mod n_1 d$

$\therefore a_1 d \alpha - b = n_1 d r \Rightarrow b$ is divisible by $d$.

---

$U(\mathbb{Z}_n) \to$ the group of units

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

$\|$

the number of natural number $< n$ & coprime to $n$.

In particular $\mathbb{Z}_p$ is a field.

$|U(\mathbb{Z}_p)| = p-1$

$\phi(p) = p-1$

$\phi(p^2) = p^2 - p$, $\phi(p^3) = p^3 - p^2$, $\phi(p^n) = \underbrace{p^n - p^{n-1}}$.

$\mathbb{Z}_{p^n} \leftarrow \mathbb{Z}/p^n\mathbb{Z}$ ~~elements~~ $\alpha \in \mathbb{Z}_{p^n}$ is ~~not~~ a zero divisor if & only if $\alpha = pk$ $\underbrace{0 \le k \le p^{n-1}-1}$ $p^{n-1}$ possibilities

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

Corollary 1. If $\gcd(a,n)=1$, then $ax \equiv b \mod n$ has a unique sol$^n$.

Proof: Existence of a sol$^n$ follows from the thm. ($\gcd(a,n)=1$ divides $b$)

Uniqueness: If $a\alpha \equiv b \mod n$ & $a\beta \equiv b \mod n$ $\longrightarrow$ $0 \le \alpha, \beta \le n-1$

$\alpha > \beta$

then $a(\underset{\sim}{\alpha-\beta}) \equiv 0 \mod n$

$\Rightarrow \alpha - \beta \equiv 0 \mod n$

$\Rightarrow \alpha = \beta$ as $0 \le \alpha, \beta \le n-1$

---

Cor: 2. If $d = \gcd(a,n)$, $b \mid d$ & $\boxed{\left(\frac{a}{d}\right)\alpha_0 \equiv \left(\frac{b}{d}\right) \mod \frac{n}{d}}$

then sol$^{ns}$ of $\boxed{ax \equiv b \pmod n}$

are given by $\alpha_0,\ \alpha_0 + \frac{n}{d},\ \alpha + \frac{2n}{d}, \ldots, \alpha + (d-1)\frac{n}{d}$.

given by the thm.

---

$$a\left(\alpha_0 + \frac{kn}{d}\right) = a\alpha_0 + k\, a\left(\frac{n}{d}\right) \equiv a\alpha_0 \left(\mod \frac{n}{d}\right)$$

so $\alpha_0 + \frac{kn}{d}$ in $\mathbb{Z}_n$ is a sol$^n$ of $ax \equiv b \mod n$.

---

E.g. 1. $7x \equiv 14 \pmod{20}$

closure $\gcd(7,20)=1$

$3 = 7^{-1} \mod 20$. $x = 14 \times 3 \mod 20 = 2 \mod 20$.

Eg. 2 $7x \equiv 14 \pmod{21}$

$x \equiv 2 \pmod 3$

$2,\quad 2+3,\quad 2+2\times3,\quad 2+3\times3$

$2,\quad 5,\quad 8,\quad 11,\quad 14,\quad 17,\quad 20$

are the sol$^n$s of $7x \equiv 14 \pmod{21}$

E.g. 3) $\quad 4x \equiv 18 \pmod{22}$

Solve $\quad 2x \equiv 9 \pmod{11}$

$\iff \quad x \equiv 6 \times 9 \equiv 10 \mod 11.$

10, $\quad 10 + 11 = 21 \quad$ are soln.

System of linear eqns (congruence)

Thm: The system of eqns.

$$ax + by \equiv r \pmod n$$
$$cx + dy \equiv s \pmod n$$

has a unique soln modulo $n$ whenever $\gcd(ad-bc, n) = 1$

Proof: $\quad adx + bdy \equiv rd \pmod n$

$bcx + bdy \equiv bs \pmod n$

Substracting $\quad \boxed{(ad-bc)x \equiv (rd - bs) \pmod n}$

Since $\gcd(ad-bc, n) = 1$, the above linear eqn

has unique soln. say $\alpha_0$.

Then find $y$ using the given eqns.

$$\begin{bmatrix} by \equiv r - a\alpha \mod n \\ dy \equiv s - c\alpha \mod n \end{bmatrix}$$

E.g.
$$\begin{cases} 5x + 3y \equiv 10 \mod 12 \\ 2x + 7y \equiv 6 \mod 12 \end{cases}$$

$ad-bc$

$ad - bc = 5 \times 7 - 2 \times 3 = 35 - 6 = 29 \quad$ co-prime to $\quad 12 = n$

$29 \equiv 5 \mod 12 \qquad 29^{-1} = 5^{-1} \pmod{12}$

$= 5 \pmod{12} \longrightarrow$ (observe $5 \times 5 = 25 \equiv 1 \mod 12$)

$$x = 5^{-1}(v_1 - 6s) = 5 \times (\underline{10 \times 7} - \underline{3 \times 6}) \mod 12$$
$$\equiv 5 \times 52 \mod 12$$
$$\equiv 5 \times 4 \mod 12$$
$$\underline{\equiv 8 \mod 12}$$

Find $y$

$$5x + 3y = 10 \Rightarrow 3y = 10 - 5 \times 8 \mod 12$$
$$= 6 \mod 12$$
$$y \equiv 2 \mod 4$$

$$\underline{y = 2 \text{ or } 6 \text{ or } 10} \mod 12$$

$$2x + 7y = 6 \Rightarrow 7y = 6 - 2 \times 8 \mod 12$$
$$= 2 \mod 12$$

$$y = 7^{-1} 2 \equiv 7 \times 2 \mod 12$$
$$\equiv 2 \mod 12$$

So $(8, 2)$ is the only soln.