# Linear congruences

Given $a, b, n \in \mathbb{N}$, find $x \in \mathbb{Z}$ s.t.

$$ax \equiv b \pmod{n}.$$

Equivalently, $n \mid ax - b \iff$ [illegible]

$$ax - b = ny \iff ax - ny = b$$

Solvable iff $d := \gcd(a, n)$ divides $b$, $d \mid b$.

when $d \mid b$, $\exists$ $d$ solutions modulo $n$: if $x_0, y_0$ solve $ax - ny = b$,

then $x = x_0 + \left(\frac{n}{d}\right)t$, $y = y_0 + \left(\frac{a}{d}\right)t$, for $t = 0, 1, \ldots, d-1$.

To see that these solutions are incongruent:

suppose that $x_0 + \left(\frac{n}{d}\right)t_1 \equiv x_0 + \left(\frac{n}{d}\right)t_2$ for $0 \le t_1 < t_2 \le d-1$

$\implies$ $\left(\frac{n}{d}\right)t_1 \equiv \left(\frac{n}{d}\right)t_2 \pmod{n}$

$\implies$ $t_1 \equiv t_2 \pmod{d}$ $\implies$ can't happen!

In addition: suppose that $x = x_0 + \left(\frac{n}{d}\right)t$ for some $t \in \mathbb{Z}$.

Division Lemma: $t = qd + r$, for $0 \leq r < d$

Then $x = x_0 + \left(\frac{n}{d}\right)(qd + r) = x_0 + nq + \left(\frac{n}{d}\right)r$

$\equiv x_0 + \left(\frac{n}{d}\right)r \pmod{n}$

---

NOTE: if $\gcd(a, n) = 1$, then $ax \equiv b \pmod{n}$ has a unique solution.

1(b) $5x \equiv 2 \pmod{26}$ :

$5x - 26y = 2$ $\qquad \gcd(5, 26) = 1$, and

$(-10)\cdot 5 + 26(2) = 2$

$(-10)(5) - (-2)(26) = 2$ $\qquad -5\cdot 5 + 26 = 1$

$x_0 = -10 \implies x = -10 + 26t \implies x = 16$ is the solution mod 26.

---

1(d) $36x \equiv 8 \pmod{102}$ $\qquad \gcd(36, 102)$: $102 = 2\cdot 36 + 30$

$36x - 102y = 8$ $\qquad \underline{6}$ $\qquad 36 = 30 + \underline{6}$

$30 = 5\cdot 6$

$6 \nmid 8$ ∴

---

1(c) $6x \equiv 15 \pmod{21}$ $\qquad \gcd(6, 21)$: $21 = 3\cdot 6 + 3$

$6x - 21y = 15$ $\qquad \underline{3}$ $\qquad 6 = 2\cdot 3$

Have $-3\cdot 6 + 21 = 3 \implies (-15)\cdot 6 + 5\cdot 21 = 15 \implies x_0 = -15$

$x = -15 + 7t \implies \boxed{x = 6, 13, 20}$

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}$$

**Assumption:** $\gcd(n_i, n_j) = 1$ for $i \neq j$

Need $\gcd(n_i, a_i) \mid b_i$ for $i = 1, \ldots, k$

If $\gcd(n_i, a_i) \mid b_i \ \forall\, i$, then divide by $\gcd(n_i, a_i)$ to get

$$\begin{cases} a_1' x \equiv b_1' \pmod{n_1'} \\ \vdots \\ a_k' x \equiv b_k' \pmod{n_k'} \end{cases}$$

where $\gcd(a_i', n_i') = 1$ for $i = 1, \ldots, k$

Then get

$$\begin{cases} x_1 \equiv c_1 \pmod{n_1'} \\ x_2 \equiv c_2 \pmod{n_2'} \\ \vdots \\ x_k \equiv c_k \pmod{n_k'} \end{cases}$$

# Chinese Remainder Theorem

Suppose that $\gcd(n_i, n_j) = 1$ for all $i \neq j$,
and let $c_1, \ldots, c_r \in \mathbb{N}$ be given. Then the system

$$x \equiv c_1 \pmod{n_1}$$
$$x \equiv c_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv c_r \pmod{n_r}$$

has a solution that is unique modulo $n_1 n_2 \cdots n_r$.

pf. Define $N := n_1 n_2 \cdot \ldots \cdot n_r$, and define $N_i = \frac{N}{n_i}$.
(ex: $N_1 = n_2 n_3 \cdot \ldots \cdot n_r$ etc.). Then $\gcd(n_i, N_i) = 1$,
and the congruence $N_i x \equiv 1 \pmod{n_i}$ has a unique solution,
$x_i$. Then $c_i N_i x_i \equiv c_i \pmod{n_i}$, and

$$x := c_1 N_1 x_1 + c_2 N_2 x_2 + \ldots + c_r N_r x_r$$ solves the system.

4(a) $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$ $\qquad 3 \cdot 5 \cdot 7 = 105$

$x \equiv 3 \pmod 7$

$35x \equiv 1 \pmod 3$ | $21x \equiv 1 \pmod 5$ | $15x \equiv 1 \pmod 7$

$x_1 = 2$ | $x_2 = 1$ | $x_3 = 1$

$x = \underline{35} \cdot 2 \cdot 1 + \underline{21} \cdot 1 \cdot 2 + \underline{15} \cdot 1 \cdot 3$

$= 70 + 42 + 45 = 157 \equiv 52 \pmod{105}$

$\boxed{x = 52}$