Linear Congruences

$ax \equiv b \pmod{m}$ $\quad m \in \mathbb{N}$, $a, b \in \mathbb{Z}$

Solve for x

(Thm) Let $d = \gcd(a, m)$. $ax \equiv b \pmod{m}$ is solvable iff $d \mid b$. If $d \mid b$, then all solutions are congruent modulo $\frac{m}{d}$. In particular, the solution is unique modulo m if a, m are coprime.

(Proof)

($\Rightarrow$) Suppose that $ax \equiv b \pmod{m}$ has a solution, say, x'.

$ax' \equiv b \pmod{m}$ i.e., $ax' = b + km$ for some $k \in \mathbb{Z}$

$d \mid a, d \mid m \Rightarrow d \mid ax' - km$ i.e., $d \mid b$.

($\Leftarrow$) Suppose that $d \mid b$. We know $d \mid a$, $d \mid m$

$a = a'd \quad m = m'd \quad b = b'd$

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

$ax \equiv b \pmod{m}$

$a'dx \equiv b'd \pmod{m'd}$ → divide the congruence by d

$a'x \equiv b' \pmod{m'}$

$\therefore a', m'$ are relatively prime, a' is invertible modulo m'.

$x \equiv \underline{(a')^{-1} b' \pmod{m'}}$

solution modulo $m' = \frac{m}{d}$

Suppose that x_1, x_2 are 2 solutions for the congruence.

$ax_1 \equiv b \equiv ax_2 \pmod{m}$

$ax_1 \equiv ax_2 \pmod{m}$

Dividing by a, we have $x_1 \equiv x_2 \pmod{\frac{m}{\gcd(a,m)}}$ $x_1 \equiv x_2 \pmod{\frac{m}{d}}$

x_0 : unique soln. modulo $\frac{m}{d}$

$x_0 + k\frac{m}{d}$ $\quad k \in \mathbb{Z}$: integer solutions

$x_i = x_0 + i\left(\frac{m}{d}\right)$ $\quad 0 \le i \le d-1$: solutions modulo m (exactly d)

Example

$15x \equiv 4 \pmod{24}$ $\quad \gcd(15, 24) = 3$

has no solns. $\quad 3 \nmid 4$

$15x \equiv 6 \pmod{24}$ $\quad 3 \mid 6$ $\quad \exists$ exactly 3 solutions modulo 24

$5x \equiv 2 \pmod{8}$

$x \equiv 5^{-1} \cdot 2 \pmod{8}$

$\equiv 5 \cdot 2 \pmod{8}$

$\equiv 2 \pmod{8}$

Solns. modulo 24 : $2, 2+8, 2+2\cdot 8$

$2, 10, 18$

Solving congruences modulo several moduli

(Thm) Chinese Remainder Theorem

Let $m_1, m_2, \cdots, m_t$ be pairwise coprime moduli
& let $a_1, a_2, \cdots, a_t \in \mathbb{Z}$.

pairwise coprime: $\gcd(m_i, m_j) = 1 \quad \forall \ 1 \le i < j \le t$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_t \pmod{m_t}$$

The above congruences are simultaneous solvable
& the solution is unique modulo $M = m_1 m_2 \cdots m_t$

Proof

$M = m_1 m_2 \cdots m_t$

Let $n_i = \frac{M}{m_i}$ for $i = 1, 2, \cdots, t$

$\gcd(n_i, m_i) = 1$

n_i is invertible modulo m_i

u_i : inverse of n_i modulo m_i

$$x' = \sum_{i=1}^{t} n_i u_i a_i$$

To show that x' satisfies all the linear congruency we need to show that $x' \equiv a_j \pmod{m_j}$ $\forall\ 1 \le j \le t$

$$x' \pmod{m_j} \equiv \left(\sum_{i=1}^{t} n_i u_i a_i\right) \pmod{m_j}$$

$$\equiv n_j u_j a_j \pmod{m_j}$$

$m_j \mid n_i \quad \forall\ i \neq j$

$u_j n_j \equiv 1 \pmod{m_j}$

$$\equiv a_j \pmod{m_j}$$

x_1, x_2 : 2 solutions

$$x_1 \equiv a_i \pmod{m_i} \equiv x_2$$

$$x_1 \equiv x_2 \pmod{m_i}$$

$$m_i \mid x_1 - x_2 \quad \forall\ i = 1, 2, \cdots, t$$

Since m_i's are pairwise coprime

$$m_1 m_2 \cdots m_t \mid x_1 - x_2$$

$$x_1 \equiv x_2 \pmod{M}$$

$x \equiv 2 \pmod 3 \quad x \equiv 7 \pmod 8 \quad x \equiv 4 \pmod{11}$

$m_1 = 3 \quad m_2 = 8 \quad m_3 = 11$

$a_1 = 2 \quad a_2 = 7 \quad a_3 = 4$

$M = m_1 m_2 m_3 = 264$

$n_1 = \frac{M}{m_1} = 88 \quad n_2 = \frac{M}{m_2} = 33 \quad n_3 = \frac{M}{m_3} = 24$

$u_1 \equiv 88^{-1} \pmod 3 \equiv 1 \quad u_2 \equiv 33^{-1} \pmod 8 \equiv 1 \quad u_3 \equiv 24^{-1} \pmod{11}$

$\equiv 2^{-1} \pmod{11}$

$\equiv 6 \pmod{11}$

$x = n_1 u_1 a_1 + n_2 u_2 a_2 + n_3 u_3 a_3$

$= 88 \cdot 2 + 33 \cdot 7 + 24 \cdot 6 \cdot 4$

$= 983 \equiv 191 \pmod{264}$

$191 + k \cdot 264$

$k \in \mathbb{Z}.$

Algorithm CRT

i/p : $a[0, \ldots, t-1]$ $m[0, \ldots, t-1]$

o/p : x satisfying $x \equiv a[i] \pmod{m[i]}$ for all $i = 0, 1, \ldots, t-1$

```
M ← 1 ; x ← 0 ;
for i ← 0 to t-1 do
    M ← M * m[i] ;
end for
for i ← 0 to t-1 do
    n ← M / m[i] ;
    u ← inverse ( n rem m[i] , m[i] ) ;
    x ← x + n*u * a[i] ;
end for
return x rem M ;
```

$t+2t=3t$ multiplications

$t+1$ Euclidean divisions

t runs of Extended GCD

t divisions