Linear congruences

A congruence is of the form.

$$ax \equiv b \mod m$$

where m is a positive integer and a, b are integers
x is an integer variable.

The solution of this congruence are all integers that satisfy this equation.

Multiplicative inverse

$\bar{a}$ is a multiplicative inverse of a modulo m if

$$a\,\bar{a} \equiv 1 \bmod m.$$

How this is used to solve linear congruence?

$$ax \equiv b \bmod m.$$

$$\Rightarrow \underbrace{\bar{a}\,a}\,x \equiv \bar{a}\,b \bmod m.$$

$$\Rightarrow x \equiv \bar{a}\,b \bmod m.$$

$\underline{\underline{Ex^n}}$ find multiplicative inverse of 5 mod 9

$\underline{\underline{Sol^n}}$ need to find $\bar{a}$ s.t

$$5 \cdot \bar{a} \equiv 1 \mod 9.$$

$$5 \cdot 1 \equiv 5 \mod 9.$$

$$5 \cdot \underline{\underline{2}} = 10 \equiv 1 \mod 9.$$

multiplicative inverse is $\underline{2}$.

Exm Find multiplicative inverse of

$7 \bmod 11$

Soln Find $\bar{a}$ s.t. $7 \cdot \bar{a} \equiv 1 \bmod 11$

$7 \cdot 1 = 7 \equiv 7 \bmod 11$

$7 \cdot 2 = 14 \equiv 3 \bmod 11$

$7 \cdot 3 = 21 \equiv 10 \bmod 11$

$7 \cdot 4 = 28 \equiv 6$ " 11

$7 \cdot 5$

.

.

.

$7 \cdot \boxed{8} = 56 \equiv 1 \bmod 11$

Ex.^{m} Find multiplicative inverse of

$3 \bmod 6$

Sol^n

$3 \cdot 1 = 3 \equiv 3$

$3 \cdot 2 = 6 \equiv 0$

$3 \cdot 3 = 9 \equiv 3$

$3 \cdot 4 = 12 \equiv 0$

If a and m are relatively prime and $m > 1$ then a multiplicative modulo m exists.
Further this inverse is unique.

Ex^n Find x such that $3x \equiv 7 \bmod 10$

Sol^n

$3x \equiv 7 \bmod 10$

$\Rightarrow x \equiv \bar{3}\,7 \bmod 10$

$\Rightarrow x \equiv 7 \cdot 7 \bmod 10$

$\Rightarrow x \equiv 49 \bmod 10$

$\Rightarrow x \equiv 9 \bmod 10$

$3 \cdot 7 \equiv 1 \bmod 10$

$3^{-1} = 7$

The chinese remainder theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers then the system.

$$x_1 \equiv a_1 \bmod m_1$$
$$x_2 \equiv a_2 \bmod m_2$$
$$\vdots$$
$$x_n \equiv a_n \bmod m_n$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot \cdots \cdot m_n$

Proof

$$p_i = m_1 m_2 \cdots m_{i-1}\, m_{i+1} \cdots m_n$$

$\gcd(p_i, m_i) = 1 \Rightarrow \exists$ two integers s_i and t_i

s.t. $\gcd(p_i, m_i) = s_i p_i + t_i m_i$

$$\Rightarrow s_i p_i + t_i m_i = 1$$

$$\Rightarrow s_i p_i + t_i m_i \equiv 1 \mod m_i$$

$$\Rightarrow s_i p_i \equiv 1 \mod m_i$$

Now assume a solutin x as,

$$x = a_1 s_1 p_1 + a_2 s_2 p_2 + \cdots + a_n s_n p_n$$

If $j \neq i$, $m_i \mid p_j$ s. take mod m_i we get,

$$x \equiv a_i s_i p_i \mod m_i$$

$$\Rightarrow x \equiv a_i \mod m_i$$

x is a unique solution

Assuming there are at least 2 solutions x and y.
modulo m,

$x \equiv a_1 \bmod m_1$ $\qquad$ $y \equiv a_1 \bmod y_1$

$\vdots$ $\qquad$ $\vdots$

$x = a_i \equiv y \bmod m_i$ $\qquad$ so, $x - y \equiv 0 \bmod m_i$

$\Rightarrow m_i \mid x-y$

$\operatorname{lcm}(m_1, m_2, \ldots, m_n) \mid x-y$

$\Rightarrow m_1 \cdot m_2 \cdot \cdots m_n \mid x-y$. $\Rightarrow x \equiv y \bmod (m_1 m_2 \cdots m_n)$

$\underline{\underline{Ex^m}}$ $\underline{\text{Solve:}}$ $x \equiv 2 \mod 7$

$x \equiv 3 \mod 8$

$\underline{\underline{Sol^n}}$

solution is $x \equiv a_1 s_1 p_1 + a_2 s_2 p_2 \pmod{m_1 m_2}$

$p_1 = 8$ so $s_1 = 1$

$p_2 = 7$ $s_2 = 7$

$s_i p_i \equiv 1 \mod m_i$

$s_1 8 \equiv 1 \mod 7$

$s_1 \equiv 8^{-1} \mod 7$

$= 1$

$$x \equiv 2 \cdot 1 \cdot 8 + 3 \cdot 7 \cdot 7 \pmod{7 \cdot 8}$$

$$\equiv 16 + 147 \pmod{56}$$

$$\equiv 163 \pmod{56}$$

$$\equiv 51$$

Ex^m

$$x \equiv 2 \mod 3$$
$$x \equiv 5 \mod 7$$
$$x \equiv 4 \mod 5$$
$$x \equiv 3 \mod 4$$

Sol^n

$$x = a_1 p_1 s_1 + a_2 s_2 p_2 + a_3 s_3 p_3 + a_4 s_4 p_4 \mod m$$

HW