

Monday 7/23/2007

Linear congruences, inverses, and Chinese remainder theorem

A linear congruence is a congruence of the form $ax \equiv b \pmod{m}$.

These may or may not have solutions:

$$3x \equiv 2 \pmod{4}$$

$$x \equiv 2$$

$$2x \equiv 1 \pmod{6}$$

no solution

$$9x \equiv 6 \pmod{12}$$

$$x \equiv 2$$

- Thm: If $\gcd(a, m) = 1$ then $ax \equiv b \pmod{m}$ has a solution.
(If $\gcd(a, m) \neq 1$, then there may or may not be a solution.)

A special situation of this is the congruence

$$ax \equiv 1 \pmod{m}.$$

Since a and x multiply to 1, we say a and x are multiplicative inverses modulo m .

- Theorem: a has a multiplicative inverse modulo m iff $\gcd(a, m) = 1$.
— We denote the inverse of a by \bar{a} .

— Eg! For $m = 7$:
if $a = 2$ then $\bar{a} = 4$
if $a = 6$ then $\bar{a} = 6$.

Q: How do we find inverses? For instance, given $\gcd(a, m) = 1$, what is \bar{a} ?

A! Here's how: Since $\gcd(a, m) = 1$, we know there are integers x and y such that $1 = ax + my$. If we take this modulo m , then we get $1 \equiv ax + 0 = ax \pmod{m}$. So x is our \bar{a} !

An application of inverses is the Chinese Remainder Theorem:

— Ex: $X \equiv 2 \pmod{3}$ Find a value of X between 0 and $3 \cdot 5 \cdot 7$ that satisfies all 3 congruences.
 $X \equiv 3 \pmod{5}$
 $X \equiv 2 \pmod{7}$

Solution: Construct X as follows:

$$X \equiv \underbrace{2 \cdot (5 \cdot 7) \cdot \overline{(5 \cdot 7)}}_{\text{mod } 3} + \underbrace{3 \cdot (3 \cdot 7) \cdot \overline{(3 \cdot 7)}}_{\text{mod } 5} + \underbrace{2 \cdot (3 \cdot 5) \cdot \overline{(3 \cdot 5)}}_{\text{mod } 7}$$

this is the value of X when taken modulo 3.
 these ensure that this term will vanish when taken modulo 5 or modulo 7.
 This cleans up the damage done by the $(5 \cdot 7)$.

$$\begin{aligned}
 &= \underbrace{2 \cdot 35 \cdot 2}_{140} + \underbrace{3 \cdot 21 \cdot 1}_{63} + \underbrace{2 \cdot 15 \cdot 1}_{30} \\
 &= 140 + 63 + 30 \\
 &= 233 \equiv \boxed{23} \pmod{105}.
 \end{aligned}$$

Now check: Indeed, $X=23$ satisfies all 3 congruences!

Thm: The Chinese Remainder Theorem:

The system $X \equiv a \pmod{m_1}$
 $X \equiv b \pmod{m_2}$
 $X \equiv c \pmod{m_3}$ has a unique solution between 0 and $m_1 \cdot m_2 \cdot m_3$, (provided that m_1, m_2, m_3 are pairwise coprime).

The solution will be $X \equiv a(m_2 m_3) \overline{(m_2 m_3)} + b(m_1 m_3) \overline{(m_1 m_3)} + c(m_1 m_2) \overline{(m_1 m_2)} \pmod{m_1 m_2 m_3}$.

Note: The Chinese Remainder theorem can be extended to any number of linear congruences, so long as all moduli are pairwise coprime. (pairwise coprime just means everything is coprime to everything else).