Equations

Problem

Solve $3x \equiv 13 \mod 26$

$$x \equiv 3^{-1} \cdot 13 \mod 26$$

$$x \equiv 9 \cdot 13 \mod 26$$

$$x \equiv 13 \mod 26$$

Problem

Solve $4x \equiv 12 \mod 26$

$$x \equiv 4^{-1} \cdot 12 \mod 26$$

One solution is

$$x \equiv 3 \mod 26.$$

Chinese Remainder Theorem

Find the smallest non-negative integer x such that the following equations hold simultaneously:

$$\left.\begin{aligned} x &\equiv 3 \pmod{13} \\ x &\equiv 6 \pmod{14} \\ x &\equiv 9 \pmod{15} \end{aligned}\right\} (*)$$

Soln

Let $a \equiv 14^{-1} \pmod{13}$

$b \equiv 15^{-1} \pmod{13}$

A first attempt at solving (*) is

$$X = 3 \cdot 14 \cdot a \cdot 15 \cdot b$$

$x \equiv 3 \pmod{13}$

$x \equiv 0 \pmod{14}$

$x \equiv 0 \pmod{15}$

Let $c \equiv 13^{-1} \pmod{14}$

$d \equiv 15^{-1} \pmod{14}$

Let

$Y = 6 \cdot 13 \cdot c \cdot 15 \cdot d$

Note:

$Y \equiv 0 \pmod{13}$

$Y \equiv 6 \pmod{14}$

$Y \equiv 0 \pmod{15}$

Now let

$e \equiv 13^{-1} \pmod{15}$

$f \equiv 14^{-1} \pmod{15}$

Let

$Z = 9 \cdot 13 \cdot e \cdot 14 \cdot f$

Note:

$z \equiv 0 \pmod{13}$

$z \equiv 0 \pmod{14}$

$z \equiv 9 \pmod{15}$

Now take

$x = X + Y + Z$

Note

$x \equiv X+Y+Z \equiv 3+0+0 \equiv 3 \pmod{13}$

$x \equiv X+Y+Z \equiv 0+6+0 \equiv 6 \pmod{14}$

$x \equiv X+Y+Z \equiv 0+0+9 \equiv 9 \pmod{15}$

To finish we must calculate

X, Y, Z and $x = X+Y+Z$.

$a \equiv 14^{-1} \mod 13$

$\boxed{a = 1}$

$b \equiv 15^{-1} \mod 13$

$b \equiv 2^{-1} \mod 13$

$\boxed{b \equiv 7}$

$c \equiv 13^{-1} \mod 14$

$c \equiv (-1)^{-1}$

$c \equiv -1$

$\boxed{c \equiv 13}$

$d \equiv 15^{-1} \mod 14$

$\boxed{d \equiv 1}$

$e \equiv 13^{-1} \mod 15$

$\boxed{e \equiv 7}$

$f \equiv 14^{-1} \mod 15$

$\boxed{f \equiv 14}$

$X = 3.14.1.15.7$

$Y = 6.13.13.15.1$

$Z = 9.13.7.14.14$

$x = X + Y + Z$

$\equiv 2694 \mod 13.14.15$

So $x = 2694$ is the smallest non-negative integer satisfying the system of equations (*).

The method works because $\gcd(13,14) = 1$, $\gcd(13,15) = 1$, $\gcd(14,15) = 1$.

The method works for any system

$$\left.\begin{aligned} x &\equiv a \mod l \\ x &\equiv b \mod m \\ x &\equiv c \mod n \end{aligned}\right\} *$$

with $\gcd(l,m) = \gcd(l,n) = \gcd(m,n) = 1$.