7 Linear Equations mod m

Given $a, c \in \mathbb{Z}$, we want to solve

$$ax \equiv c \ (\text{mod } m) \qquad (*)$$

Note that we can solve the "congruence" (I) iff we can solve

$$ax + my = c \qquad \star$$

with $x, y \in \mathbb{Z}$.

We have looked at $\star$ before.

Recall:

(i) For $\star$ to have a solution in integers, it is necessary and sufficient to have c be divisible by the gcd, say d, of a, m.

(ii) Let u, v satisfy

$$\left(\frac{a}{d}\right) u + \left(\frac{m}{d}\right) v = 1 \qquad \star'$$

This is possible as $(\frac{a}{d}, \frac{m}{d}) = 1$.

All the solutions for $\star'$ are obtained by first finding one solution, say (u_0, v_0) and writing the general solution as

$$(u, \mathrm{v}) = \left(u_0 + k\frac{m}{d}, \mathrm{v}_0 - k\frac{a}{d}\right)$$

for any $k \in \mathbb{Z}$.

So the general solution of $\star$ is given by

$$\begin{aligned}(x, y) &= \left(c\left(u_0 + \frac{km}{d}\right),\ c\left(\mathrm{v}_0 - \frac{ka}{d}\right)\right) \\ &= \left(cu_0 + k\frac{c}{d}m,\ c\mathrm{v}_0 - k\frac{c}{d}a\right)\end{aligned}$$

So the general solution to (*) is given by

$$x = cu_0 + k\left(\frac{c}{d}\right)m$$

Suppose x, x' are both solutions of (*) mod m. Then

$$a(x - x') \equiv 0 \text{ mod } m,$$

so

$$m|a(x-x').$$

Since $d = gcd(a, m)$ we need

$$\frac{m}{d}|(x-x')$$

Example. $m = 6,\ a = 4$

$$4(x-x') \equiv 0 \pmod 6,\ d = 2 \Leftrightarrow 3|(x-x')$$

So

$$(x-x') \equiv 0 \text{ or } 3 \pmod 6$$

In general, if $(a, m) = d$, then

$$a(x-x') \equiv 0 \pmod m \Rightarrow x-x' \text{ is divisible by } \frac{m}{d}$$

There exists exactly d distinct solutions of (*) mod m. So we have

Lemma. $ax \equiv c \pmod m$ has solutions if

$$d{=}gcd(a, m) \mid c.$$

When $d|c$, there are d distinct solutions mod m.

Corollary: $ax \equiv 1 \pmod m$ can be solved iff $(a, m) = 1$. Moreover, the solution is unique in this case.

Definition: If $(a, m) = 1$, we call the unique $x \pmod m$ such that $ax \equiv 1 \pmod m$ the **inverse** of a mod m.

Often, people write it as $a' \pmod m$.

Example. $m = 7,\ a = 2,\ a' = 4 \pmod 7$.

Recall

$$\mathrm{S}_0 = \{0, 1, \ldots, m-1\}$$

is a set of reps. for $\mathbb{Z}/m$. (It is the standard set of reps.)

Definition:

$$(\mathbb{Z}/m)^* = \{\text{Invertible elements of } \mathbb{Z}/m\}$$

$$\varphi(m) = \#(\mathbb{Z}/m)^*$$

Explicitly,

$$\varphi(m) = |\{a \in \{0, 1, \ldots, m-1\}\ |(a, m) = 1\}|.$$