9 Linear congruences revisited

Theorem. Fix $m > 1$. Let $a, c \in \mathbb{Z}$. Put $d = gcd(a, m)$. Then the congruence

$$ax \equiv c \pmod{m} \tag{*}$$

has a solution $x \pmod{m}$ iff $d|c$. Moreover, when $d|c$, all d solutions are of the form

$$x \equiv \frac{cu_0 + mk}{d} \pmod{m},$$

with $k \in \mathbb{Z}$, where (u_0, v_0) is a solution of $au + mv = d$.

We already proved (*) has a solution $x \pmod{m}$ iff $d|c$. So let $d|c$. Let (u_0, v_0) be a solution of

$$au + mv = d. \tag{**}$$

Multiply by c, get

$$acu_0 + mcv_0 = cd,$$

i.e.,

$$a\left(\frac{cu_0}{d}\right) + m\left(\frac{cv_0}{d}\right) = c$$

$$\Rightarrow a\left(\frac{cu_0}{d}\right) \equiv c \pmod{m}$$

$$\Rightarrow x \equiv \frac{cu_0}{d} \pmod{m} \text{ is a solution of (*).}$$

Recall that we get all the solutions of (**) by taking

$$(u, v) = \left(u_0 + \frac{km}{d},\ v_0 - \frac{kc}{d}\right),$$

as k runs over $\mathbb{Z}$. So the general solution of (*) is given by

$$x \equiv \frac{cu_0}{d} + \frac{km}{d} \equiv \frac{cu_0 + km}{d} \pmod{m}$$

Corollary: $ax \equiv 1 \pmod{m}$ has a solution iff $(a, m) = 1$. In this case, $\exists!$ solution, the multiplicative inverse of a mod m, and denoted $a' \pmod{m}$.

We knew before that a has a multiplicative inverse if $(a, m) = 1$. This corollary replaces the if by iff.

Definition:

$$(\mathbb{Z}/m)^* = \{a \in \mathbb{Z}/m | (a, m) = 1\}.$$

Note: By corollary, $(\mathbb{Z}/m)^*$ is precisely the subset of $\mathbb{Z}/m$ consisting of elements which have multiplicative inverses mod m.
Recall:

$$\begin{aligned} \varphi(m) &= |(\mathbb{Z}/m)^*|. \\ &= |\{a \in \{0, 1, \ldots, m-1\} | (a, m) = 1\}|. \end{aligned}$$

In the previous section we proved the following:

Theorem: (Euler) For any $a \in \mathbb{Z}$ with $(a, m) = 1$,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Corollary. (Fermat's Little Theorem)

$$m = p \text{ (prime)},\ p|a \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

Remark. Fermat's Little Theorem says that

$$x^{p-1} \equiv 0 \pmod{p}$$

has $p - 1$ solutions mod p, namely

$$x \equiv 1, 2, \ldots, p-1 \pmod{p}$$

$$\Rightarrow a^p - a \equiv 0 \pmod{p},\ \forall a = 1, 2, \ldots, p-1.$$

This is also true for

$$a \equiv 0 \pmod{p}.$$

So,

$$x^p - x \equiv 0 \pmod{p}$$

has p solutions mod p. On the other hand,

$$x^p \equiv 0 \pmod{p}$$

has only one solution, namely $x \equiv 0 \pmod{p}$. In other words, if $a \neq 0$ (mod p), then a^p cannot be 0 (mod p).

Claim. If $ab \equiv 0 \pmod{p}$, then either a or b must be $\equiv 0 \pmod{p}$.

Proof of Claim. Suppose $a \not\equiv 0 \pmod{p}$. Then

$$a \in (\mathbb{Z}/p)^*,$$

and so $\exists a'$ such that $a'a \equiv 1 \pmod{p}$. Multiple both sides of $ab = 0$ (mod p) by a' to get $(aa')b \equiv 0 \pmod{p}$, giving

$$b \equiv 0 \pmod{p}.$$

Conclusion: $\mathbb{Z}/p$ has no "zero divisors."

Note: If m is any integer > 1 which is **not** a prime, then $\mathbb{Z}/m$ has zero divisors.

Proof. Since m is composite, we can write $m = m_1, m_2$ with $m_1, m_2 > 1$. then

$$m_1 m_2 \equiv 0 \pmod{m},$$

but neither m_1 nor m_2 is $\equiv 0 \pmod{m}$.

Moral: Congruences modulo a prime p are nicer to study. They have much more structure.