Linear Congruences and the Chinese Remainder Theorem

Ryan C. Daileda

Trinity University

Number Theory

Linear Congruences

Given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, a *linear congruence* has the form

$$ax \equiv b \pmod{n}. \tag{1}$$

Goal: Describe the set of solutions to (1).

Notice that if $x_0 \in \mathbb{Z}$ is a solution to (1) and $x_1 \equiv x_0 \pmod{n}$, then

$$ax_1 \equiv ax_0 \equiv b \pmod{n},$$

so that x_1 is also a solution.

It follows that every integer in the congruence class $x_0 + n\mathbb{Z}$ solves (1).

It is therefore natural to describe the solution set in terms of congruence classes (i.e. as elements of $\mathbb{Z}/n\mathbb{Z}$).

Notice that

$$\begin{aligned} ax \equiv b \pmod{n} &\Leftrightarrow n | ax - b \\ &\Leftrightarrow ax - b = ny \\ &\Leftrightarrow ax - ny = b, \end{aligned}$$

for some $y \in \mathbb{Z}$.

The Diophantine equation $ax - ny = b$ can be solved iff $(a, n) | b$, in which case

$$x = r\frac{b}{(a, n)} + m\frac{n}{(a, n)}, \quad y = \cdots ,$$

where $ar + ns = (a, n)$ and $m \in \mathbb{Z}$.

These will be distinct modulo n only for $m = 0, 1, 2, \ldots, (a, n) - 1$.

We have therefore reached our goal.

Theorem 1

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. The linear congruence $ax \equiv b \pmod{n}$ has solutions iff $(a,n)|b$. In this case there are exactly (a,n) incongruent solutions modulo n, given by

$$x \equiv r\frac{b}{(a,n)} + m\frac{n}{(a,n)} \pmod{n}$$

for $m = 0, 1, 2, \ldots, (a,n) - 1$, where $ar + ns = (a,n)$.

Remark. The solutions can also be described by the *single* congruence

$$x \equiv r\frac{b}{(a,n)} \left(\bmod \frac{n}{(a,n)} \right).$$

Example 1

Solve the congruence $231x \equiv 228 \pmod{345}$.

Solution. We have $(231, 345) = 3$ and $3|228$, so there are exactly 3 solutions modulo 345.

The Euclidean Algorithm gives

$$231 \cdot 3 - 345 \cdot 2 = 3,$$

so that

$$x \equiv 3 \cdot \frac{228}{3} + m\frac{345}{3} \equiv 228 + 115m \pmod{345},$$

for $m = 0, 1, 2$. That is,

$$\boxed{x \equiv 113, 228, 343 \pmod{345}.}$$

The Ring $\mathbb{Z}/n\mathbb{Z}$

Fix $n \in \mathbb{N}$. We can define two binary operations on $\mathbb{Z}/n\mathbb{Z}$. Given $a, b \in \mathbb{Z}$ we set

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z},$$
$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z}.$$

These operations are *well-defined*: they do not depend on which members of the congruence classes we choose to compute them.

To see this, suppose $a + n\mathbb{Z} = c + n\mathbb{Z}$ and $b + n\mathbb{Z} = d + n\mathbb{Z}$. Then $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$.

Properties of modular arithmetic then imply that

$$a + b \equiv c + d \pmod{n} \quad \text{and} \quad ab \equiv cd \pmod{n}.$$

Thus

$$(a+b)+n\mathbb{Z}=(c+d)+n\mathbb{Z} \quad \text{and} \quad (ab)+n\mathbb{Z}=(cd)+n\mathbb{Z},$$

as needed.

With the operations of congruence class addition and multiplication, $\mathbb{Z}/n\mathbb{Z}$ becomes a *commutative ring*:

- Addition and multiplication are associative and commutative (why?);
- There is an additive identity $(0+n\mathbb{Z})$ and there are additive inverses $(-(a+n\mathbb{Z})=(-a)+n\mathbb{Z})$;
- There is a multiplicative identity $(1+n\mathbb{Z})$;
- Multiplication distributes over addition.

We can view the linear congruence $ax \equiv b \pmod{n}$ as an *equation* in $\mathbb{Z}/n\mathbb{Z}$.

Our main result then states that this equation has exactly (a, n) solutions in $\mathbb{Z}/n\mathbb{Z}$, when $(a, n)|b$.

There is one particular instance that is worth mentioning separately.

Corollary 1

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $(a, n) = 1$, then $ax \equiv b \pmod{n}$ has exactly one *solution modulo n.*

Multiplicative Inverses in $\mathbb{Z}/n\mathbb{Z}$

Although every element of $\mathbb{Z}/n\mathbb{Z}$ has an additive inverse, the same is not true with multiplication.

For instance, the congruence $2x \equiv 1 \pmod 4$ cannot be solved, since $(2,4) \nmid 1$.

Thus, $2 + 4\mathbb{Z}$ cannot have a multiplicative inverse in $\mathbb{Z}/4\mathbb{Z}$.

An element of $\mathbb{Z}/n\mathbb{Z}$ with a multiplicative inverse is called a *unit* modulo n.

We will denote the set of units in $\mathbb{Z}/n\mathbb{Z}$ by $(\mathbb{Z}/n\mathbb{Z})^\times$.

According to Theorem 1:

$$\boxed{(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \,|\, (a,n) = 1\}.}$$

Because every congruence class is uniquely represented by a remainder, it is easy to see that

$$
\begin{aligned}
(\mathbb{Z}/2\mathbb{Z})^\times &= \{1+2\mathbb{Z}\},\\
(\mathbb{Z}/3\mathbb{Z})^\times &= \{1+3\mathbb{Z}, 2+3\mathbb{Z}\},\\
(\mathbb{Z}/4\mathbb{Z})^\times &= \{1+4\mathbb{Z}, 3+4\mathbb{Z}\},\\
(\mathbb{Z}/5\mathbb{Z})^\times &= \{1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\},\\
(\mathbb{Z}/6\mathbb{Z})^\times &= \{1+6\mathbb{Z}, 5+6\mathbb{Z}\}.
\end{aligned}
$$

In general, if p is a prime, then

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{1+p\mathbb{Z}, 2+p\mathbb{Z}, \dots, (p-1)+p\mathbb{Z}\}.$$

Multiplicative Inverses and Bézout's Lemma

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Suppose $(a, n) = 1$.

According to Bézout's Lemma, there exist $r, s \in \mathbb{Z}$ so that

$$\begin{aligned} ra + sn = 1 \;\; &\Rightarrow \;\; ra \equiv 1 \pmod{n} \\ &\Rightarrow \;\; (a + n\mathbb{Z})(r + n\mathbb{Z}) = 1 + n\mathbb{Z} \\ &\Rightarrow (a + n\mathbb{Z})^{-1} = r + n\mathbb{Z}. \end{aligned}$$

That is *the coefficient of a in Bézout's Lemma gives its multiplicative inverse in* $\mathbb{Z}/n\mathbb{Z}$.

The Euclidean Algorithm therefore provides us with an efficient means of computing inverses modulo n.

Let $m, n \in \mathbb{N}$ with $m|n$. Notice that for any $a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{n} \;\Rightarrow\; n|a-b \;\Rightarrow\; m|a-b \;\Rightarrow\; a \equiv b \pmod{m}.$$

It follows that the rule

$$a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$$

yields a well-defined function $r : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

It is easy to see that r is a *ring homomorphism*:

$$r\left((a + n\mathbb{Z}) + (b + n\mathbb{Z})\right) = r(a + n\mathbb{Z}) + r(b + n\mathbb{Z}),$$
$$r\left((a + n\mathbb{Z})(b + n\mathbb{Z})\right) = r(a + n\mathbb{Z})r(b + n\mathbb{Z}),$$

for all $a, b \in \mathbb{Z}$ (HW).

A factorization $n = m_1 m_2$ therefore defines

$$\begin{aligned} R : \mathbb{Z}/n\mathbb{Z} &\to (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \\ a + n\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, a + m_2\mathbb{Z}). \end{aligned}$$

Notice that

$$\left|(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})\right| = m_1 m_2 = n = \left|\mathbb{Z}/n\mathbb{Z}\right|.$$

This means R will be a bijection iff it is one-to-one. Is this true? Suppose that $R(a + n\mathbb{Z}) = R(b + n\mathbb{Z})$. Then

$$(a + m_1\mathbb{Z}, a + m_2\mathbb{Z}) = (b + m_1\mathbb{Z}, b + m_2\mathbb{Z}),$$

which is equivalent to saying that $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$.

Thus, $m_1 | a - b$ and $m_2 | a - b$. To conclude that R is injective we need to be able to conclude that $n = m_1 m_2$ divides $a - b$.

This implication fails in general, but if we also assume that $(m_1, m_2) = 1$, it is valid!

To summarize:

Theorem 2

Let $m_1, m_2 \in \mathbb{N}$ with $(m_1, m_2) = 1$. The map

$$a + m_1 m_2 \mathbb{Z} \mapsto (a + m_1 \mathbb{Z}, a + m_2 \mathbb{Z})$$

is a well defined bijection between $\mathbb{Z}/m_1 m_2 \mathbb{Z}$ and $\mathbb{Z}/m_1 \mathbb{Z} \times \mathbb{Z}/m_2 \mathbb{Z}$.

What does this say at the level of congruences?

Let $a_1, a_2 \in \mathbb{Z}$. Then $(a_1 + m_1\mathbb{Z}, a_2 + m_2\mathbb{Z}) \in \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$.

Theorem 2 ensures that there is a unique $a + m_1 m_2\mathbb{Z} \in \mathbb{Z}/m_1 m_2\mathbb{Z}$ so that

$$(a + m_1\mathbb{Z}, a + m_2\mathbb{Z}) = (a_1 + m_1\mathbb{Z}, a_2 + m_2\mathbb{Z}).$$

That is, there is an integer $x = a$ (unique modulo $m_1 m_2$) which solves the *simultaneous congruences*

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2}.$$

This is the *Chinese Remainder Theorem*.

Theorem 3 (Chinese Remainder Theorem)

Let $m_1, m_2 \in \mathbb{Z}$ *with* $(m_1, m_2) = 1$. *For any* $a_1, a_2 \in \mathbb{Z}$, *the system of congruences*

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2}.$$

has a unique solution modulo $m_1 m_2$.

Remarks.

- This generalizes to an arbitrary number of pairwise relatively prime moduli $m_1, m_2, \ldots, m_k$.
- The proof we have given is nonconstructive. We will give a constructive proof of the more general version shortly.

We need a preparatory lemma.

Lemma 1

Let $a, b, c \in \mathbb{Z}$*. If* $(a, c) = (b, c) = 1$*, then* $(ab, c) = 1$*.*

Proof. Use Bézout's Lemma to write

$$ar_1 + cs_1 = br_2 + cs_2 = 1$$

for some $r_i, s_i \in \mathbb{Z}$.

Then

$$1 = (ar_1 + cs_1)(br_2 + cs_2) = (ab)(r_1 r_2) + c(bs_1 r_2 + ar_1 s_2 + cs_1 s_2).$$

Since $r_1 r_2, bs_1 r_2 + ar_1 s_2 + cs_1 s_2 \in \mathbb{Z}$, this proves that $(ab, c) = 1$. □

Remark. The lemma immediately implies that

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \,|\, (a,n) = 1\}$$

is closed under multiplication of congruence classes.

An easy induction yields the following corollary.

Corollary 2

Let $a_1, a_2, \ldots, a_r, b \in \mathbb{Z}$. *If* $(a_i, b) = 1$ *for all* i, *then* $(a_1 a_2 \cdots a_r, b) = 1$.

The Chinese Remainder Theorem Revisited

Let $n_1, n_2, \ldots, n_r \in \mathbb{N}$ with $(n_i, n_j) = 1$ for all $i \neq j$.

Set $n = n_1 n_2 \cdots n_r$ and $N_i = n/n_i v = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_r$.

By Corollary 2, we have $(N_i, n_i) = 1$ for all i.

It follows that for each i there exists $x_i \in \mathbb{Z}$ so that $N_i x_i \equiv 1 \pmod{n_i}$.

Finally, given arbitrary $a_1 a_2, \ldots, a_r \in \mathbb{Z}$, set

$$a = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r.$$

Since $n_i | N_j$ for $j \neq i$, $a_j N_j x_j \equiv 0 \pmod{n_i}$ for sll $j \neq i$.

Furthermore, $a_i N_i x_i \equiv a_i \pmod{n_i}$.

Thus

$$\begin{aligned} a &= a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r \\ &\equiv 0 + 0 + \cdots + a_i + \cdots + 0 \equiv a_i \pmod{n_i} \end{aligned}$$

for any i.

That is, $x = a$ is a solution to the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_r \pmod{n_r}. \end{aligned}$$

We have therefore given a constructive proof of the existence portion of the following result.

Theorem 4 (Chinese Remainder Theorem)

Let $n_1, n_2, \ldots, n_r \in \mathbb{N}$ with $(n_i, n_j) = 1$ for all $i \neq j$. For any $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_r \pmod{n_r}. \end{aligned}$$

has a unique solution modulo $n_1 n_2 \cdots n_r$.

To prove uniqueness of the solution, note that our work so far shows that the map

$$\begin{aligned} \mathbb{Z}/n_1 n_2 \cdots n_r\mathbb{Z} &\to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \\ a + n_1 n_2 \cdots n_r\mathbb{Z} &\mapsto (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \ldots, a + n_r\mathbb{Z}) \end{aligned}$$

is surjective.

Because the domain and codomain both have size $n_1 n_2 \cdots n_r$, the pigeonhole principle implies the map is injective as well.

So any two solutions of the system must yield the same element of $\mathbb{Z}/n_1 n_2 \cdots n_r\mathbb{Z}$, i.e. they must be congruent modulo $n_1 n_2 \cdots n_r$.

Example

Example 2

Solve the system of congruences

$$\begin{aligned} 2x &\equiv 1 \pmod 5), & 3x &\equiv 9 \pmod 6),\\ 4x &\equiv 1 \pmod 7), & 5x &\equiv 9 \pmod{11}. \end{aligned}$$

Solution. We solve the congruences individually, then "glue" our solutions together using the CRT.

If we multiply both sides of the first congruence by 3 it becomes $x \equiv 3 \pmod 5$.

If we divide by 3 in the second congruence it becomes $x \equiv 3 \equiv 1 \pmod 2$.

If we multiply both sides of the third congruence by 2 we obtain $x \equiv 2 \pmod{7}$.

And if we multiply both sides of the final congruence by 2 it becomes $10x \equiv -x \equiv 18 \equiv 7 \pmod{11}$, or $x \equiv -7 \equiv 4 \pmod{11}$.

We therefore have the equivalent system

$$x \equiv 1 \pmod{2}, \quad x \equiv 3 \pmod{5},$$
$$x \equiv 2 \pmod{7}, \quad x \equiv 4 \pmod{11}.$$

Following the proof of the CRT, we set $n_1 = 2$, $n_2 = 5$, $n_3 = 7$ and $n_4 = 11$.

Then define $N_1 = 5 \cdot 7 \cdot 11 = 385$, $N_2 = 2 \cdot 7 \cdot 11 = 154$, $N_3 = 2 \cdot 5 \cdot 11 = 110$ and $N_4 = 2 \cdot 5 \cdot 7 = 70$.

We now need to invert each N_i modulo n_i.

Because the moduli are small, we can proceed by trial and error. We have

$$\begin{aligned} N_1 = 385 \equiv 1 \pmod 2 &\Rightarrow x_1 = 1, \\ N_2 = 154 \equiv -1 \pmod 5 &\Rightarrow x_2 = -1, \\ N_3 = 110 \equiv 5 \pmod 7 &\Rightarrow x_3 = 3, \\ N_4 = 70 \equiv 4 \pmod{11} &\Rightarrow x_4 = 3. \end{aligned}$$

Thus, one solution to the system is

$$a = 1 \cdot 385 \cdot 1 + 3 \cdot 154 \cdot (-1) + 2 \cdot 110 \cdot 3 + 4 \cdot 70 \cdot 3 = 1423,$$

and the general solution is

$$\boxed{x \equiv 1423 \equiv 653 \pmod{770}}.$$