Recap on Linear Congruence Equations

Emanuel Mompó

1 Goal

For a given linear congruence equation

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

we seek a value $x \in \mathbb{Z}_n$ that verifies it. Ideally, since $x + kn \equiv x \pmod{n}$ for any $k \in \mathbb{Z}$, we want $0 \leq x < n$.

2 How to solve them

First we will check if there's any solution, then find one, and finally find the remaining ones (if that's the case).

1. Let $d := \gcd(a, n)$. If $d|b$, there exists a solution to Eq. (1).
   Remark: We use Euclid's Lemma to compute d.

2. Solve an auxiliary equation:

   $$ax \equiv d \pmod{n} \tag{2}$$

   Notice that we replaced b by d. This is equivalent to finding $u, w \in \mathbb{Z}$ such that $au + nw = d = \gcd(a, n)$.
   Remark: Since $d = \gcd(a, n)$, Bézout's Identity says there are integer solutions to this equation, and we can find one tracking back on the computation of d by means of Euclid's Lemma.

3. From the previous step, we have that u solves Eq. (2), which means that $au \equiv d \pmod{n}$. As $d|b$, there's $q \in \mathbb{Z}$ such that $b = q \cdot d$. Then we can take $x \equiv q \cdot u \pmod{n}$ as it solves Eq. (1).

4. If $d > 1$, there are more solutions than this one. We can span the set of solutions using the expression $x_k = x_0 + \frac{b}{d}k$, where x_0 is the previously known solution, and giving integer values to k.
   Remark: Ideally, we only keep the d values of x_k that check $0 \leq x_k < n$.

3 Simplifications

The smaller a, b and n are, the easier it is to apply the previous approach by hand. Sometimes we can lower them.

1. If r divides a, b and n, then

$$ax \equiv b \pmod{n} \iff \frac{a}{r}x \equiv \frac{b}{r} \pmod{\frac{n}{r}}$$

   Remark 1: This "removes" solutions (more on this later).
   Remark 2: This rule makes sense since solving $ax \equiv b \pmod{n}$ is tightly related to solving $ax + ny = b$, so we can take common factors of a, n and b out.

2. If r divides a and b, and $\gcd(r, n) = 1$, then

$$ax \equiv b \pmod{n} \iff \frac{a}{r}x \equiv \frac{b}{r} \pmod{n}$$

   Remark: In this case only a and b are divided by r. This can be done since $\gcd(r, n) = 1$ and thus r has a multiplicative inverse on $\mathbb{Z}_n$.

3.1 Simplification examples

- $6x \equiv 4 \pmod{10}$. Since $r = 2$ divides 6, 4, and 10, we divide everything (rule 1) and solve $3x \equiv 2 \pmod{5}$. In this case $x \equiv 4 \pmod{5}$ is a solution, and it is unique since $\gcd(3, 5) = 1$.

Notice that we have given a solution but on $\mathbb{Z}_5$. The original equation is stated on $\mathbb{Z}_{10}$. Notice that $x \equiv 4 \pmod{10}$ is a solution (on $\mathbb{Z}_{10}$). But on $\mathbb{Z}_{10}$ we have $\gcd(6,10) = 2$ solutions.

- $6x \equiv 4 \pmod 7$. Here $r = 2$ divides 6 and 4, but $\gcd(2,7) = 1$, hence by using (rule 2) we restate the problem as solving $3x \equiv 2 \pmod 7$, which has $x \equiv 3 \pmod 7$ as solution, and also solves $6x \equiv 4 \pmod 7$.

4 Example

Let's solve

$$30x \equiv 18 \pmod{99} . \tag{3}$$

Notice that 3 divides 30, 18, and 99. Hence we simplify (rule 1) into a simpler equation $10x \equiv 6 \pmod{33}$. Moreover, as 2 divides 10 and 6, but $\gcd(33,2) = 1$, we simplify again (rule 2) and solve

$$5x \equiv 3 \pmod{33} . \tag{4}$$

1. We compute $d = \gcd(33,5)$:

$$\begin{aligned} 33 &= 5 \cdot 6 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + \boxed{1} \\ 2 &= 1 \cdot 2 + 0 \qquad \text{(we stop here)} \end{aligned}$$

   So there's $d = 1$ solutions on $\mathbb{Z}_{33}$.

2. We solve the auxiliar equation

$$5x \equiv d \pmod{33} , \tag{5}$$

   with $d = 1$. Reading the $\gcd(5,33)$ computation backwards, we have:

$$\begin{aligned} 1 &= 3 + (-1)2 && = 3 + (-1)[5 + (-1)3] = \\ &= (-1)5 + (2)3 && = (-1)5 + (2)[33 + (-6)5] = \\ &= (-13)5 + (2)33 && . \end{aligned}$$

Hence $u = -13$ and $w = 2$ solve the Bézout's Identity. So we take $\tilde{x} \equiv -13 \equiv 20 \pmod{33}$ as solution to the Eq. (5).

3. Go back to Eq. (4). As $3 = 3 \cdot d$, $x \equiv 20 \cdot 3 \pmod{33}$ solves Eq. (4). Thus $x \equiv 20 \cdot 3 \equiv 60 \equiv 27 \pmod{33}$ solves $5x \equiv 3 \pmod{33}$. So we have a solution, but on $\mathbb{Z}_{33}$.

4. Go back to Eq. (3). As the simplifications we did do not change the value of x, we can take as our first solution $x_0 = 27 \pmod{99}$.

   Also, notice that by going from Eq. (3) to Eq. (4), we divided 99 by 3 when using the simplification rule 1. So $\gcd(30, 99) = 3 \cdot \gcd(5, 33)$.[1] Thus there are 3 solutions on $\mathbb{Z}_{33}$. These are found by giving integer values to k in the expression
   $$x_k = x_0 + \frac{99}{3} k = 27 + 33k \,.$$
   If we restrict ourselves to values of x_k that land in $\{0, 1, \ldots, 99\}$, we have that the three solutions are $x \equiv 27,\ 60,\ 93 \pmod{99}$.

[1] Notice that simplification rule 2 does not affect the greatest common divisor of these two numbers, as the common factors (if any) of 33 and 10 were left untouched by rule 2.