SOLVING LINEAR CONGRUENCES

I have isolated proofs at the end. *Fancy not, even for a moment, that this means the proofs are unimportant!* They are *essential* to understanding the algorithm. Rather, I thought it easier to use this as a reference if you could see the algorithms with the examples first, and the proofs later.

LINEAR CONGRUENCES

Suppose $b, c, m \in \mathbb{Z}$, and $m \neq 0$. We often encounter problems of the form

(1) $$cx \equiv b \pmod{m}.$$

We would like to answer the following questions:

- *When* does a solution exist?
- *How many* solutions exist, modulo m?
- *What are* the solutions?

We will solve them by rewriting as a *different* problem. By definition, (1) is true if and only if we can find $y \in \mathbb{Z}$ such that

$$cx = b + my,$$

or, in other words,

(2) $$cx + m(-y) = b.$$

When we want integer solutions to such an equation, we call it a **Diophantine equation**.

Existence of solutions to a linear congruence. *A solution to (1) exists if and only if* $\gcd(c, m)$ *divides* b.

Number of solutions to a linear congruence. *If a solution to (2) exists, then:*

- *there are infinitely many solutions,*
- *the number of* unique *solutions, modulo* m, *is* $d = \gcd(b, m)$, *and*
- *if* (x_0, y_0) *is a solution, then so are* $(x_0 + m/d, y_0 - c/d)$, $(x_0 + 2 \cdot m/d, y_0 - 2 \cdot c/d)$, $\ldots$, *and* $(x_0 + (d-1) \cdot m/d, y_0 - (d-1) \cdot c/d)$.

Particular solutions to a linear congruence, *or*, Particular solutions to Diophantine equations, *or*, The Extended Euclidean Algorithm, *or*, Bezout's Identity. *For any integers* c, m *we can find integers* χ, υ *such that*

$$\gcd(c, m) = c\chi + m\upsilon.$$

In addition, we can find χ, υ *by reversing the equations generated during the Euclidean Algorithm. Thus,* $\chi \cdot b/\gcd(c,m)$ *is a particular solution to (1).*

Example. Suppose we want to solve $3x \equiv 6 \pmod{2}$. Since $\gcd(2, 3) = 1$, and 1 divides 3, there is one solution. We can find it using Bezout's Identity, since

$$3\chi + 2\upsilon = 1$$

when $\chi = 1$ and $\upsilon = -1$. Multiply the equation on both sides by 6 to obtain

$$3(6) + 2(-6) = 6.$$

Given the relationship between (1) and (2), our solution will be $x = 6$.

Example. Suppose we want to solve $4x \equiv 1 \pmod{6}$. This time, $\gcd(4,6) = 2$, which *does not* divide 1, so there is no solution. We can verify this by checking that the multiples of 4, modulo 6 are $4,2,0,4,2,0,\ldots$.

Example. Suppose we want to solve $4x \equiv 8 \pmod{12}$. Observe that $\gcd(4,12) = 4$, which divides 8, so there should be 4 solutions. The first one comes from scaling Bezout's identity,

$$4 \cdot 4 + 12 \cdot (-1) = 4,$$

by $2 = {}^{b}/_{\gcd(c,m)}$ to match $b = 8$,

$$4 \cdot 8 + 12 \cdot (-2) = 8,$$

so $x = 8$ is one solution to the congruence. The other ones that are unique *modulo 12* are

$$8 + {}^{12}/_{4} \equiv 11 \quad , \quad 8 + 2 \cdot {}^{12}/_{4} \equiv 2 \quad , \quad \text{and} \quad 8 + 3 \cdot {}^{12}/_{4} \equiv 5.$$

You can verify easily that $4 \cdot 11 \equiv 8 \pmod{12}$, $4 \cdot 2 \equiv 8 \pmod{12}$, and $4 \cdot 5 \equiv 8 \pmod{12}$.

Systems of linear congruences

The Chinese Remainder Theorem. *Let $a, b, m, n \in \mathbb{Z}$. If $\gcd(m,n) = 1$, then there exist infinitely many solutions to*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

In addition, there is only one solution between 0 and $mn - 1$ (inclusive), and all other solutions can be obtained by adding an integer multiple of mn.

Remark. While the theorem does not prescribe a particular way to find x, you can find it using the same ideas as in the previous section.

Remark. If either congruence has the form $cx \equiv a$ (mod m), and $\gcd(c,m)$ divides a, then you can solve by rewriting, just as above.

Example. Suppose we need to solve

$$\begin{aligned} x &\equiv 2 \pmod{8} \\ x &\equiv 12 \pmod{15}. \end{aligned}$$

The condition $x \equiv 2 \pmod{8}$ is equivalent to the equation $x = 2 + 8q$, for some $q \in \mathbb{Z}$. Substitute this into the second congruence, obtaining

$$2 + 8q \equiv 12 \pmod{15},$$

which we rewrite as

$$8q \equiv 10 \pmod{15}.$$

Now, $\gcd(8,15) = 1$, which divides 10, so there exists a unique solution, modulo 15. We can find it using the same technique as above, *or* by multiplying both sides by the multiplicative inverse of 8, modulo 15. That would be 2, since $8 \cdot 2 = 16 \equiv 1$. Hence

$$q \equiv 20 \equiv 5 \pmod{15}.$$

The solution to the system is thus $x = 2 + 8q = 42$, which is unique modulo $8 \cdot 15 = 120$.

We can verify easily that, in fact,

$$42 \equiv 2 \pmod{8} \quad \text{and} \quad 42 \equiv 12 \pmod{15}.$$

SO WHY DOES THIS WORK?

The discussion in the first section shows that we can determine a criterion for existence to solutions of a linear congruence (1) by looking at solutions of Diophantine equation (2). So, we restrict ourselves to the context of Diophantine equations.

***Existence* of solutions to a linear congruence.** Suppose a solution exists. Let $d = \gcd(c, m)$, and choose $q, r \in \mathbb{Z}$ such that $c = dq$ and $m = dr$. If b is a solution to (1), then it is also a solution to (2). Thus,

$$\begin{aligned} b &= cx + m(-y) \\ &= (dq)x + (dr)(-y) \\ &= d(qx - ry). \end{aligned}$$

By definition, d divides b.

On the other hand, if d divides b, then choose $q \in \mathbb{Z}$ such that $b = dq$. Bezout's Identity tells us that we can find t, u such that

$$d = ct + mu.$$

Multiply both sides by q transforms the equation to

$$b = dq = (ct + mu)q = c(tq) + m(uq).$$

Its extreme ends show that b is a solution to the Diophantine equation (2).

***Number* of solutions to a linear congruence.** If (x_0, y_0) is a solution to (2), then by definition $cx_0 + my_0 = b$. Let $d = \gcd(c, m)$. Observe that

$$\begin{aligned} b &= cx_0 + my_0 \\ &= cx_0 + my_0 + (cm/d - cm/d) \\ &= (cx_0 + cm/d) + (my_0 - cm/d) \\ &= c(x_0 + m/d) + m(y_0 - c/d). \end{aligned}$$

Since (x_0, y_0) was *any* solution, we can repeat this indefinitely. Hence, if *a* solution exists, *infinitely* many solutions must exist! However,

$$c(x_0 + d \cdot m/d) = cx_0 + cm \equiv cx_0 \pmod{m},$$

so there are no more than d distinct solutions, modulo m. On the other hand, if $0 \le t \le u < d$,

$$c(x_0 + t \cdot m/d) \equiv c(x_0 + u \cdot m/d),$$

is true if and only if

$$cx_0 + t \cdot cm/d \equiv cx_0 + u \cdot cm/d,$$

which is true if and only if

$$t \equiv u.$$

So there are in fact d distinct solutions, modulo m.

***Particular* solutions to a linear congruence.** This is already explained in the explanation for *Existence* of solutions to a linear congruence.