5.2 Linear congruences

Let us consider the linear congruence $ax \equiv b \pmod{n}$, where we are looking for solutions x.

We will regard solutions x_1, x_2 as the same if $x_1 \equiv x_2 \pmod{n}$.

Example 87.

(a) $3x \equiv 2 \pmod{7}$ has the solution $x = 3$. We regard $x = 10$ or $x = 17$ as the same solution. We therefore write that $x \equiv 3 \pmod{7}$ is the unique solution to the equation.

(b) $3x \equiv 2 \pmod{9}$ has no solutions x.

Why? Reducing $3x = 2 + 9m$ modulo 3, we get $0 \equiv 2 \pmod{3}$ which is a contradiction.

Just to make sure! Why does the same argument not apply to $3x \equiv 2 \pmod{7}$?

(c) $6x \equiv 3 \pmod{9}$ has solutions $x = 2$, $x = 5$, $x = 8$.

$6x = 3 + 9m$ is equivalent to $2x = 1 + 3m$ or $2x \equiv 1 \pmod{3}$. Which has solution $x \equiv 2 \pmod{3}$.

Theorem 88. Consider the linear congruence $ax \equiv b \pmod{n}$. Let $d = \gcd(a, n)$.

(a) The linear congruence has a solution if and only if $d|b$.

(b) If $d = 1$, then there is a unique solution modulo n.

(c) If $d|b$, then it has d different solutions modulo n.

(In fact, it has a unique solution modulo n/d.)

Proof.

(a) Finding x such that $ax \equiv b \pmod{n}$ is equivalent to finding x, y such that $ax + ny = b$.
The latter is a diophantine equation of the kind we studied earlier. In particular, we know that it has a solution if and only if $\gcd(a, n)$ divides b.

(b) If $d = 1$, then $ax + ny = b$ has general solution $x = x_0 + tn$, $y = y_0 - ta$ (where x_0, y_0 is some particular solution). But, modulo n, all of these lead to the same solution $x \equiv x_0 \pmod{n}$.

(c) If $d|b$, then $ax \equiv b \pmod{n}$ is equivalent to $a_1 x \equiv b_1 \pmod{n_1}$ with $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $n_1 = \frac{n}{d}$. Since $\gcd(a_1, n_1) = 1$, we get a unique solution x modulo n_1.
Being congruent to x modulo n_1 is the same as being congruent to one of $x, x + n_1, \ldots, x + (d-1)n_1$ modulo n. □

Example 89. Solve $4x \equiv 1 \pmod{5}$.

Brute force solution. We can try the values $0, 1, 2, 3, 4$ and find that $x = 4$ is the only solution modulo 5.
This approach is fine for small examples when working by hand, but is not practical for serious congruences.

Solution. $4x \equiv 1 \pmod{5}$ is equivalent to $4x + 5y = 1$. This is a diophantine equation!
Since $\gcd(4, 5)$, Bézout's identity guarantees x, y such that $4x + 5y = 1$.
Indeed, $4 \cdot 4 + 5 \cdot (-3) = 1$. Modulo 5, this reduces to $4 \cdot 4 \equiv 1 \pmod{5}$.
Hence, $x \equiv 4 \pmod{5}$.

In other words, we have found the **modular inverse** of 4 modulo 5! We write $4^{-1} \equiv 4 \pmod{5}$.
(It is not surprising that 4 is its own inverse, if we realize that $4 \equiv -1 \pmod{5}$.)
Note that a has a modular inverse modulo n if and only if $\gcd(a, n) = 1$.

Armin Straub
straub@southalabama.edu

Example 90. Solve $16x \equiv 4 \pmod{25}$.

Solution.

- We first solve $16x \equiv 1 \pmod{25}$ to find $16^{-1} \pmod{25}$.
  We use the extended euclidean algorithm: $\underbrace{\gcd(16,25)}_{25=1\cdot 16+9} = \underbrace{\gcd(9,16)}_{16=2\cdot 9-2} = \underbrace{\gcd(-2,9)}_{9=(-4)\cdot(-2)+1} = \gcd(1,-2) = 1$
  Hence, Bézout's identity takes the form $1 = 9 + 4\cdot \underbrace{(-2)}_{-2=16-2\cdot 9} = -7\cdot \underbrace{9}_{9=25-16} + 4\cdot 16 = -7\cdot 25 + 11\cdot 16$.
  Reducing $-7\cdot 25 + 11\cdot 16$ modulo 25, we get $11\cdot 16 \equiv 1 \pmod{25}$.
  Hence, $16^{-1} \equiv 11 \pmod{25}$.
- It follows that $16x \equiv 4 \pmod{25}$ has the (unique) solution $x \equiv 11\cdot 4 \equiv 19 \pmod{25}$.

5.3 Chinese remainder theorem

Example 91. Solve $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$.

Brute force solution. If x is a solution, then so is $x + 35$. So we only look for solutions modulo 35.
Since $x \equiv 4 \pmod 7$, the only candidates for solutions are $4, 11, 18, \ldots$ Among these, we find $x = 32$.
[We can also focus on $x \equiv 2 \pmod 5$ and consider the candidates $2, 7, 12, \ldots$, but that is more work.]
This brute force solution is fine for small examples like this one. It is too slow to be used for large problems.

Solution. Let us break the problem into two pieces:

- $x \equiv 1 \pmod 5$, $x \equiv 0 \pmod 7$.
  By the second congruence, $x = 7z$.
  We thus solve $7z \equiv 1 \pmod 5$ and find $z = 3$. Hence, $x = 7\cdot 3 = 21$ does the trick.
- $x \equiv 0 \pmod 5$, $x \equiv 1 \pmod 7$.
  By the first congruence, $x = 5z$.
  We thus solve $5z \equiv 1 \pmod 7$ and find $z = 3$. Hence, $x = 5\cdot 3 = 15$ does the trick.

Combining these two, $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$ has solution $2\cdot 21 + 4\cdot 15 = 102 \equiv 32 \pmod{35}$.
[Make sure you see why we are combining the two pieces the way we do! It's a simple idea.]

Theorem 92. (Chinese Remainder Theorem) Let $n_1, n_2, \ldots, n_r$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad \ldots, \quad x \equiv a_n \pmod{n_r}$$

has a simultaneous solution, which is unique modulo $n = n_1 \cdots n_r$.

Armin Straub
straub@southalabama.edu