Sketch of Lecture 6

Tue, 9/11/2018

4.1 Congruences: modular inverses

Review. Last time, we saw that $ac \equiv bc \pmod{n}$ does not always imply $a \equiv b \pmod{n}$.

For instance, $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$ but $4 \not\equiv 1 \pmod{6}$.

The reason is that 2 is not invertible modulo 6.

The issue is that $2|6$ which results in $2 \cdot 3 \equiv 0 \pmod{6}$.

Let us briefly discuss residues that are invertible modulo n.

Example 46. Note that $3 \cdot 7 \equiv 1 \pmod{10}$. Hence, we write $3^{-1} \equiv 7 \pmod{10}$ and say that 7 is the **modular inverse** of 3 modulo 10.

Comment. As expected, we have $(x^{-1})^{-1} \equiv x \pmod{n}$. Here, $(3^{-1})^{-1} \equiv 7^{-1} \equiv 3 \pmod{10}$.

Example 47. Determine $4^{-1} \pmod{13}$.

Brute force solution. We need to find a residue x such that $4x \equiv 1 \pmod{13}$. We can try the values $0, 1, 2, 3, \ldots, 12$ and find that $x = 10$ is the only solution modulo 13 (because $4 \cdot 10 \equiv 1 \pmod{13}$).

This approach may be fine for small examples when working by hand, but is not practical for serious congruences. On the other hand, the Euclidean algorithm, reviewed below, can compute modular inverses extremely efficiently.

Glancing. In this special case, we can actually see the solution if we notice that $4 \cdot 3 = 12$, so that $4 \cdot 3 \equiv -1 \pmod{13}$ and therefore $4^{-1} \equiv -3 \pmod{13}$. [Or, equivalently, $-4^{-1} \equiv 10 \pmod{13}$.]

Solution. Since $\gcd(4, 13) = 1$, Bézout's identity promises that $4r + 13s = 1$ for some integers r, s. Reducing $4r + 13s = 1$ modulo 13, we find $4r \equiv 1 \pmod{13}$, so that $4^{-1} \equiv r \pmod{13}$.

Using the Euclidean algorithm, we find, for instance, $r = 10$ and $s = -3$. Hence, $4^{-1} \equiv 10 \pmod{13}$.

Example 48. Determine $16^{-1} \pmod{25}$.

Solution. Using the Euclidean algorithm, in Example 14, we found that $11 \cdot 16 - 7 \cdot 25 = 1$.

Reducing that modulo 25, we get $11 \cdot 16 \equiv 1 \pmod{25}$.

Hence, $16^{-1} \equiv 11 \pmod{25}$.

Let $a, b \in \mathbb{Z}$, not both zero. Recall that the diophantine equation $ax + by = c$ has a solution if and only if c is a multiple of $\gcd(a, b)$. In particular, $ax + by = 1$ has a solution if and only if $\gcd(a, b) = 1$.

Lemma 49. a is invertible modulo n if and only if $\gcd(a, n) = 1$.

Proof. The congruence $ax \equiv 1 \pmod{n}$ is equivalent to $ax + ny = 1$ where y is some integer. Note that $ax + mn = 1$ is a diophantine equation (we are looking for integer solutions x, y) and that it has a solution if and only if $\gcd(a, n) = 1$. □

Corollary 50. Let p be a prime. Then all nonzero residues are invertible modulo p.

Advanced comment. It is common to write $\mathbb{Z}/n\mathbb{Z}$ for the set of all residues modulo n. The fact that we can add an multiply as usual, makes $\mathbb{Z}/n\mathbb{Z}$ into a (finite) **ring**.

Let p be a prime. The fact that, in addition, all nonzero residues are invertible makes $\mathbb{Z}/p\mathbb{Z}$ into a (finite) **field**. The fields we are familiar with, such as $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers) are all infinite.

Example 51. List all invertible residues modulo 10.

Solution. $1, 3, 7, 9$

(We start with all residues $0, 1, 2, \ldots, 9$ and only keep those which have no common divisor with 10.)

4.2 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 52. Solve $4x \equiv 5 \pmod{13}$.

Solution. From an earlier problem, we know that $4^{-1} \equiv -3 \pmod{13}$.
Hence, $x \equiv 4^{-1} \cdot 5 \equiv -3 \cdot 5 = -2 \pmod{13}$.

Example 53.

(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 54. 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 a is invertible modulo n. Multiplying the congruence $ax \equiv b \pmod{n}$ with a^{-1}, we obtain $x \equiv a^{-1} b \pmod{n}$. That's the unique solution.
Alternatively. 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 $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $n_1 = \frac{n}{d}$. (Make sure you see why! Spell out the congruences as equalities.) 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. □