# Sketch of Lecture 1

Mon, 1/8/2018

## Review: The calculus of congruences

$$a \equiv b \pmod{n} \qquad \text{means} \qquad a = b + mn \quad (\text{for some } m \in \mathbb{Z})$$

In that case, we say that "$a$ is congruent to $b$ modulo $n$".

In other words: $a \equiv b \pmod{n}$ if and only if $a - b$ is divisible by $n$.

**Example 1.** $17 \equiv 5 \pmod{12}$ as well as $17 \equiv 29 \equiv -7 \pmod{12}$

We say that $5, 17, 29, -7$ all represent the same **residue** modulo $12$.
There are exactly $12$ different residues modulo $12$.

**Example 2.** Every integer $x$ is congruent to one of $0, 1, 2, 3, 4, \ldots, 11$ modulo $12$.

We therefore say that $0, 1, 2, 3, 4, \ldots, 11$ form a **complete set of residues** modulo $12$.

Another natural complete set of residues modulo $12$ is: $0, \pm 1, \pm 2, \ldots, \pm 5, 6$

[$-6$ is not included because $-6 \equiv 6$ modulo $12$.]

**Online homework.** When entering solutions modulo $n$ for online homework, your answer needs to be from one of the two natural sets of residues above.

**Example 3.** $67 \cdot 24 \equiv 4 \cdot 3 \equiv 5 \pmod{7}$

The point being that we can (and should!) reduce the factors individually first (to avoid the large number we would get when actually computing $67 \cdot 24$ first). This idea is crucial in the computations we (better, our computers) will later do for cryptography.

**Example 4. (but careful!)** If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$ for any integer $c$.

However, the converse is not true! We can have $ac \equiv bc \pmod{n}$ without $a \equiv b \pmod{n}$ (even assuming that $c \not\equiv 0$).

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

**However.** $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$ means $2 \cdot 4 = 2 \cdot 1 + 6m$. Hence, $4 = 1 + 3m$, or, $4 \equiv 1 \ (\operatorname{mod} 3)$.

The issue is that $2$ is not invertible modulo $6$.

$a$ is invertible modulo $n$ $\iff$ $\gcd(a, n) = 1$

Similarly, $ab \equiv 0 \ (\operatorname{mod} n)$ does not always imply that $a \equiv 0 \ (\operatorname{mod} n)$ or $b \equiv 0 \ (\operatorname{mod} n)$.

**For instance.** $4 \cdot 15 \equiv 0 \pmod{6}$ but $4 \not\equiv 0 \pmod{6}$ and $15 \not\equiv 0 \pmod{6}$

**Good news.** These issues do not occur when $n$ is a **prime** $p$.

- If $ab \equiv 0 \ (\operatorname{mod} p)$, then $a \equiv 0 \ (\operatorname{mod} p)$ or $b \equiv 0 \ (\operatorname{mod} p)$.
- Suppose $c \not\equiv 0 \pmod{p}$. If $ac \equiv bc \pmod{p}$, then $a \equiv b \pmod{p}$.

**Example 5.** Determine $4^{-1} \pmod{13}$.

**Recall.** This is asking for the **modular inverse** of $4$ modulo $13$. That is, a residue $x$ such that $4x \equiv 1 \pmod{13}$.

**Brute force solution.** 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 $4^{-1} \equiv -3 \pmod{13}$.

**Example 6.** Solve $4x \equiv 5 \pmod{13}$.

**Solution.** From the previous problem, we know that $4^{-1} \equiv -3 \pmod{13}$.

Hence, $x \equiv 4^{-1} \cdot 5 \equiv -3 \cdot 5 = -2 \pmod{13}$.

**(Bézout's identity)** Let $a, b \in \mathbb{Z}$ (not both zero). There exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by.$$

The integers $x, y$ can be found using the **extended Euclidean algorithm**.

In particular, if $\gcd(a, b) = 1$, then $a^{-1} \equiv x \pmod{b}$.

Here, $\mathbb{Z}$ denotes the set of all integers $0, \pm 1, \pm 2, \ldots$

**Example 7.** Determine $16^{-1} \pmod{25}$.

**Solution.** We determine $16^{-1} \pmod{25}$ using the extended Euclidean algorithm:

$$\begin{array}{lll}
\gcd(16, 25) & \boxed{25} = 1 \cdot \boxed{16} + 9 & \text{or:} \quad \boxed{A} \quad 9 = 1 \cdot \boxed{25} - 1 \cdot \boxed{16} \\
= \gcd(9, 16) & \boxed{16} = 2 \cdot \boxed{9} - 2 & \qquad\;\; \boxed{B} \quad 2 = -1 \cdot \boxed{16} + 2 \cdot \boxed{9} \\
= \gcd(2, 9) & \boxed{9} = 4 \cdot \boxed{2} + 1 & \qquad\;\; \boxed{C} \quad 1 = \boxed{9} - 4 \cdot \boxed{2} \\
= 1 & &
\end{array}$$

Backtracking through this, we find that **Bézout's identity** takes the form

$$1 \underset{\boxed{C}}{=} \boxed{9} - 4 \cdot \boxed{2} \underset{\boxed{B}}{=} 4 \cdot \boxed{16} - 7 \cdot \boxed{9} \underset{\boxed{A}}{=} -7 \cdot \boxed{25} + 11 \cdot \boxed{16}$$

Reducing $-7 \cdot 25 + 11 \cdot 16 = 1$ modulo $25$, we get $11 \cdot 16 \equiv 1 \pmod{25}$.

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

**Course comment:**

Homework is posted after every class to our course website.

Today's homework needs to be submitted online before 1/17.