Sketch of Lecture 1

Mon, 1/9/2017

1 Review

1.1 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 $0, 1, 2, 3, 4$ modulo 5.
We therefore say that $0, 1, 2, 3, 4$ form a **complete set of residues** modulo 5.
Another natural complete set of residues modulo 5 is: $0, \pm 1, \pm 2$
A not so natural complete set of residues modulo 5 is: $-5, 2, 4, 8, 16$

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

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, $4 \equiv 1 \pmod{3}$.
The issue is that 2 is not invertible modulo 6.

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

Similarly, $ab \equiv 0 \pmod{n}$ does not always imply that $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.

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

Example 5. Solve $3x \equiv 2 \pmod{5}$.

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 may be fine for small examples when working by hand, but is not practical for serious congruences.

Solution. We first determine the **modular inverse** of 3 modulo 5. This is $3^{-1} \equiv 2 \pmod{5}$ since $3 \cdot 2 \equiv 1 \pmod{5}$. Hence, $x \equiv 3^{-1} \cdot 2 \equiv 2 \cdot 2 = 4 \pmod{5}$.

Armin Straub
straub@southalabama.edu

(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 6. Solve $16x \equiv 3 \pmod{25}$.

Solution.

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

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

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

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

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

- It follows that $16x \equiv 3 \pmod{25}$ has the (unique) solution $x \equiv 11 \cdot 3 \equiv 8 \pmod{25}$.

Example 7. (homework) Find the modular inverse of 17 modulo 23.

Solution. The final answer is $17^{-1} \equiv -4 \pmod{23}$.