Lecture 5: Congruences

William Stein

Math 124 Harvard University **Fall 2001**

The point of this lecture:
Define the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. Prove Fermat's little theorem, which asserts that if $\gcd(x, n) = 1$, then $x^{\varphi(n)} \equiv 1 \pmod{n}$.

1 Notation

Definition 1.1 (Congruence). Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then

$$a \equiv b \pmod{n}$$

if $n \mid a - b$.

That is, there is $c \in \mathbb{Z}$ such that

$$nc = a - b.$$

One way I think about it: a is congruent to b modulo n, if we can get from b to a by adding multiples of n.

Congruence modulo n is an *equivalence relation.* Let

$$\mathbb{Z}/n\mathbb{Z} = \{ \text{ the set of equivalence classes } \}$$

The set $\mathbb{Z}/n\mathbb{Z}$ is a *ring*, the "ring of integers modulo n". It is the quotient of the ring $\mathbb{Z}$ by the ideal generated by n.

Example 1.2.

$$\mathbb{Z}/3\mathbb{Z} = \{\{\ldots, -3, 0, 3, \ldots\}, \{\ldots, -2, 1, 4, \ldots\}, \{\ldots, -1, 2, 5, \ldots\}\} = \{[0], [1], [2]\}$$

where we let $[a]$ denote the equivalence class of a.

2 Arithmetic Modulo N

Suppose a, $a', b\, b' \in \mathbb{Z}$ and

$$a \equiv a' \pmod{n}, \qquad b \equiv b' \pmod{n}.$$

Then

$$a + b \equiv a' + b' \pmod{n} \tag{1}$$
$$a \times b \equiv a' \times b' \pmod{n} \tag{2}$$

So it makes sense to define $+$ and $\times$ by $[a] + [b] = [a + b]$ and $[a] \times [b] = [a \times b]$.

2.1 Cancellation

Proposition 2.1. *If* $\gcd(c, n) = 1$ *and*

$$ac \equiv bc \pmod{n}$$

then $a \equiv b \pmod{n}$.

Proof. By definition

$$n \mid ac - bc = (a - b)c.$$

Since $\gcd(n, c) = 1$, it follows that $n \mid a - b$, so

$$a \equiv b \pmod{n},$$

as claimed. □

2.2 Rules for Divisibility

Proposition 2.2. *A number* $n \in \mathbb{Z}$ *is divisible by* 3 *if and only if the sum of the digits of* n *is divisible by* 3.

Proof. Write

$$n = a + 10b + 100c + \cdots .$$

Since $10 \equiv 1 \pmod{3}$,

$$n = a + 10b + 100c + \cdots \equiv a + b + c + \cdots \pmod{3},$$

from which the proposition follows. □

Similarly, you can find rules for divisibility by 5, 9 and 11. What about divisibility by 7?

3 Linear Congruences

Definition 3.1 (Complete Set of Residues). A *complete set of residues* modulo n is a subset $R \subset \mathbb{Z}$ of size n whose reductions modulo n are distinct. In other words, a complete set of residues is a choice of representive for each equivalence class in $\mathbb{Z}/n\mathbb{Z}$.

Some examples:

$$R = \{0, 1, 2, \ldots, n - 1\}$$

is a complete set of residues modulo n. When $n = 5$, a complete set of residues is

$$R = \{0, 1, -1, 2, -2\}.$$

Lemma 3.2. *If* R *is a complete set of residues modulo* n *and* $a \in \mathbb{Z}$ *with* $\gcd(a, n) = 1$, *then* $aR = \{ax : x \in R\}$ *is also a complete set of residues.*

Proof. If $ax \equiv ax' \pmod{n}$ with $x, x' \in R$, then Proposition 2.1 implies that $x \equiv x' \pmod{n}$. Because R is a complete set of residues, this implies that $x = x'$. Thus the elements of aR have distinct reductions modulo n. It follows, since $\#aR = n$, that aR is a complete set of residues modulo n. $\square$

Definition 3.3 (Linear Congruence). A *linear congruence* is an equation of the form
$$ax \equiv b \pmod{n}.$$

Proposition 3.4. *If* $\gcd(a, n) = 1$*, then the equation*
$$ax \equiv b \pmod{n}$$
must have a solution.

Proof. Let R be a complete set of residues modulo n (for example, $R = \{0, 1, \ldots, n-1\}$). Then by Lemma 3.2, aR is also a complete set of residues. Thus there is an element $ax \in aR$ such that $ax \equiv b \pmod{n}$, which proves the proposition. $\square$

The point in the proof is that left multiplication by a defines a map $\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, which must be surjective because $\mathbb{Z}/n\mathbb{Z}$ is finite.

Illustration:
$$2x \equiv 3 \pmod{7}$$
Set $R = \{0, 1, 2, 3, 4, 5, 6\}$. Then
$$2R = \{0, 2, 4, 6, 8 \equiv 1, 10 \equiv 3, 12 \equiv 5\},$$
so $2 \cdot 5 \equiv 3 \pmod{7}$.

Warning:
Note that the equation $ax \equiv b \pmod{n}$ might have a solution even if $\gcd(a, n) \neq 1$. To construct such examples, let a be any divisor of n, x any number, and set $b = ax$. For example, $2x \equiv 6 \pmod{8}$ has a solution!

4 Fermat's Little Theorem

Definition 4.1 (Order). Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ with $\gcd(x, n) = 1$. The *order* of x modulo n is the smallest $m \in \mathbb{N}$ such that
$$x^m \equiv 1 \pmod{n}.$$

We must show that this definition makes sense. To do so, we verify that such an m exists. Consider $x, x^2, x^3, \ldots$ modulo n. There are only finitely many residue classes modulo n, so we must eventually find two integers i, j with $i < j$ such that
$$x^i \equiv x^j \pmod{n}.$$
Since $\gcd(x, n) = 1$, Proposition 2.1 implies that we can cancel x's and conclude that
$$x^{j-i} \equiv 1 \pmod{n}.$$

Definition 4.2 (Euler Phi function). Let

$$\varphi(n) = \#\{a \in \mathbb{N} : a \leq n \text{ and } \gcd(a,n) = 1\}.$$

For example,

$$\begin{aligned}\varphi(1) &= \#\{1\} = 1,\\ \varphi(5) &= \#\{1,2,3,4\} = 4,\\ \varphi(12) &= \#\{1,5,7,11\} = 4.\end{aligned}$$

If p is any prime number then

$$\varphi(p) = \#\{1,2,\ldots,p-1\} = p-1.$$

Theorem 4.3 (Fermat's Little Theorem). *If* $\gcd(x,n) = 1$*, then*

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. Let

$$P = \{a : 1 \leq a \leq n \text{ and } \gcd(a,n) = 1\}.$$

In the same way that we proved Lemma 3.2, we see that the reductions modulo n of the elements of xP are exactly the same as the reductions of the elements of P. Thus

$$\prod_{a\in P}(xa) = \prod_{a \in P} a \pmod{n},$$

since the products are over exactly the same numbers modulo n. Now cancel the a's on both sides to get

$$x^{\#P} \equiv 1 \pmod{n},$$

as claimed. □

4.1 Group-theoretic Interpretation

The set of invertible elements of $\mathbb{Z}/n\mathbb{Z}$ is a group

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}.$$

This group has order $\varphi(n)$. Theorem 4.3 asserts that the order of an element of $(\mathbb{Z}/n\mathbb{Z})^\times$ divides the order $\varphi(n)$ of $(\mathbb{Z}/n\mathbb{Z})^\times$. This is a special case of the more general theorem that if G is a finite group and $g \in G$, then the order of g divide $\#G$.

5 What happened?

Take out a piece of paper and answer the following two questions:

1. What is a central idea that you learned in this lecture?

2. What part of this lecture did you find murky?