Lecture 14: Review for Midterm

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

Today I will briefly describe some key ideas that we've covered in this course up until now. Make sure you understand these, so you can do well on the midterm, which is Wednesday, October 17, and is worth 20% of your grade.

1 Some Basic Definitions

Greatest common divisor:

$$\gcd(a,b) = \max\{d : d \mid a \text{ and } d \mid b\}$$

Congruence: $a \equiv b \pmod{n}$ means that $n \mid a - b$.

Example 1.1. We have $7 \equiv -19 \pmod{13}$ since $13 \mid 7 - (-19) = 26$.

If a is an integer such that $\gcd(a,n) = 1$, then the order of a modulo n is

$$\min\left\{i \in \mathbb{N} : a^i \equiv 1 \pmod{n}\right\}.$$

For example, the order of 2 modulo 15 is 4.

Some Rings and Groups: We let $\mathbb{Z}/n\mathbb{Z}$ denote the ring of equivalence classes of integers modulo n. We also frequently consider the group

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a : 1 \le a \le n \text{ and } \gcd(a,n) = 1\}.$$

The order of a modulo n is then the order of the image of a in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$.

2 Equations Modulo n

2.1 Linear Equations

The equation $ax \equiv b \pmod{n}$ must have a solution if $\gcd(a,n) = 1$. *Warning:* It might still have a solution even if $\gcd(a,n) \neq 1$.

Example 2.1. The equation $3x \equiv 2 \pmod{5}$ has the solution $x = 4$.
The equation $3x \equiv 9 \pmod{18}$ has a solution $x = 3$ even though $\gcd(3,18) = 3 \neq 1$.

2.2 Quadratic Equations

Suppose a is an integer that is not divisible by p. The solvability or nonsolvability of the quadratic equation $x^2 \equiv a \pmod{p}$ is addressed by quadratic reciprocity. (So far we have not discussed how to find a solution, only whether or not one exists.) The quadratic residue symbol is

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{otherwise.} \end{cases}$$

We have

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

The **Quadratic Reciprocity Law**, which was proved by Gauss, asserts that if p and q are distinct odd primes then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

This is the deepest result that we've proved in the course so far. On the midterm, you will *not* be held responsible for understanding the proof I gave last Friday. However, you should know the statement of the quadratic reciprocity law and have some practice applying it.

3 Systems of Equations

Suppose that n and m are coprime integers. Then the **Chinese Remainder Theorem** (CRT) asserts that the system of equations

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n} \end{aligned}$$

has solutions. (There is exactly one nonnegative solution $x < nm$.)

Example 3.1. Because of CRT, I know that there is an x such that

$$\begin{aligned} x &\equiv 1 \pmod{37}, \\ x &\equiv 17 \pmod{23} \end{aligned}$$

even though I am too lazy to find x right now.

4 The Euler φ Function

Define a function $\varphi : \mathbb{N} \to \mathbb{N}$ by

$$\varphi(n) = \#\{a : 1 \leq a \leq n \text{ and } \gcd(a,n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^*.$$

Using the Chinese Remainder Theorem we proved that φ is a *multiplicative function*, i.e., if $m, n \in \mathbb{N}$ and $\gcd(m,n) = 1$, then

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Also, if p is a prime then $\varphi(p^n) = p^n - \frac{p^n}{p} = p^n - p^{n-1}$.

Example 4.1.

$$\varphi(2^3 \cdot 5^2) = \varphi(2^3) \cdot \varphi(5^2) = (2^3 - 2^2) \cdot (5^2 - 5) = 4 \cdot 20 = 80.$$

5 Public-key Cryptography

5.1 The Diffie-Hellman Key Exchange

1. Nikita chooses a prime p and a number g that is a primitive root modulo p. She tells Michael both p and g.

2. Nikita secretely chooses a random number n and sends Michael $g^n \pmod{p}$.

3. Michael secretely chooses a random number m and sends Nikita $g^m \pmod{p}$.

4. The *secret key* is $s = g^{nm} \pmod{p}$. Both Michael and Nikita can easily compute s, but The Collective can't because of the difficulty of the "discrete logarithm problem".

5.2 The RSA Cryptosystem

1. Nikita creates her public key as follows:

   (a) She chooses two distinct large primes p and q, then computes both $n = pq$ and $\varphi(n) = (p-1)(q-1)$.

   (b) She picks a random natural number $e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$.

   (c) She computes a number d such that $ed \equiv 1 \pmod{\varphi(n)}$.

   (d) Her public key is (n, e). (And her private decoding key is d.)

2. To send Nikita a message, Michael encodes it (or a piece of it) as a number $m \pmod{n}$. He then sends $m^e \pmod{n}$ to Nikita.

3. Nikita recovers m from $m^e \pmod{n}$ by using that

$$m \equiv (m^e)^d \pmod{n}.$$

6 Important Algorithms

6.1 Euclid's Algorithm

Given integers a and b, a slight extension of Euclid's gcd algorithm enables us to find integers x and y such that

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

Example 6.1. $a = 12$, $b = 101$.

$$\begin{aligned} \underline{101} &= 8 \cdot \underline{12} + \underline{5} & \qquad \underline{5} &= \underline{101} - 8 \cdot \underline{12} \\ \underline{12} &= 2 \cdot \underline{5} + \underline{2} & \underline{2} &= -2 \cdot \underline{101} + 17 \cdot \underline{12} \\ \underline{5} &= 2 \cdot \underline{2} + \underline{1} & \underline{1} &= \underline{5} - 2 \cdot \underline{2} = 5 \cdot \underline{101} - 42 \cdot \underline{12}. \end{aligned}$$

Thus $x = -42$, $y = 5$ works, and $\gcd(a, b) = 1$.

We can use the result of this computation to solve

$$12x \equiv 1 \pmod{101}.$$

Indeed, $1 = (-42) \cdot 12 + 5 \cdot 101$, so $x = -42$ is a solution.

6.2 Powering Algorithm

There is a clever trick that makes computing a^n easier. Write n in binary, that is is write $n = \sum_{i=0}^{r} \varepsilon_i 2^i$ with $\varepsilon_i \in \{0, 1\}$. Then

$$a^n = \prod_{i \text{ with } \varepsilon_i \neq 0} a^{2^i}.$$

6.3 PARI

The midterm will **NOT** test knowledge of PARI.