Introduction to Cryptography
CS 355
Lecture 3

Elementary Number Theory (1)

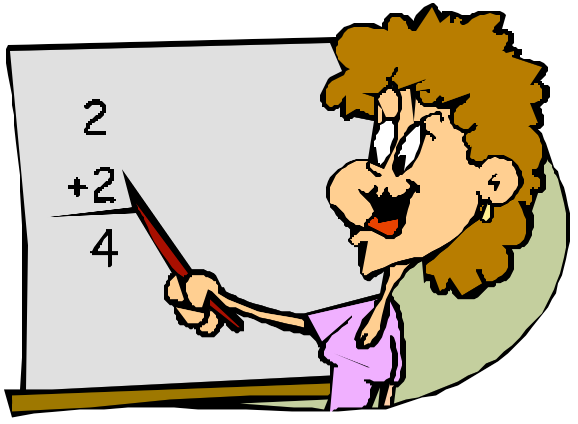
Review of Last Lecture

- **Ciphertext-only attack**:
- **Known-plaintext attack:**
- **Chosen-plaintext:**
- **Chosen-ciphertext:**
- Transposition cipher: Scytale
- Substitution cipher:
  - Shift cipher
  - general mono-alphabetical substitution cipher

Lecture Outline

- Divisibility
- Prime and composite numbers
- The Fundamental theorem of arithmetic
- Great Common Divisor
- Modular operation
- Congruence relation

Begin Math



Divisibility

Definition

Given integers a and b, with a $\neq$ 0, a divides b (denoted a|b) if $\exists$ integer k, s.t. b = ak.

a is called a **divisor** of b, and b a **multiple** of a.

Proposition:

(1) If a $\neq$ 0, then a|0 and a|a. Also, 1|b for every b

(2) If a|b and b|c, then a | c.

(3) If a|b and a|c, then a | (sb + tc) for all integers s and t.

Divisibility (cont.)

Theorem (Division algorithm)
Given integers a, b such that $a>0$, $a<b$ then there exist two unique integers q and r, $0 \leq r < a$ s.t. $b = aq + r$.

Proof:
Uniqueness of q and r:
assume $\exists$ q' and r' s.t $b = aq' + r'$, $0 \leq r' < a$, q' integer
then $aq + r = aq' + r' \Rightarrow a(q-q') = r'-r \Rightarrow q-q' = (r'-r)/a$
as $0 \leq r, r' < a \Rightarrow -a < (r'-r) < a \Rightarrow -1 < (r'-r)/a < 1$
So $-1 < q-q' < 1$, but q-q' is integer, therefore
$q = q'$ and $r = r'$

Prime and Composite Numbers

Definition
An integer $n > 1$ is called a prime number if its positive divisors are 1 and n.

Definition
Any integer number $n > 1$ that is not prime, is called a composite number.

Example
Prime numbers: 2, 3, 5, 7, 11, 13, 17 …
Composite numbers: 4, 6, 25, 900, 17778, …

Decomposition in Product of Primes

Theorem (Fundamental Theorem of Arithmetic)
Any integer number n > 1 can be written as a product of prime numbers (>1), and the product is unique if the numbers are written in increasing order.

$$n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$$

Example: $84 = 2^2 \bullet 3 \bullet 7$

Classroom Discussion Question (Not a Quiz)

- Are the total number of prime numbers finite or infinite?

Greatest Common Divisor (GCD)

Definition

Given integers $a > 0$ and $b > 0$, we define $gcd(a, b) = c$, the greatest common divisor (GCD), as the greatest number that divides both a and b.

Example

$gcd(256, 100)=4$

Definition

Two integers $a > 0$ and $b > 0$ are relatively prime if $gcd(a, b) = 1$.

Example

25 and 128 are relatively prime.

GCD as a Linear Combination

Theorem
Given integers a, b > 0 and a > b, then d = gcd(a,b) is the least positive integer that can be represented as ax + by, x, y integer numbers.

Proof: Let t be the smallest positive integer s.t. t = ax + by.
We have $d \mid a$ and $d \mid b \Rightarrow d \mid ax + by$, so $d \mid t$, so $d \leq t$.
We now show t = d.
First $t \mid a$; otherwise, a = tu + r, 0 < r < t;
r = a - ut = a - u(ax+by) = a(1-ux) + b(-uy), so we found another linear combination and r < t. Contradiction.
Similarly $t \mid b$, so t is a common divisor of a and b, thus
t = gcd (a, b) = d. So t = d.

Example

gcd(100, 36) = 4 **=** $4 \times 100 - 11 \times 36 = 400 - 396$

GCD and Multiplication

Theorem

Given integers a, b, m >1. If

gcd(a, m) = gcd(b, m) = 1, then gcd(ab, m) = 1

Proof idea:

$ax + ym = 1 = bz + tm$

Find u and v such that $(ab)u + mv = 1$

GCD and Division

Theorem

Given integers $a>0$, b, q, r, such that $b = aq + r$, then $\gcd(b, a) = \gcd(a, r)$.

Proof:

Let $\gcd(b, a) = d$ and $\gcd(a, r) = e$, this means

$d \mid b$ and $d \mid a$, so $d \mid b - aq$, so $d \mid r$
Since $\gcd(a, r) = e$, we obtain $d = e$.

$e \mid a$ and $e \mid r$, so $e \mid aq + r$, so $e \mid b$,
Since $\gcd(b, a) = d$, we obtain $e = d$.

Therefore $d = e$

Finding GCD

Using the Theorem: Given integers a>0, b, q, r, such that b = aq + r, then gcd(b, a) = gcd(a, r).

Euclidian Algorithm

Find gcd (b, a)

while $a \neq 0$ *do*

$r \leftarrow b \bmod a$

$b \leftarrow a$

$a \leftarrow r$

return a

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.

Euclidian Algorithm Example

Find gcd(143, 110)

$$
\begin{aligned}
143 &= 1 \times 110 + 33 \\
110 &= 3 \times 33 + 11 \\
33 &= 3 \times 11 + 0
\end{aligned}
$$

gcd (143, 110) = 11

Modulo Operation

Definition:

$$a \bmod n = r \Leftrightarrow \exists q, \text{s.t. } a = q \times n + r$$

$$\text{where } 0 \le r \le n-1$$

Example:

7 mod 3 = 1

-7 mod 3 = 2

Definition (Congruence):

$$a \equiv b \bmod n \Leftrightarrow a \bmod n = b \bmod n$$

Equivalence Relation

Definition

A binary relation R over a set X is a subset of X\times X. We denote a relation $(a,b) \in R$ as aRb.

•example of relations over integers?

Definition

A relation is an equivalence relation on a set X, if R is

Reflexive: aRa for all $a \in R$

Symmetric: for all $a, b \in R$, $aRb \Rightarrow bRa$.

Transitive: for all $a,b,c \in R$, aRb and $bRc \Rightarrow aRc$

Example

"=" is an equivalence relation on the set of integers

Congruence Relation

Theorem

Congruence mod n is an equivalence relation:

Reflexive: $a \equiv a \pmod{n}$

Symmetric: $a \equiv b \pmod{n}$ iff $b \equiv a \bmod n$.

Transitive: $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow$
$a \equiv c \pmod{n}$

Congruence Relation Properties

Theorem

1) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

   $a \pm c \equiv b \pm d \pmod{n}$ and

   $ac \equiv bd \pmod{n}$

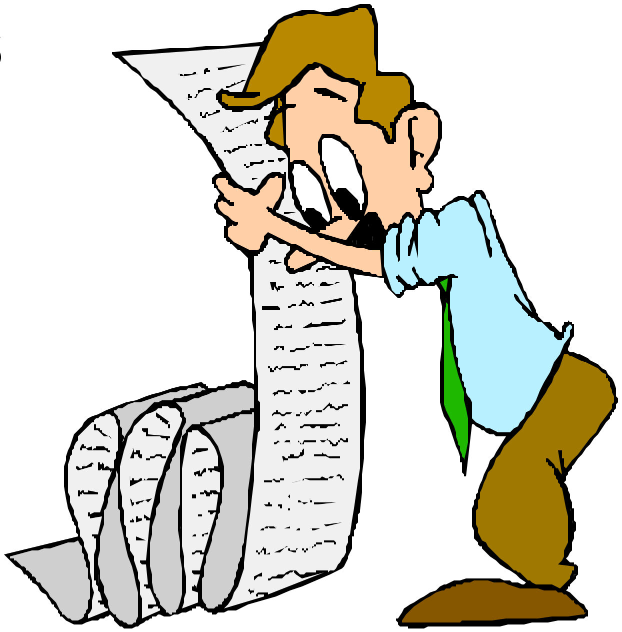
2) If $a \equiv b \pmod{n}$ and $d \mid n$ then:

   $a \equiv b \pmod{d}$

End Math

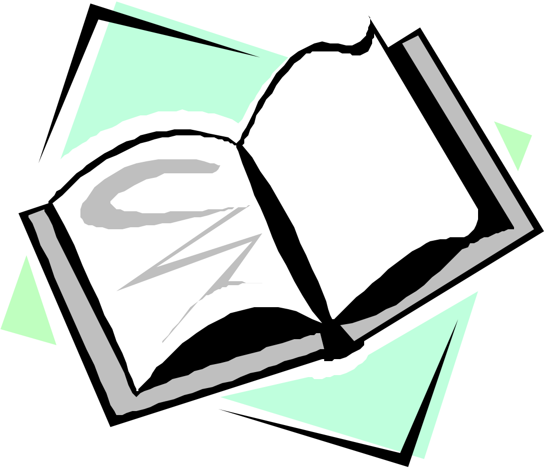
Summary

- Divisibility
- Prime and composite numbers
- The Fundamental theorem of arithmetic
- Great Common Divisor
- Modular operation
- Congruence relation



Recommended Reading for This Lecture

- Trappe & Washington:
  - 3.1, 3.3



Coming Attractions …

- The Vigenère Cipher

- Recommended reading for next lecture:
  - The Codebook Chapter 2
  - Trappe & Washington: 2.3