CS 5319
Advanced Discrete Structure

Lecture 9:
Introduction to Number Theory II

Outline

- Divisibility
- Greatest Common Divisor
- Fundamental Theorem of Arithmetic
- Modular Arithmetic
- Euler Phi Function
- RSA Cryptosystem

Reference: Course Notes of MIT 6.042J (Fall 05)
by Prof. Meyer and Prof. Rubinfeld

Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic

Theorem 3:

Any positive integer $n > 1$ can be written in a unique way as a product of primes :

$$n = p_1 p_2 \ldots p_j \qquad (p_1 \leq p_2 \leq \ldots \leq p_j)$$

The above theorem is called the fundamental theorem of arithmetic

Before we prove it, let us prove a useful lemma

Fundamental Theorem of Arithmetic

Lemma 3:

Let p be a prime.

(1) If $p \mid ab$, then $p \mid a$ or $p \mid b$

(2) If $p \mid a_1 a_2 \ldots a_n$, then p divides some a_i

Proof of (1): $\gcd(a, p)$ must be either 1 or p (why?)

If $\gcd(a, p) = p$, then the claim holds.

Else $\gcd(a, p) = 1$, so $p \mid b$ by Lemma 2 (part (4)).

Proof of (2): By induction

Proof of the Fundamental Theorem

- First, we prove (by strong induction) that all n can be written as a product of primes.
  - Base case: $n = 2$ is a prime.
  - Inductive case: Assume all $k < n$ can be written as product of primes. If n is a prime, then the statement is true. Else, $n = a\,b$ for some $a, b < n$. Then by the induction assumption, a and b can both be written as product of primes, which implies that $n = a \cdot b$ can be as well.

Proof of the Fundamental Theorem

- Next, we prove (by contradiction) that all *n* can be written as a product of primes in a *unique* way.
  - Suppose the statement is not true
  - Let *n* be the smallest integer that can be written as product of primes in more than one way
  - Let
$$\begin{aligned} n &= p_1\, p_2 \ldots p_j \\ &= q_1\, q_2 \ldots q_k \end{aligned}$$
    be two of the (possibly many) ways to write *n* as a product of primes

Proof of the Fundamental Theorem

- Proof (cont) :
  - Then $p_1 \mid n$ so that p_1 divides some q_i
  - Since q_i is a prime, we must have $p_1 = q_i$
  - Now we delete p_1 from the first product, and q_i from the second product, we find that n / p_1 is a positive integer *smaller* than n and can be written as product of primes in more than one way ➔ Contradiction occurs, proof completes

Modular Arithmetic

Modular Arithemetic

- Gauss introduced the notion of congruence in his book *Disquisitiones Arithmeticae*

- We say a is congruent to b modulo n if $n \mid (a - b)$

- It is denoted by : $\boxed{a \equiv b \pmod{n}}$

- For instance,

$$29 \equiv 15 \pmod{7} \quad \text{because} \quad 7 \mid (29 - 15)$$

Facts About Congruence

Lemma 4:

Congruence modulo n is an equivalent relation.

That is :

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

Facts About Congruence

Lemma 5: (Congruence and Remainder)

1. $a \equiv (a \text{ rem } n) \quad (\text{mod } n)$
2. $a \equiv b \quad (\text{mod } n)$

   implies $(a \text{ rem } n) = (b \text{ rem } n)$

Proof of (2) : Let q_1 and q_2 be integers such that

$$(a \text{ rem } n) = a - q_1 n \quad \text{and} \quad (b \text{ rem } n) = b - q_2 n$$

Thus $(a \text{ rem } n) - (b \text{ rem } n)$

$= (a - b) + n\,(q_2 - q_1)$ is a multiple of n

Facts About Congruence

Lemma 6:

For all $n \geq 1$, the following statements hold.

1. $a \equiv b \pmod{n}$ implies $a + c \equiv b + c \pmod{n}$
2. $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$
3. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ implies $a + c \equiv b + d \pmod{n}$
4. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ implies $ac \equiv bd \pmod{n}$

Cancellation Law

- The previous statements show that under the same modulo, we can validly perform addition, subtraction, and multiplication of congruences
- However, division may not be okay.

  For instance,

$$14 \equiv 4 \pmod{10} \quad \text{but} \quad 7 \not\equiv 2 \pmod{10}$$

- The theorem on the next page provides conditions where division is okay

Cancellation Law

Theorem 4:

If $bc \equiv bd \pmod{n}$ and $\gcd(b, n) = 1$,

then $c \equiv d \pmod{n}$

Proof :

Since $n \mid bc - bd$, and $\gcd(b, n) = 1$, we have

$n \mid c - d$ by Lemma 2 part (4)

Multiplicative Inverse

- In fact, the previous theorem can be proved in an alternative way :

  Since gcd(b, n) = 1, there exists b' such that

  $$b'b + qn = 1 \qquad \text{for some } q.$$

  Thus $b'b = 1 \pmod{n}$. The theorem follows by multiplying b' on both sides of the congruence
- The value b' is called the multiplicative inverse of b modulo n, and is usually denoted by b^{-1}

Cancellation Law

Corollary 1:

Suppose p is a prime and k is not a multiple of p. Then the sequence :

$(0 \cdot k)$ rem p, $(1 \cdot k)$ rem p, … , $((p–1) \cdot k)$ rem p

is a permutation of the sequence :

$$0, 1, 2, \ldots, p - 1$$

This remains true if the first term of each sequence is omitted

Cancellation Law

Proof : The first sequence contains p numbers, ranging from 0 to $p - 1$. Also, the numbers in the first sequence are distinct; otherwise, there exists distinct i and j ($i, j < p$) such that

$$(i \cdot k) \text{ rem } p = (j \cdot k) \text{ rem } p$$

$$\Rightarrow \quad i \cdot k \equiv j \cdot k \pmod{p} \quad \Rightarrow \quad i \equiv j \pmod{p}$$

which is impossible. Thus, the first sequence contains *all* numbers from 0 to $p - 1$. The claim is still true if first terms are omitted, as both are 0

Fermat's Little Theorem

Theorem 5:

Let p be a prime. Then for any integer a ,

$$a^p \equiv a \pmod{p}$$

Proof: If $p \mid a$, then $p \mid a^p - a$. Else, we have

$$(p-1)! \equiv (a \text{ rem } p)\,(2a \text{ rem } p)\,\ldots\,((p-1)a \text{ rem } p)$$

$$\equiv a^{p-1}\,(p-1)! \pmod{p}$$

The claim follows by multiplying the multiplicative inverse of $(p-1)!$ to both sides

Wilson's Theorem

Theorem 6:

The congruence

$$(m-1)! \equiv -1 \pmod{m}$$

is true if and only if m is a prime

Euler Phi Function

Euler Phi Function

- If $\gcd(a, b) = 1$, we say a is coprime to b
  (or we say a and b are relatively prime)
- Euler first studied the following function :

$$\boxed{\begin{array}{c}\varphi(n) = \text{\# of positive integers at most } n \\ \text{which are coprime to } n\end{array}}$$

- $\varphi(n)$ is called the Euler phi function
- For instance, $\varphi(1) = 1$, $\varphi(9) = 6$, $\varphi(10) = 4$

Fermat's Little Theorem (Revisited)

Corollary 2:

Suppose k is a positive integer coprime to n.
Let $k_1, k_2, \ldots, k_{\varphi(n)}$ denote all integers coprime to n, with $0 \le k_i < n$.

Then the sequence :

$$(k_1 \cdot k) \text{ rem } n,\ (k_2 \cdot k) \text{ rem } n,\ \ldots,\ (k_{\varphi(n)} \cdot k) \text{ rem } n$$

is a permutation of the sequence :

$$k_1, k_2, \ldots, k_{\varphi(n)}$$

Euler's Theorem

Theorem 7:

If gcd(k, n) = 1, then

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

Proof :

$$k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)}$$

$$\equiv (k_1\, k \text{ rem } n) \cdot (k_2\, k \text{ rem } n) \cdot \ldots \cdot (k_{\varphi(n)}\, k \text{ rem } n)$$

$$\equiv k^{\varphi(n)}\, k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)} \qquad \pmod{n}$$

Euler Phi Function

Theorem 8:

The φ function can be expressed as :

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Main Idea of Proof:

Induction on number of prime factors of *n*

Euler Phi Function

Proof :

Base Case: n has one prime factor

In that case, $n = q^k$ for some prime q and k

Then out of all numbers from 1 to q^k ,

exactly q^{k-1} of them are multiples of q

$$
\begin{aligned}
\Rightarrow \varphi(n) &= \varphi(q^k) \\
&= q^k - q^{k-1} \\
&= n\,(1 - 1/q)
\end{aligned}
$$

Euler Phi Function

Proof :

Inductive Case: n has j prime factors

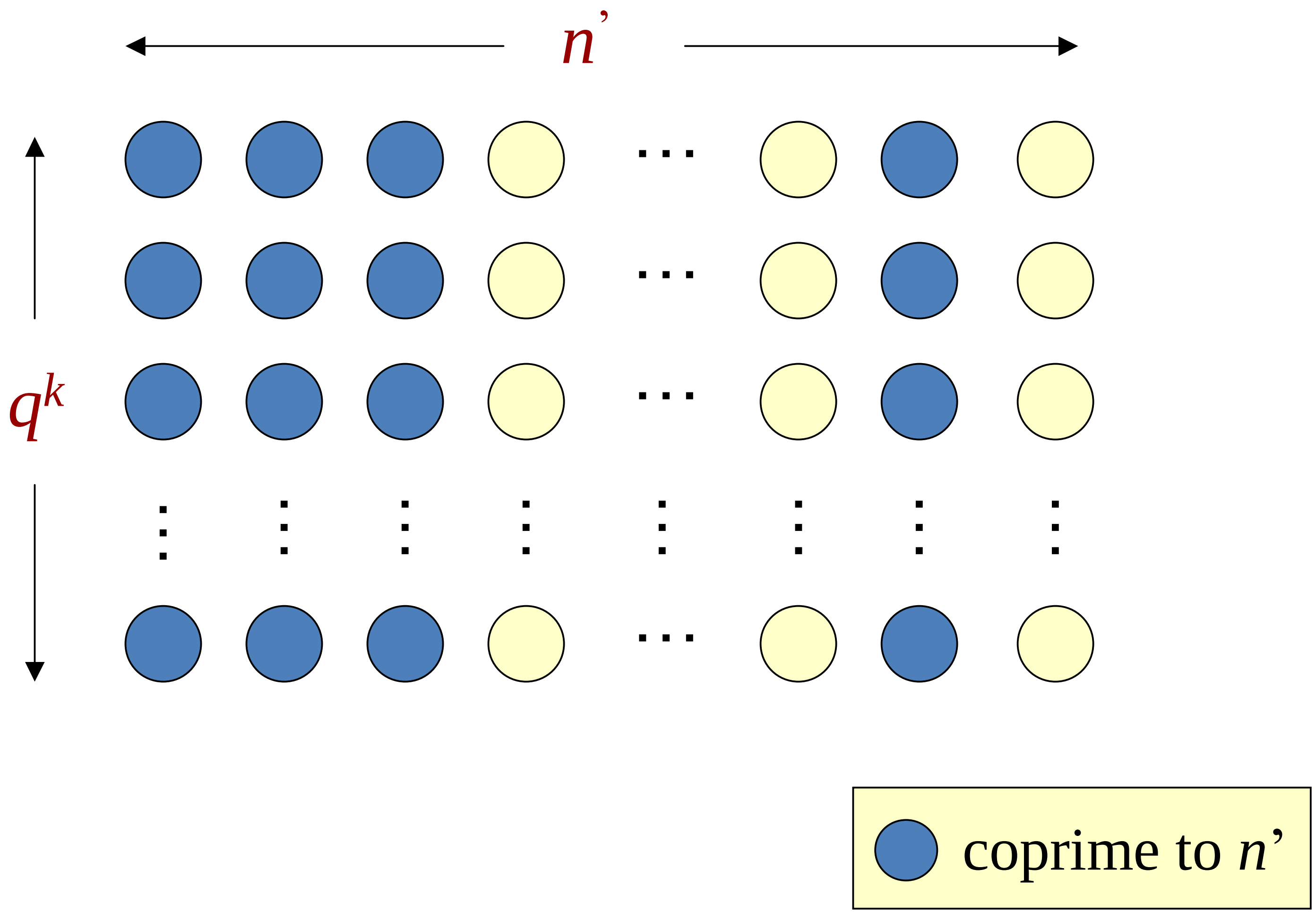
Let $n = q^k n'$ for some prime q and k,
with $\gcd(q, n') = 1$

Thus, n' has exactly $j - 1$ factors

Now, consider arranging the integers $[1, n]$ into q^k groups, each group with n' integers

Then we have (see next page) :

Euler Phi Function



Euler Phi Function

Proof (cont) :

Number of integers coprime to n'

$= q^k\,\varphi(n')$

Among these integers, exactly $1/\,q$ of them are multiples of q (why?)

➔ Number of integers coprime to $q^k n'$

$= q^k\,\varphi(n')\,(1 - 1/q) = n \prod_{p\,|\,n} (1 - 1/p)$

Euler Phi Function

Corollary 3:

The φ function obeys the following properties :

1. Suppose the prime factorization of n is :

$$n = p_1^{e_1} p_2^{e_2} \ldots p_j^{e_j} \qquad \text{(all } p_i\text{'s are distinct)}$$

   Then $\varphi(n) = \varphi(p_1^{e_1})\, \varphi(p_2^{e_2}) \ldots \varphi(p_j^{e_j})$

2. Suppose a and b are relatively prime.

   Then $\varphi(ab) = \varphi(a)\, \varphi(b)$