# CS 5319
# Advanced Discrete Structure

## Lecture 8:
## Introduction to Number Theory I

# 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

# What is Number Theory ?

- Number theory is the study of integers
- Once thought to be purely for interest
- Full of questions that can be easily described, but incredibly difficult to answer
- These “difficulties” lead to useful applications (e.g., cryptography)
- This lecture shall introduce some basic results in number theory

# Some Famous Problems

- Fermat Last Theorem

  Are there any positive integers $x$, $y$, $z$ such that $x^n + y^n = z^n$ for some integer $n > 2$ ?

  (1994: Proved by Andrew Wiles)

- Goldbach Conjecture

  Is it true that every even integer $\geq 4$ can be expressed as the sum of two primes?

  (1995 : Ramare showed at most 6 primes )

# Some Famous Problems

- Twin Prime Conjecture

  Are there infinitely many primes $p$ such that $p + 2$ is also a prime?

  (1966 : Chen showed that there are infinitely many primes $p$ such that $p + 2$ is a product of at most two primes)

# Some Famous Problems

- Primality Testing

  Any efficient way to check if $n$ is a prime?

  (2002 : Agarwal, Kayal, and Saxena gave a $O((\log n)^{12})$-time algorithm)

- Factoring

  Given the product of two large primes $n = pq$, any efficient way to recover primes $p$ and $q$ ?

  (Best known algo: $O(e^{1.9(\ln n)^{1/3}(\ln \ln n)^{2/3}})$ time )

# Divisibility

# Divisibility

- Throughout this lecture, we will assume that all variables range over integers
- We say that $a$ divides $b$ if there is an integer $k$ such that $ak = b$
- This is denoted by : $\boxed{a \mid b}$
- For instance, we write

$$7 \mid 63 \quad \text{because} \quad 7 \cdot 9 = 63$$

# Divisibility

- By previous definition, every integer divides 0 because $a \cdot 0 = 0$
- If *a* divides *b*, then *b* is a multiple of *a*
- Any number *p* with no positive divisors other than 1 and itself is called a prime ;

  Every other number > 1 is called composite

  (Note: 1 is neither prime nor composite)
- E.g., 2, 3, 5, 7, 11, 13, … are primes.

  4, 6, 8, 9, 10, 12, … are composite

# Divisibility

Lemma 1: The following statements hold.

1. If $a \mid b$, then $a \mid bc$ for all $c$
2. If $a \mid b$ and $b \mid c$, then $a \mid c$
3. If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all $s$ and $t$
4. For all $c \neq 0$, $a \mid b$ if and only if $ac \mid bc$

Proof of (2): Since $a \mid b$, $b = aj$ for some $j$. Since $b \mid c$, $c = bk$ for some $k$. Thus $c = ajk$ so that $a \mid c$

# Division Theorem

Theorem 1:

Let $n$ and $d$ be integers such that $d > 0$. Then there exists a unique pair of integers $q$ and $r$ such that $n = qd + r$ and $0 \le r < d$.

Proof:

Existence : By induction on $n$

Uniqueness: By contradiction

# Greatest Common Divisor

# Greatest Common Divisor

- The greatest common divisor of $a$ and $b$ is the largest number that is a divisor of both $a$ and $b$

- It is denoted by : $\boxed{\gcd(a, b)}$

- For instance,

$\gcd(12, 40) = 4, \quad \gcd(5, 18) = 1, \quad \gcd(7, 0) = 7$

# Greatest Common Divisor

Theorem 2:

> The greatest common divisor of *a* and *b* is the smallest positive linear combination of *a* and *b*

- For example, gcd(52, 44) = 4

  And we can see that

  $$6 \cdot 52 + (-7) \cdot 44 = 4 .$$

  Furthermore, no other linear combination of 52 and 44 gives a smaller positive integer

# Greatest Common Divisor

Proof :

Let $m$ = smallest linear combination of $a$ and $b$
We shall show that

$$m \geq \gcd(a, b) \quad \text{and} \quad m \leq \gcd(a, b)$$

Firstly, we show $m \geq \gcd(a, b)$. By definition of common divisor, we have :

$$\gcd(a, b) \mid a \quad \text{and} \quad \gcd(a, b) \mid b$$

$\Rightarrow$ $\gcd(a, b) \mid m$ so that $m \geq \gcd(a, b)$ [why?]

# Greatest Common Divisor

Proof (cont) :

Next, we show $m \leq \gcd(a, b)$.

We do this by showing $m \mid a$ . Then a symmetric argument shows $m \mid b$ so that $m$ is a common divisor of $a$ and $b$.

Consequently, $m$ must be smaller than or equal to the "greatest" common divisor

All that remains is to show $m \mid a$

# Greatest Common Divisor

Proof (cont) :

By the Division Theorem, there exists $q$ and $r$ such that $a = qm + r$ and $0 \leq r < m$

Recall that $m = sa + tb$ for some $s$ and $t$, so that

$$a = q(sa + tb) + r$$

$$\Rightarrow \quad r = (1 - qs)a + (-qt)b$$

Thus $r = 0$ (otherwise $m$ is not the smallest positive linear combination of $a$ and $b$ )

Consequently, this implies $m \mid a$

# Properties of GCD

Lemma 2: The following statements hold.

1. Every common divisor of $a$ and $b$ divides $\gcd(a, b)$
2. $\gcd(ka, kb) = k \cdot \gcd(a, b)$
3. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$
4. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$
5. $\gcd(a, b) = \gcd(b, a \text{ rem } b)$

# Properties of GCD

Proof of (3) : Theorem 2 implies that there exist $s$, $t$, $u$, $v$ such that $sa + tb = 1$ and $ua + vc = 1$

Thus $(sa + tb)(ua + vc) = 1$

$\Rightarrow$ $a\,(asu + btu + csv) + bc\,(tv) = 1$

$\Rightarrow$ $\gcd(a, bc) = 1$

Proof of (4) :

Since $a \mid bc$, and $a \mid ac$ $\Rightarrow$ $a \mid \gcd(ac, bc)$.

Next, by Statement 2 of the lemma,

$$\gcd(ac, bc) = c \cdot \gcd(a, b) \;\Rightarrow\; a \mid c$$

# Properties of GCD

Proof of (5) :

Any linear combination of $b$ and "$a$ rem $b$" must be a linear combination of $a$ and $b$

➔ $\gcd(a, b) \leq \gcd(b, a \text{ rem } b)$

However, any linear combination of $a$ and $b$ must be a linear combination of $b$ and "$a$ rem $b$"

➔ $\gcd(a, b) \geq \gcd(b, a \text{ rem } b)$

Thus $\gcd(a, b) = \gcd(b, a \text{ rem } b)$