南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Dr. Qi Wang

Department of Computer Science and Engineering
Office: Room903, Nanshan iPark A7 Building
Email: wangqi@sustc.edu.cn

Primes

- A positive integer p that is greater than 1 and is divisible only by 1 and by itself is called a *prime*.

Primes

- A positive integer p that is greater than 1 and is divisible only by 1 and by itself is called a *prime*.

- A positive integer p that is greater than 1 and is not a prime is called a *composite*.

Primes

- A positive integer p that is greater than 1 and is divisible only by 1 and by itself is called a *prime*.

- A positive integer p that is greater than 1 and is not a prime is called a *composite*.

- **Fundamental Theorem of Arithmetic** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Primes and Composites

- How to determine whether a number is a prime or a composite?

Primes and Composites

- How to determine whether a number is a prime or a composite?

  Approach 1: test if each number $x < n$ divides n.

Primes and Composites

- How to determine whether a number is a prime or a composite?

Approach 1: test if each number $x < n$ divides n.

Approach 2: test if each prime number $x < n$ divides n.

Primes and Composites

- How to determine whether a number is a prime or a composite?

Approach 1: test if each number $x < n$ divides n.

Approach 2: test if each prime number $x < n$ divides n.

Approach 3: test if each prime number $x < \sqrt{n}$ divides n.

Primes and Composites

- If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Primes and Composites

- If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof.

◇ if n is composite, then it has a positive integer factor a such that $1 < a < n$ by definition. This means that $n = ab$, where b is an integer greater than 1.

◇ assume that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $ab > n$, contradiction. So either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

◇ Thus, n has a divisor less than $\sqrt{n}$.

◇ By the Fundamental Theorem of Arithmetic, this divisor is either prime, or is a product of primes. In either case, n has a prime divisor less than $\sqrt{n}$.

Primes

- There are infinitely many primes.

Proof (by contradiction)

Greatest Common Divisor (GCD)

- Let a and b be integers, not both 0. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b, denoted by $\gcd(a, b)$.

Greatest Common Divisor (GCD)

- Let a and b be integers, not both 0. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b, denoted by $\gcd(a, b)$.

  The integers a and b are *relatively prime* if their greatest common divisor is 1.

Greatest Common Divisor (GCD)

- Let a and b be integers, not both 0. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b, denoted by $\gcd(a, b)$.

  The integers a and b are *relatively prime* if their greatest common divisor is 1.

  A systematic way to find the gcd is **factorization**. Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$. Then $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_k, b_k)}$

Least Common Multiple (LCM)

- Let a and b be integers. The *least common multiple* of a and b is the smallest positive integer that is divisible by both a and b, denoted by $\mathrm{lcm}(a, b)$.

Least Common Multiple (LCM)

- Let a and b be integers. The *least common multiple* of a and b is the smallest positive integer that is divisible by both a and b, denoted by $\text{lcm}(a, b)$.

We can also use **factorization** to find the lcm. Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$. Then
$\text{gcd}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_k, b_k)}$

Euclidean Algorithm

- Factorization can be **cumbersome** and **time consuming** since we need to find all factors of the two integers.

Euclidean Algorithm

- Factorization can be **cumbersome** and **time consuming** since we need to find all factors of the two integers.

- Luckily, we have an efficient algorithm, called **Euclidean algorithm**. This algorithm has been known since ancient times and named after the ancient Greek mathmaticain Euclid.

Euclidean Algorithm

- For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Euclidean Algorithm

- For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Euclidean Algorithm

- For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Euclidean Algorithm

- For two integers 287 and 91, we want to find $\gcd(287, 91)$.

  Step 1: $287 = 91 \cdot 3 + 14$

  Step 2: $91 = 14 \cdot 6 + 7$

  Step 3: $14 = 7 \cdot 2 + 0$

Euclidean Algorithm

- For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

Euclidean Algorithm

- The Euclidean algorithm in pseudocode

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

Euclidean Algorithm

- The Euclidean algorithm in pseudocode

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\text{gcd}(a, b) \text{ is } x\}$

The number of divisions required to find $\gcd(a, b)$ is $O(\log b)$, where $a \geq b$. (this will be proved later.)

Correctness of Euclidean Algorithm

- **Lemma** Let $a = bq + r$, where a, b, q and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Correctness of Euclidean Algorithm

- **Lemma** Let $a = bq + r$, where a, b, q and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Proof.

◇ suppose that $d|a$ and $d|b$. Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be any common divisor of b and r.

◇ suppose that $d|b$ and $d|r$. Then d also divdes $bq + r = a$. Hence, any common divisor of a and b must also be a common divisor of b and r.

◇ Therefore, $\gcd(a, b) = \gcd(b, r)$.

Correctness of Euclidean Algorithm

- Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$.

Correctness of Euclidean Algorithm

- Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$.

$$
\begin{array}{llr}
r_0 & = r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 & = r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\
 & \vdots & \\
r_{n-2} & = r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\
r_{n-1} & = r_n q_n \,. &
\end{array}
$$

Correctness of Euclidean Algorithm

- Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$.

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2, \\
&\;\cdot \\
&\;\cdot \\
&\;\cdot \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n .
\end{aligned}
$$

$$\gcd(a,b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

Euclidean Algorithm

- **Example**: Find the GCD of 286 and 503.

Euclidean Algorithm

- **Example**: Find the GCD of 286 and 503.

$$\begin{aligned} &\gcd(503, 286) \\ &= \gcd(286, 217) \end{aligned}$$

$$503 = 1 \cdot 286 + 217$$

Euclidean Algorithm

- **Example**: Find the GCD of 286 and 503.

$$\begin{aligned} &\gcd(503, 286) \\ &= \gcd(286, 217) \\ &= \gcd(217, 69) \end{aligned}$$

$$\begin{aligned} 503 &= 1 \cdot 286 + 217 \\ 286 &= 1 \cdot 217 + 69 \end{aligned}$$

Euclidean Algorithm

- **Example**: Find the GCD of 286 and 503.

$$\begin{aligned} &\gcd(503, 286) \\ &= \gcd(286, 217) \\ &= \gcd(217, 69) \\ &= \gcd(69, 10) \end{aligned}$$

$$\begin{aligned} 503 &= 1 \cdot 286 + 217 \\ 286 &= 1 \cdot 217 + 69 \\ 217 &= 3 \cdot 69 + 10 \end{aligned}$$

Euclidean Algorithm

- **Example**: Find the GCD of 286 and 503.

$$
\begin{aligned}
&\gcd(503, 286)\\
&= \gcd(286, 217)\\
&= \gcd(217, 69)\\
&= \gcd(69, 10)\\
&= \gcd(10, 9)\\
&= 1
\end{aligned}
$$

$$
\begin{aligned}
503 &= 1 \cdot 286 + 217\\
286 &= 1 \cdot 217 + 69\\
217 &= 3 \cdot 69 + 10\\
69 &= 6 \cdot 10 + 9\\
10 &= 1 \cdot 9 + 1\\
9 &= 9 \cdot 1
\end{aligned}
$$

GCD as Linear Combinations

- **Bezout's Theorem** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. This is called *Bezout's identity*.

GCD as Linear Combinations

- **Bezout's Theorem** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. This is called *Bezout's identity*.

We may use *extended Euclidean algorithm* to find Bezout's identity.

GCD as Linear Combinations

- **Bezout's Theorem** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. This is called *Bezout's identity*.

  We may use *extended Euclidean algorithm* to find Bezout's identity.

  Example: Express 1 as the linear combination of 503 and 286.

GCD as Linear Combinations

- **Bezout's Theorem** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. This is called *Bezout's identity*.

We may use *extended Euclidean algorithm* to find Bezout's identity.

Example: Express 1 as the linear combination of 503 and 286.

$$
\begin{aligned}
503 &= 1 \cdot 286 + 217 \\
286 &= 1 \cdot 217 + 69 \\
217 &= 3 \cdot 69 + 10 \\
69 &= 6 \cdot 10 + 9 \\
10 &= 1 \cdot 9 + 1
\end{aligned}
$$

GCD as Linear Combinations

- **Bezout's Theorem** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. This is called *Bezout's identity*.

We may use *extended Euclidean algorithm* to find Bezout's identity.

Example: Express 1 as the linear combination of 503 and 286.

$$503 = 1 \cdot 286 + 217$$
$$286 = 1 \cdot 217 + 69$$
$$217 = 3 \cdot 69 + 10$$
$$69 = 6 \cdot 10 + 9$$
$$10 = 1 \cdot 9 + 1$$

$$\begin{aligned} 1 &= 10 - 1 \cdot 9 \\ &= 7 \cdot 10 - 1 \cdot 69 \\ &= 7 \cdot 217 - 22 \cdot 69 \\ &= 29 \cdot 217 - 22 \cdot 286 \\ &= 29 \cdot 503 - 51 \cdot 286 \end{aligned}$$

Corollaries of Bezout's Theorem

- If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a | bc$, then $a | c$.

Corollaries of Bezout's Theorem

- If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a | bc$, then $a | c$.

  Proof. Since $\gcd(a, b) = 1$, by Bezout's Theorem there exist s and t such that $1 = sa + tb$. This yields $c = sac + tbc$. Since $a | bc$, we have $a | tbc$, and then $a | (sac + tbc) = c$.

Corollaries of Bezout's Theorem

- If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a | bc$, then $a | c$.

  Proof. Since $\gcd(a, b) = 1$, by Bezout's Theorem there exist s and t such that $1 = sa + tb$. This yields $c = sac + tbc$. Since $a | bc$, we have $a | tbc$, and then $a | (sac + tbc) = c$.

- If p is prime and $p | a_1 a_2 \cdots a_n$, then $p | a_i$ for some i.

Corollaries of Bezout's Theorem

- If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

  Proof. Since $\gcd(a, b) = 1$, by Bezout's Theorem there exist s and t such that $1 = sa + tb$. This yields $c = sac + tbc$. Since $a|bc$, we have $a|tbc$, and then $a|(sac + tbc) = c$.

- If p is prime and $p|a_1 a_2 \cdots a_n$, then $p|a_i$ for some i.

  Proof. by induction

Uniqueness of Prime Factorization

- We prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique.

Uniqueness of Prime Factorization

- We prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique.

Proof. (by contradiction) Suppose that the positive integer n can be written as a product of primes in two distinct ways:

$n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$

Remove all common primes from the factorizations to get

$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$

It then follows that p_{i_1} divides q_{j_k} for some k, contradicting the assumption that p_{i_1} and q_{j_k} are distinct primes.

Dividing Congruences by an Integer

- **Theorem** Let m be a positive integer and let a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Dividing Congruences by an Integer

- **Theorem** Let m be a positive integer and let a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof. Since $ac \equiv bc \pmod{m}$, we have $m | ac - bc = c(a - b)$. Because $\gcd(c, m) = 1$, it follows that $m | a - b$.

Mersenne Primes

- Prime numbers of the form $2^p - 1$, where p is a prime.

Marin Mersenne

Mersenne Primes

- Prime numbers of the form $2^p - 1$, where p is a prime.

  ◇ $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, $2^7 - 1 = 127$ are Mersenne primes.

  ◇ $2^{11} - 1 = 2047 = 23 \cdot 89$ is not a Mersenne prime.

Marin Mersenne

Mersenne Primes

- Prime numbers of the form $2^p - 1$, where p is a prime.
  - ◇ $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, $2^7 - 1 = 127$ are Mersenne primes.
  - ◇ $2^{11} - 1 = 2047 = 23 \cdot 89$ is not a Mersenne prime.
  - ◇ The largest known prime numbers are Mersenne primes.

Marin Mersenne

Mersenne Primes

- Prime numbers of the form $2^p - 1$, where p is a prime.

Marin Mersenne

◇ $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, $2^7 - 1 = 127$ are Mersenne primes.

◇ $2^{11} - 1 = 2047 = 23 \cdot 89$ is not a Mersenne prime.

◇ The largest known prime numbers are Mersenne primes.

Largest Known Prime, 49th Known Mersenne Prime Found!

January 7, 2016 — GIMPS celebrated its 20th anniversary with the discovery of the largest known prime number, $2^{74,207,281}$-1.

http://www.mersenne.org/

Conjectures about Primes

- *Goldbach's Conjecture* $(1+1)$: Every even integer $n > 2$, is the sum of two primes.

Conjectures about Primes

- *Goldbach's Conjecture* $(1+1)$: Every even integer $n > 2$, is the sum of two primes.

"$3+4$", "$3+3$", "$2+3$" – Y. Wang, 1956

"$1+5$" – C. Pan, 1962

"$1+4$" – Y. Wang, 1962

"$1+2$" – J. Chen, 1973

Conjectures about Primes

- *Goldbach's Conjecture* $(1+1)$: Every even integer $n > 2$, is the sum of two primes.

  “$3+4$”, “$3+3$”, “$2+3$” – Y. Wang, 1956

  “$1+5$” – C. Pan, 1962

  “$1+4$” – Y. Wang, 1962

  “$1+2$” – J. Chen, 1973

- *Twin-prime Conjecture*: There are infinitely many twin primes.

Linear Congruences

- A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

Linear Congruences

- A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

  The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Linear Congruences

- A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

  The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

  Systems of linear congruences have been studied since ancient times.

  今有物不知其数 三三数之剩二 五五数之剩三 七七数之剩二 问物几何

Modular Inverse

- An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse* of a modulo m.

Modular Inverse

- An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse* of a modulo m.

  One method of solving linear congruences makes use of an inverse $\bar{a}$ if it exists. From $ax \equiv b \pmod{m}$, it follows that $\bar{a}ax \equiv \bar{a}b \pmod{m}$ and then $x \equiv \bar{a}b \pmod{m}$.

Modular Inverse

- An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse* of a modulo m.

  One method of solving linear congruences makes use of an inverse $\bar{a}$ if it exists. From $ax \equiv b \pmod{m}$, it follows that $\bar{a}ax \equiv \bar{a}b \pmod{m}$ and then $x \equiv \bar{a}b \pmod{m}$.

  When does an inverse of a modulo m exist?

Inverse of a modulo m

- **Theorem** If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, the inverse is uinque modulo m.

Inverse of a modulo m

- **Theorem** If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, the inverse is uinque modulo m.

  Proof. Since $\gcd(a, m) = 1$, there are integers s and t such that $sa + tm = 1$. Hence $sa + tm \equiv 1 \pmod{m}$. Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$. This means that s is an inverse of a modulo m.

Inverse of a modulo m

- **Theorem** If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, the inverse is uinque modulo m.

  Proof. Since $\gcd(a, m) = 1$, there are integers s and t such that $sa + tm = 1$. Hence $sa + tm \equiv 1 \pmod{m}$. Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$. This means that s is an inverse of a modulo m.

  How to prove the uniqueness of the inverse?

How to find inverses?

- Using *extended Euclidean algorithm*

How to find inverses?

- Using *extended Euclidean algorithm*

  Example. Find an inverse of 101 modulo 4620.

How to find inverses?

- Using *extended Euclidean algorithm*

Example. Find an inverse of 101 modulo 4620.

$$4620 = 45 \cdot 101 + 75$$
$$101 = 1 \cdot 75 + 26$$
$$75 = 2 \cdot 26 + 23$$
$$26 = 1 \cdot 23 + 3$$
$$23 = 7 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

How to find inverses?

- Using *extended Euclidean algorithm*

Example. Find an inverse of 101 modulo 4620.

$$
\begin{aligned}
4620 &= 45\cdot 101 + 75\\
101 &= 1\cdot 75 + 26\\
75 &= 2\cdot 26 + 23\\
26 &= 1\cdot 23 + 3\\
23 &= 7\cdot 3 + 2\\
3 &= 1\cdot 2 + 1\\
2 &= 2\cdot 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 1\cdot 2\\
1 &= 3 - 1\cdot(23 - 7\cdot 3) = -1\cdot 23 + 8\cdot 3\\
1 &= -1\cdot 23 + 8\cdot(26 - 1\cdot 23) = 8\cdot 26 - 9\cdot 23\\
1 &= 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 26\cdot 26 - 9\cdot 75\\
1 &= 26\cdot(101 - 1\cdot 75) - 9\cdot 75\\
&= 26\cdot 101 - 35\cdot 75\\
1 &= 26\cdot 101 - 35\cdot(4620 - 45\cdot 101)\\
&= -35\cdot 4620 + 1601\cdot 101
\end{aligned}
$$

Using Inverses to Solve Congruences

- Solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Using Inverses to Solve Congruences

- Solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

  Example. What are the solutions of the congruence $3x \equiv 4 \pmod{7}$?

Using Inverses to Solve Congruences

- Solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

  Example. What are the solutions of the congruence $3x \equiv 4 \pmod{7}$?

  Solution: We found that -2 is an inverse of 3 modulo 7. Multiply both sides of the congruence by -2, we have $x \equiv -8 \equiv 6 \pmod{7}$.

Number of Solutions to Congruences *

- **Theorem** Let $d = \gcd(a, m)$ and $m' = m/d$. The congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d|b$. If $d|b$, then there are exactly d solutions. If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$.

Number of Solutions to Congruences *

- **Theorem** Let $d = \gcd(a, m)$ and $m' = m/d$. The congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d|b$. If $d|b$, then there are exactly d solutions. If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$.

Proof.
1) "only if": If x_0 is a solution, then $ax_0 - b = km$. Thus, $ax_0 - km = b$. Since d divides $ax_0 - km$, we must have $d|b$.

Number of Solutions to Congruences *

- **Theorem** Let $d = \gcd(a, m)$ and $m' = m/d$. The congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d|b$. If $d|b$, then there are exactly d solutions. If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$.

Proof.
1) "only if": If x_0 is a solution, then $ax_0 - b = km$. Thus, $ax_0 - km = b$. Since d divides $ax_0 - km$, we must have $d|b$.

2) "if": Suppose that $d|b$. Let $b = kd$. There exist integers s, t such that $d = as + mt$. Multiply both sides by k. Then $b = ask + mtk$. Let $x_0 = sk$. Then $ax_0 \equiv b \pmod{m}$.

Number of Solutions to Congruences *

- **Theorem** Let $d = \gcd(a, m)$ and $m' = m/d$. The congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d|b$. If $d|b$, then there are exactly d solutions. If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$.

Proof.

1) "only if": If x_0 is a solution, then $ax_0 - b = km$. Thus, $ax_0 - km = b$. Since d divides $ax_0 - km$, we must have $d|b$.

2) "if": Suppose that $d|b$. Let $b = kd$. There exist integers s, t such that $d = as + mt$. Multiply both sides by k. Then $b = ask + mtk$. Let $x_0 = sk$. Then $ax_0 \equiv b \pmod{m}$.

3) "$\# = d$": $ax_0 \equiv b \pmod{m}$ $ax_1 \equiv b \pmod{m}$ imply that $m|a(x_1 - x_0)$ and $m'|a'(x_1 - x_0)$. This implies further that $x_1 = x_0 + km'$, where $k = 0, 1, \ldots, d-1$.

The Chinese Remainder Theorem

- In the first century, the Chinese mathematician Sun-Tsu asked:
  "There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?"

今有物不知其数 三三数之剩二 五五数之剩三 七七数之剩二 问物几何

The Chinese Remainder Theorem

- In the first century, the Chinese mathematician Sun-Tsu asked:
  "There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?"

今有物不知其数 三三数之剩二 五五数之剩三 七七数之剩二 问物几何

$$
\begin{aligned}
x &\equiv 2 \pmod 3 \\
x &\equiv 3 \pmod 5 \\
x &\equiv 2 \pmod 7
\end{aligned}
$$

The Chinese Remainder Theorem

- **Theorem** (*The Chinese Remainder Theorem*) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

The Chinese Remainder Theorem

- **Proof** Let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$ and $m = m_1 m_2 \cdots m_n$. Since $\gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k such that $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots a_n M_n y_n.$$

It is checked that x is a solution to the n congruences.

The Chinese Remainder Theorem

- **Proof** Let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$ and $m = m_1 m_2 \cdots m_n$. Since $\gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k such that $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots a_n M_n y_n.$$

It is checked that x is a solution to the n congruences.

How to prove the uniqueness of the solution modulo m?

The Chinese Remainder Theorem

- **Example**

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

The Chinese Remainder Theorem

- **Example**

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.

$$35 \cdot 2 \equiv 1 \pmod 3$$
$$21 \equiv 1 \pmod 5$$
$$15 \equiv 1 \pmod 7$$

- **Example**

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.

$$35 \cdot 2 \equiv 1 \pmod 3 \qquad y_1 = 2$$
$$21 \equiv 1 \pmod 5 \qquad y_2 = 1$$
$$15 \equiv 1 \pmod 7 \qquad y_3 = 1$$

- **Example**

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.

$$35 \cdot 2 \equiv 1 \pmod{3} \qquad y_1 = 2$$
$$21 \equiv 1 \pmod{5} \qquad y_2 = 1$$
$$15 \equiv 1 \pmod{7} \qquad y_3 = 1$$

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \pmod{105}$$

Back Substitution

- We may also solve systems of linear congruences with pairwise relatively prime moduli by *back substitution*.

Back Substitution

- We may also solve systems of linear congruences with pairwise relatively prime moduli by *back substitution*.

Example

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Back Substitution

- We may also solve systems of linear congruences with pairwise relatively prime moduli by *back substitution*.

Example

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

$$\begin{aligned} x &\equiv 8 \pmod{15} \\ x &\equiv 2 \pmod{21} \end{aligned}$$

Modular Arithmetic in CS

- Modular arithmetic and congruencies are used in CS:
  - Pseudorandom number generators
  - Hash functions
  - Cryptography

Pseudorandom Number Generators

- *Linear congruential method*

  We choose four numbers:

  - the modulus m
  - multiplier a
  - increment c
  - seed x_0

- *Linear congruential method*

We choose four numbers:

- the modulus m
- multiplier a
- increment c
- seed x_0

We generate a sequence of numbers $x_1, x_2, \ldots, x_n, \ldots$ with $0 \leq x_i < m$ by using the congruence

$$x_{n+1} = (ax_n + c) \pmod{m}$$

Pseudorandom Number Generators

- *Linear congruential method*

$$x_{n+1} = (ax_n + c) \pmod{m}$$

Pseudorandom Number Generators

- *Linear congruential method*

$$x_{n+1} = (ax_n + c) \pmod{m}$$

Example:

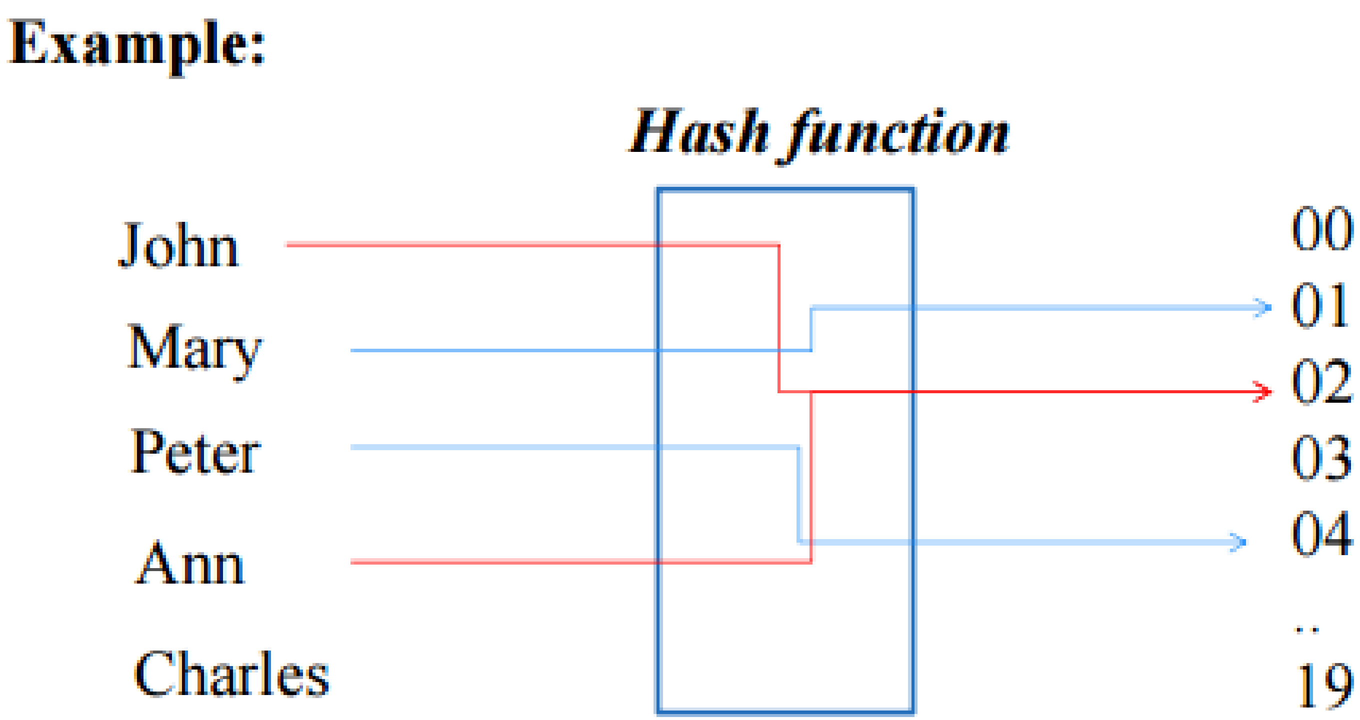
- Assume : m=9,a=7,c=4, $x_0 = 3$

- x_1= 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- x_4= 46 mod 9 =1
- x_5 = 11 mod 9 =2
- x_6 = 18 mod 9 =0
- ....

Hash Functions

- A *hash function* is an algorithm that maps data of arbitrary length to data of a fixed length. The values returned by a hash function are called *hash values* or hash codes.

- A *hash function* is an algorithm that maps data of arbitrary length to data of a fixed length. The values returned by a hash function are called *hash values* or hash codes.



Hash Functions

- **Problem**: Given a large collection of records, how can we store and find a record quickly?

Hash Functions

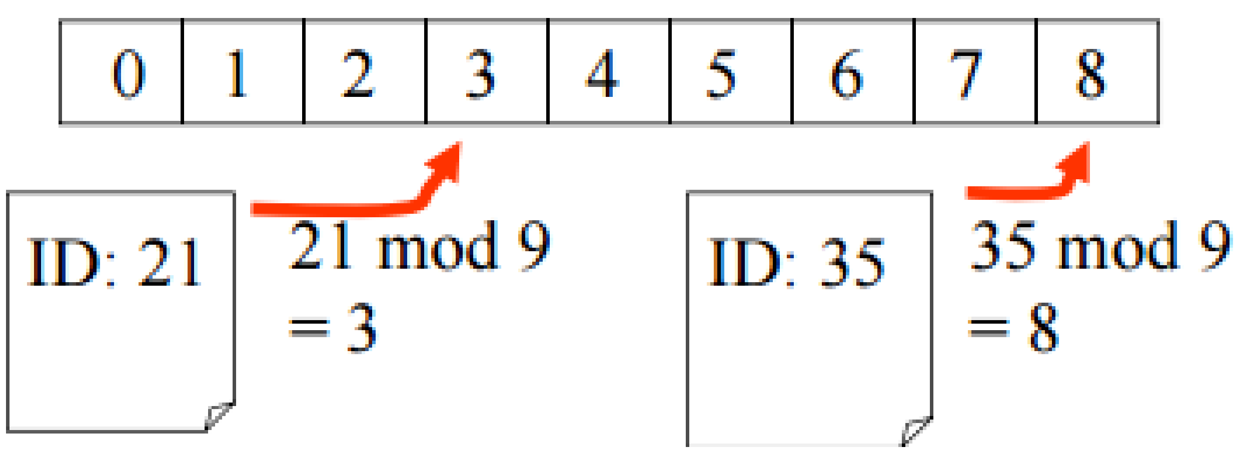
- **Problem**: Given a large collection of records, how can we store and find a record quickly?

  Solution: Use a hash function, calculate the location of the record based on the record's ID.

Example: A common hash function is

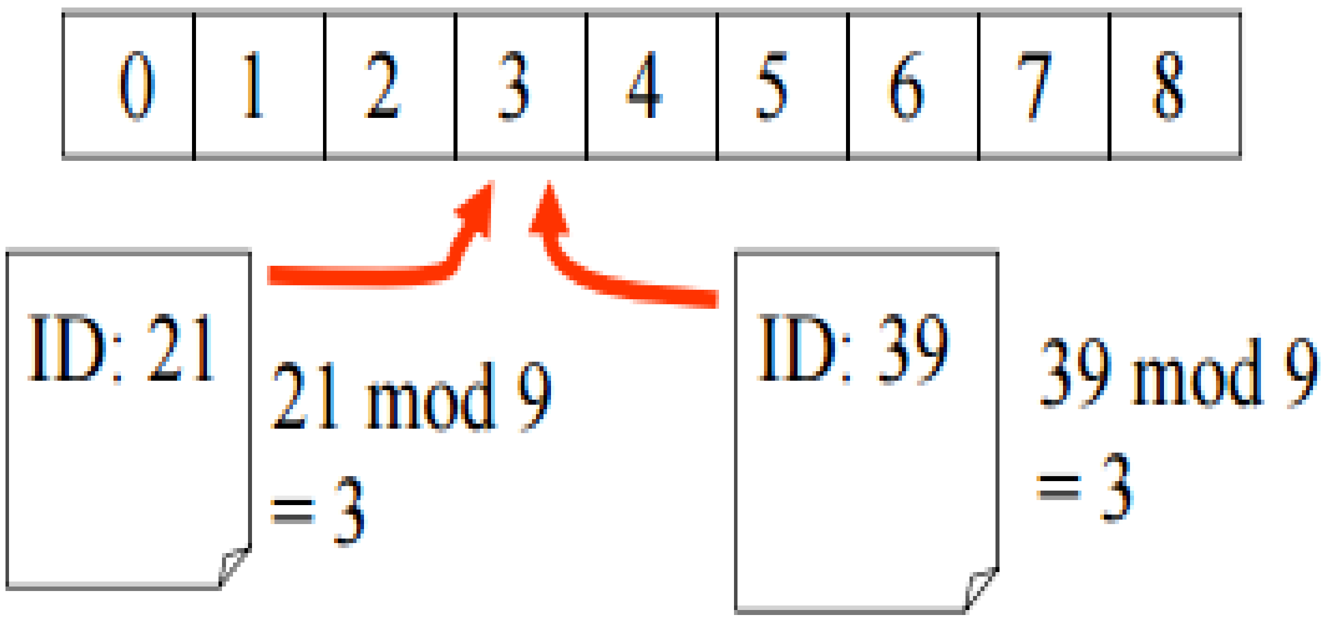
- $h(k) = k \textbf{ mod } n$,

where n is the number of available storage locations.



Hash Functions

- Two records mapped to the same location

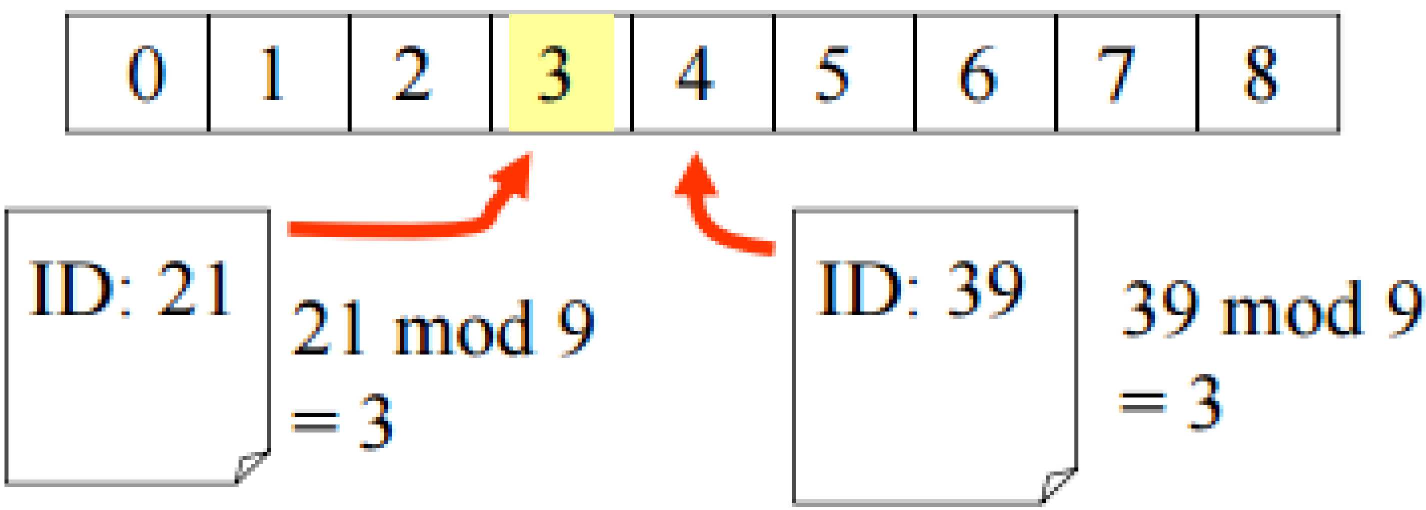


Hash Functions

- **Solution 1**: move to the next available location

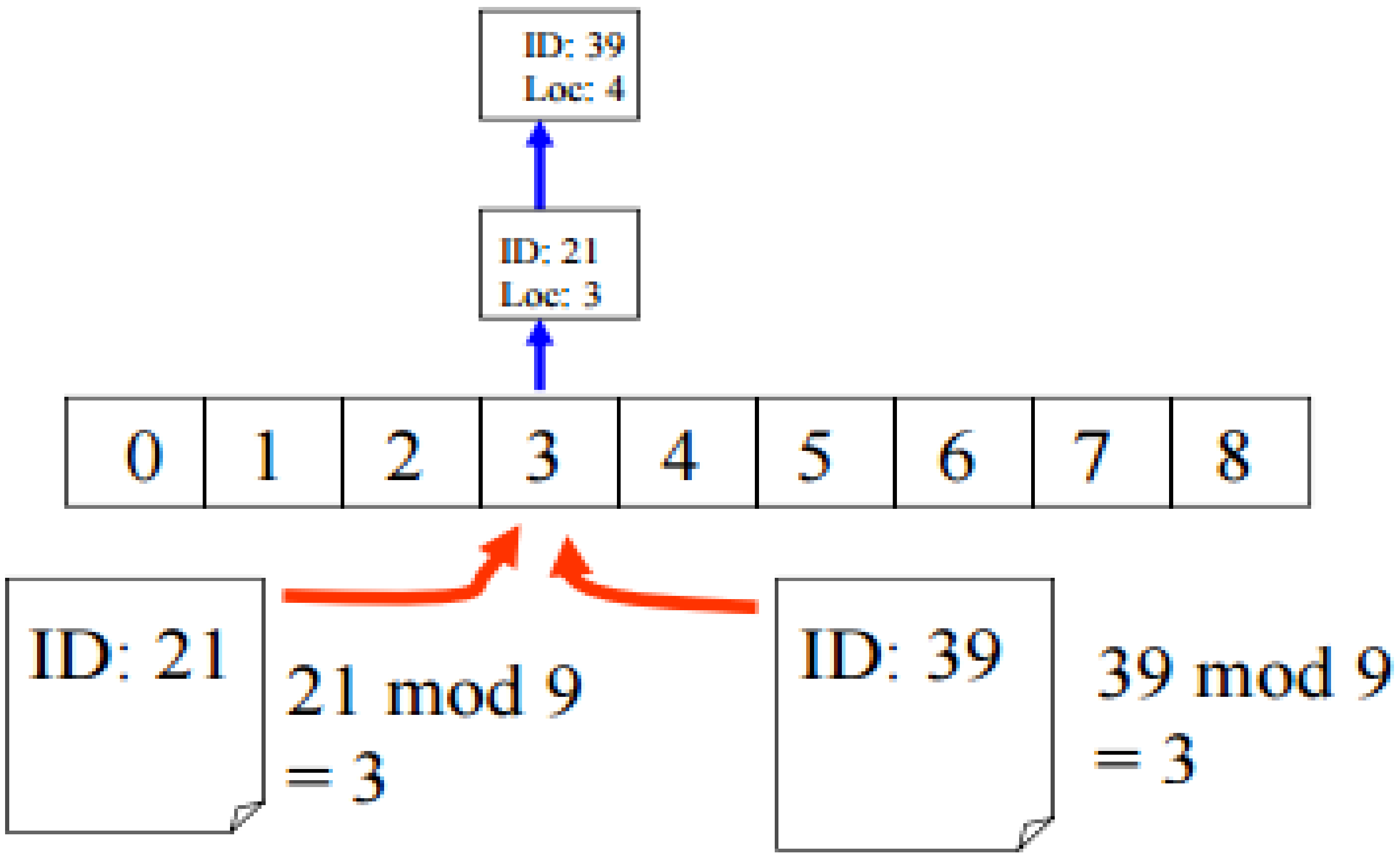
try

$$h_0(k) = k \textbf{ mod } n$$
$$h_1(k) = (k+1) \textbf{ mod } n$$
$$\ldots$$
$$h_m(k) = (k+m) \textbf{ mod } n$$



Hash Functions

- **Solution 2**: remember the exact location in a secondary structure that is searched sequentially



Applications of Number Theory in Cryptography

- Introduction
- Symmetric cryptography
- Asymmetric cryptography
- RSA Cryptosystem
- DLP and El Gamal cryptography
- Diffie-Hellman key exchange protocol
- Crytocurrency, e.g., bitcoin

Next Lecture

- cryptography, ...