南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

CS201 DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Dr. Qi Wang

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

Number Theory

- Division, Primes
- Congruence
- Greatest Common Divisor (GCD)

Number Theory

- Division, Primes

  $a = dq + r$

- Congruence

- Greatest Common Divisor (GCD)

Number Theory

- Division, Primes

  $a = dq + r \qquad q = a \text{ div } d \qquad r = a \text{ mod } d$

- Congruence

- Greatest Common Divisor (GCD)

Number Theory

- Division, Primes

  $a = dq + r \quad q = a \; div \; d \quad r = a \; mod \; d$

- Congruence

- Greatest Common Divisor (GCD)

Number Theory

- Division, Primes

  $a = dq + r \qquad q = a \; div \; d \qquad r = a \; mod \; d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

Number Theory

- Division, Primes

  $a = dq + r \quad q = a \textit{ div } d \quad r = a \textit{ mod } d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

Number Theory

- Division, Primes

  $a = dq + r \qquad q = a \ div \ d \qquad r = a \ mod \ d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

  (extended) Euclidean algorithm

Number Theory

- Division, Primes

$$a = dq + r \qquad q = a \; div \; d \qquad r = a \; mod \; d$$

- Congruence

$$a \equiv b \pmod{m} \text{ if } m \text{ divides } a - b$$

- Greatest Common Divisor (GCD)

Find the GCD of 286 and 503.

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

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

Number Theory

- Division, Primes

  $a = dq + r \quad q = a \ div \ d \quad r = a \ mod \ d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

  (extended) Euclidean algorithm
  find the modular inverse
  solve linear congruence $ax \equiv b \pmod{m}$ $(\gcd(a, m) = 1)$

Number Theory

- Division, Primes

  $a = dq + r \qquad q = a \; div \; d \qquad r = a \; mod \; d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

  (extended) Euclidean algorithm
  find the modular inverse
  solve linear congruence $ax \equiv b \pmod{m}$ $(\gcd(a, m) = 1)$
  Chinese Remainder Theorem / back substitution

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.

Marin Mersenne

  ◇ The largest known prime numbers are Mersenne primes.

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

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.

50th Known Mersenne Prime Found!

January 3, 2018 — Persistence pays off. Jonathan Pace, a GIMPS volunteer for over 14 years, discovered the 50th known Mersenne prime, $2^{77,232,917}$-1 on December 26, 2017. The prime number is calculated by multiplying together 77,232,917 twos, and then subtracting one. It weighs in at 23,249,425 digits, becoming the largest prime number known to mankind. It bests the previous record prime, also discovered by GIMPS, by 910,807 digits.

51st Known Mersenne Prime Found!

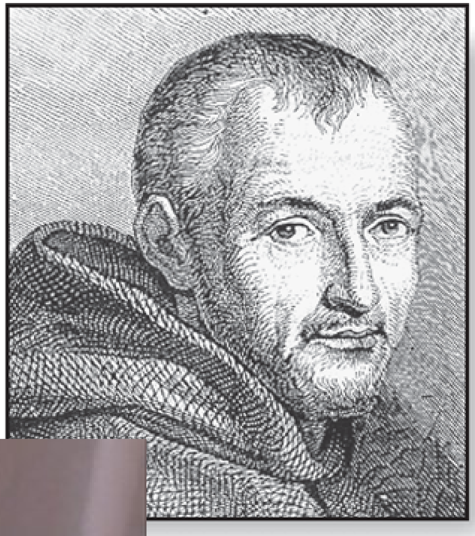
December 21, 2018 — The Great Internet Mersenne Prime Search (GIMPS) has discovered the largest known prime number, $\mathbf{2^{82,589,933}}$**-1**, having 24,862,048 digits. A computer volunteered by Patrick Laroche from Ocala, Florida made the find on December 7, 2018. The new prime number, also known as M82589933, is calculated by multiplying together 82,589,933 twos and then subtracting one. It is more than one and a half million digits larger than the previous record prime number.

http://www.mersenne.org/

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.



Marin Mersenne

Prime Found!

Januar

number, $2^{74,207,281}$-1.

January

December 2

the largest

e prime, $2^{77,232,917}$-1 on

23,249,425 digits, becoming

Decembe

589,933-1, having 24,862,048

digits. A cor

known as M82589933, is

calculated b

previous record prime

number.

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

  About 1500 years ago, 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?"

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.

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

$$1 = 3 - 1\cdot 2$$
$$1 = 3 - 1\cdot(23 - 7\cdot 3) = -1\cdot 23 + 8\cdot 3$$
$$1 = -1\cdot 23 + 8\cdot(26 - 1\cdot 23) = 8\cdot 26 - 9\cdot 23$$
$$1 = 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 26\cdot 26 - 9\cdot 75$$
$$1 = 26\cdot(101 - 1\cdot 75) - 9\cdot 75$$
$$= 26\cdot 101 - 35\cdot 75$$
$$1 = 26\cdot 101 - 35\cdot(4620 - 45\cdot 101)$$
$$= -35\cdot 4620 + 1601\cdot 101$$

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 $d|b$.

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

- About 1500 years ago, 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

- About 1500 years ago, 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

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

- **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

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

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**

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

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

$$\begin{aligned} 35 \cdot 2 &\equiv 1 \pmod{3} \\ 21 &\equiv 1 \pmod{5} \\ 15 &\equiv 1 \pmod{7} \end{aligned}$$

The Chinese Remainder Theorem

- **Example**

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

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

$$\begin{aligned} 35 \cdot 2 &\equiv 1 \pmod{3} & \quad y_1 &= 2 \\ 21 &\equiv 1 \pmod{5} & \quad y_2 &= 1 \\ 15 &\equiv 1 \pmod{7} & \quad y_3 &= 1 \end{aligned}$$

The Chinese Remainder Theorem

- **Example**

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

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

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

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

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

Pseudorandom Number Generators

- *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, $x_0 = 3$

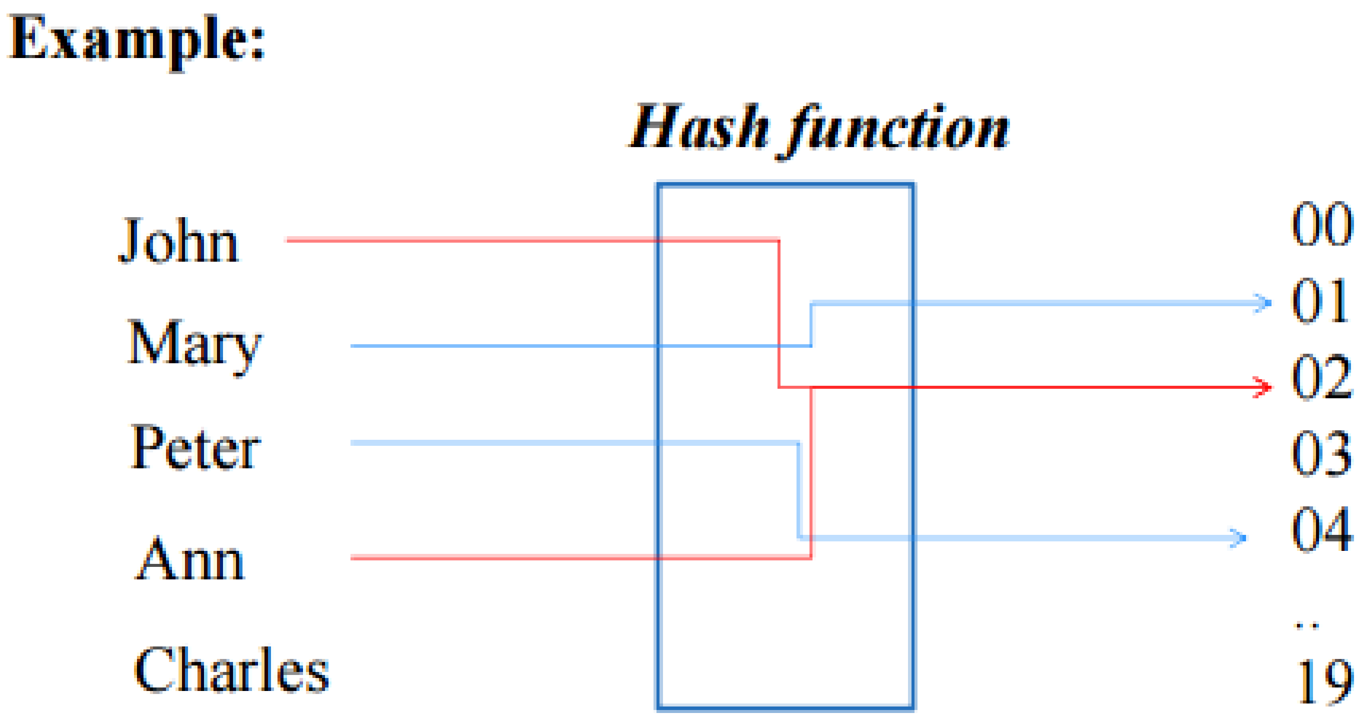
- x_1= 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- x_4= 46 mod 9 =1
- x_5 = 11 mod 9 =2
- x_6 = 18 mod 9 =0
- ....

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.

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.



Hash Functions

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

Hash Functions

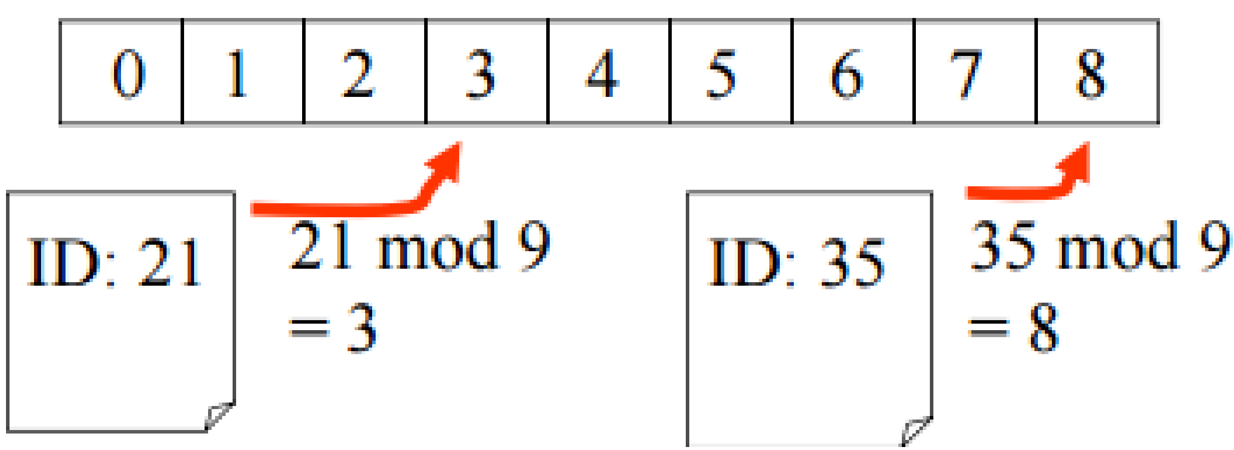
- **Problem**: Given a large collection of records, how can we store and find a record quickly?

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

  Example: A common hash function is

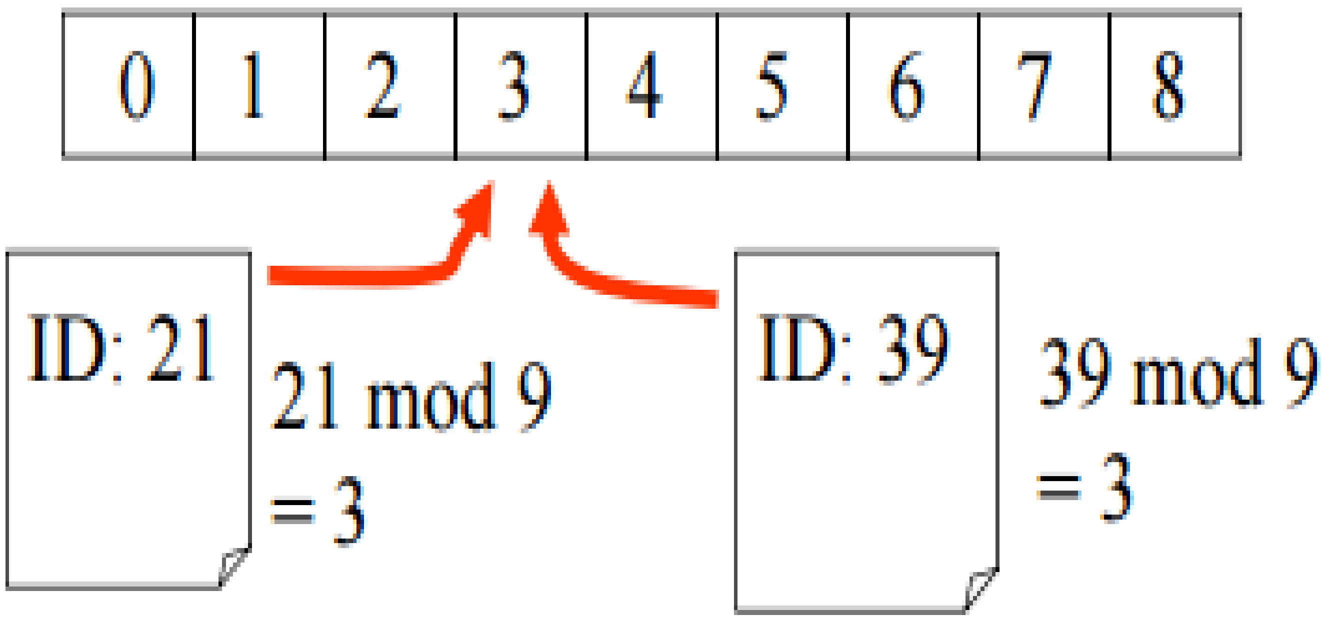
  - $h(k) = k \textbf{ mod } n$,

  where n is the number of available storage locations.



Hash Functions

- Two records mapped to the same location

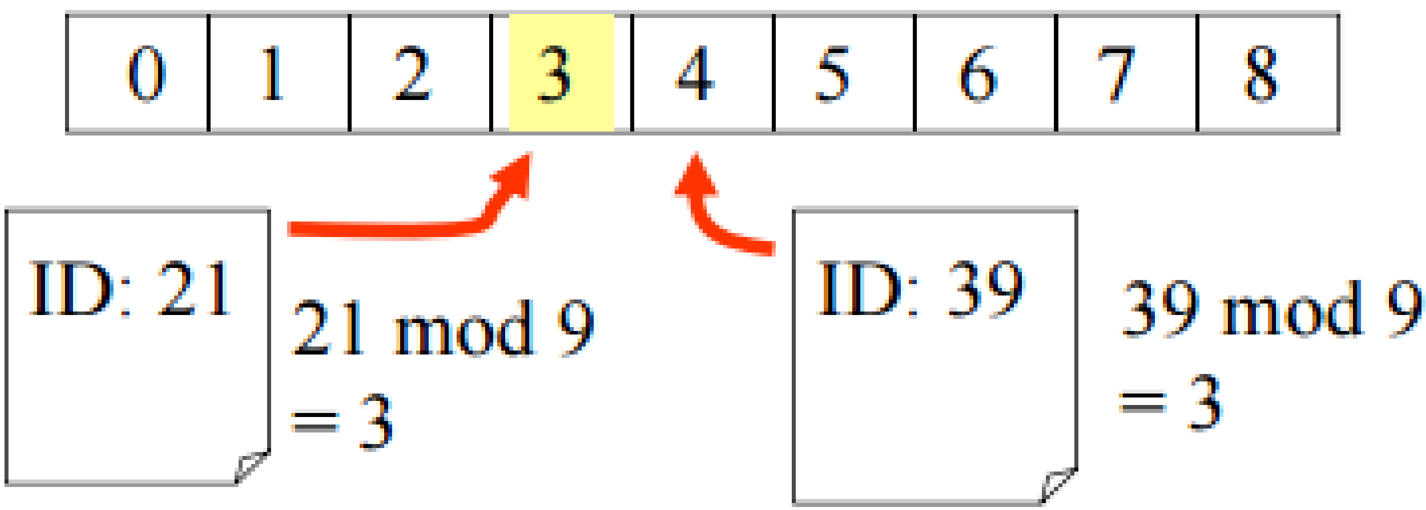


Hash Functions

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

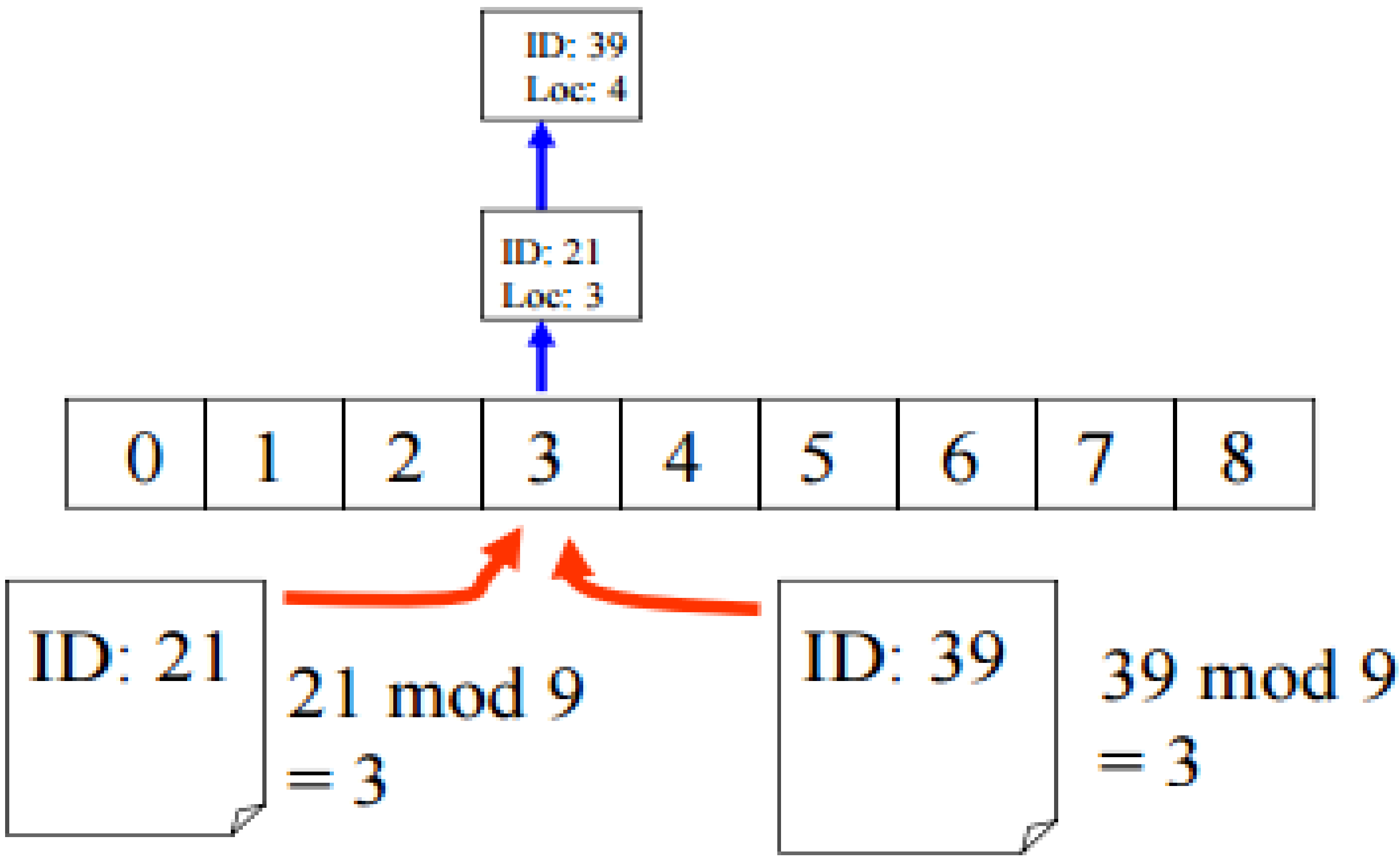
try

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



Hash Functions

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



Next Lecture

- cryptography ...