Discrete Mathematics: Lecture 11. Number Theory and application

Discrete Mathematics:

4.3 Primes and Great Common Divisors

Euclidean algorithm: finding the greatest common divisor

when $a = bq + r$, where $a, b, q, r \in Z$,

$\gcd(a, b) = \gcd(b, r)$

if d divides both a and b, $a = dk_1$, $b = dk_2$
because $r = a - bq = dk_1 - dk_2q = d(k_1 - k_2q)$, d also divides r
thus, any common divisor of a and b is also a common divisor of b and r

find gcd(91, 287)?

$287 = 91 \cdot 3 + 14$, $\Rightarrow \gcd(91, 287) = \gcd(91, 14)$
$91 = 14 \cdot 6 + 7$, $\Rightarrow \gcd(91, 14) = \gcd(14, 7)$
$14 = 7 \cdot 2$, $\Rightarrow \gcd(14, 7) = 7$

gcd as linear combination

BEZOUT's theorem:

if $a, b \in Z^+$, $\gcd(a, b) = sa + tb$ $(s, t \in Z)$

s and t is Bezout coefficients of a and b

express gcd(252, 198) = 18 as a linear combination of 252 and 198

by Euclidean algorithm

$252 = 198 \cdot 1 + 54$ $\quad\Rightarrow 54 = 252 - 1 \cdot 198$

$198 = 54 \cdot 3 + 36$ $\quad\Rightarrow 36 = 198 - 3 \cdot 54$

$54 = 36 \cdot 1 + 18$ $\quad\Rightarrow 18 = 54 - 1 \cdot 36$

$36 = 18 \cdot 2$

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$$
$$= 4(252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$$

gcd as linear combination

if a, b, c $\in Z^+$, gcd(a, b) = 1 and a|bc, then a|c

by Bezout's theorem,
sa + tb = 1
sac + tbc = c
if a|bc, then a|tbc
if a|sac and a|tbc, a|(sac + tbc)
if a|(sa+tb)c => a|c

"if a|b, then a|bc
"if a|b and a|c, then a|(b+c)"

gcd as linear combination

$m \in Z^+, a, b, c \in Z$

If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$

if $ac \equiv bc \pmod{m}$, $m \mid (ac - bc) \Rightarrow m \mid c\,(a - b)$

since $\gcd(c, m) = 1$, $m \nmid c$

by lemma if $a, b, c \in Z^+$, $\gcd(a, b) = 1$ and $a|bc$, then $a|c$

$m \mid (a - b) \Rightarrow a \equiv b \pmod{m}$

Discrete Mathematics:

4.4, 4.5 Linear combinations and applications

linear congruences

- Linear congruences: $ax \equiv b \pmod{m}$,

  where $m \in Z^+$, $a, b \in Z$, and x is variable
- $\bar{a}a \equiv 1 \pmod{m}$, $\bar{a}$ is inverse of a modulo m

- if a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists

if a and m are relatively prime integer, $\gcd(a, m) = 1 \Rightarrow sa + tm = 1$

$\Rightarrow sa + tm \equiv 1 \pmod{m}$

because $tm \equiv 0 \pmod{m}$, $sa \equiv 1 \pmod{m}$

thus s is an inverse of a modulo m

linear congruences

find an inverse of 3 modulo 7 by first finding Bezout coefficient of 3 and 7

=> find x such that $x \cdot 3 \equiv 1 \pmod{7}$

since gcd(3, 7) = 1, an inverse of 3 modulo 7 exists

by Euclidean algorithm

$7 = 2 \cdot 3 + 1$ => $-2 \cdot 3 + 7 = 1$ => -2 and 1 are Bezout coefficient of 3 and 7

since $7 \equiv 0 \pmod{7}$, $-2 \cdot 3 \equiv 1 \pmod{7}$

-2 is an inverse of 3 modulo 7

linear congruences

find an inverse of 101 modulo 4620

=> $x \cdot 101 \equiv 1 \pmod{4620}$

1) show that gcd(101, 4620) =1 to confirm there exists an inverse of 101 modulo 4620

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

=> gcd(101, 4620) = 1

2) find Bezout coefficients for 101 and 4620

1

$= 3 - 1 \cdot 2$

$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$

$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$

$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$

$= -35 \cdot 4620 + 1601 \cdot 101$

=>1601 is an inverse of 101 modulo 4620

linear congruences

find an inverse of 13 modulo 2436

$\Rightarrow x \cdot 13 \equiv 1 \pmod{2436}$

1) show that gcd(13, 2436) =1 to confirm there exists an inverse of 13 modulo 2436

$2436 = 13 \cdot 187 + 5$

$13 = 5 \cdot 2 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2$

=> gcd(13, 2436) = 1

2) find Bezout coefficients for 13 and 2436

1

$= 3 - 2 \cdot 1$

$= 3 - (5 - 3 \cdot 1) \cdot 1 = -5 + 2 \cdot 3$

$= -5 + 2\,(13 - 5 \cdot 2) = 2 \cdot 13 - 5 \cdot 5$

$= 2 \cdot 13 - 5 \cdot (2436 - 13 \cdot 187)$

$= 937 \cdot 13 - 5 \cdot 2436$

=>937 is an inverse of 13 modulo 2436

linear congruences

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

We already know that -2 is the inverse of 3 modulo 7.

$3x \equiv 4 \pmod{7}$

$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}$

$-6x \equiv -8 \pmod{7}$

Because $-6 \equiv 1 \pmod{7}$ and

$-8 \equiv 6 \pmod{7}$, $1 \cdot x \equiv 6 \pmod{7}$

$x = 6, 13, 20, \ldots,$ and $-1, -8, -15, \ldots$

Fermat's little theorem

if p is prime number and a is not divisible by p,

$$a^{p-1} \equiv 1 \pmod{p}$$

$p = 5$

$2^{5-1} \equiv 1 \pmod{5}$

$3^4 \equiv 1 \pmod{5}$

$4^4 \equiv 1 \pmod{5}$

$5^4 \equiv 0 \pmod{5}$

$6^4 \equiv 1 \pmod{5}$

:

Fermat's little theorem

if p is prime number and a is not divisible by p,

$a^{p-1} \equiv 1 \pmod{p}$

Find $7^{222} \bmod 11$

ab mod m = ((a mod m)(b mod m)) mod m

$7^{10} \equiv 1 \pmod{11}$

$7^{222} \bmod 11 = (7^{10})^{22}\, 7^2 \bmod 11 = ((7^{10})^{22} \bmod 11)(7^2 \bmod 11)$

$= (7^2 \bmod 11) = 49 \bmod 11 = 5$

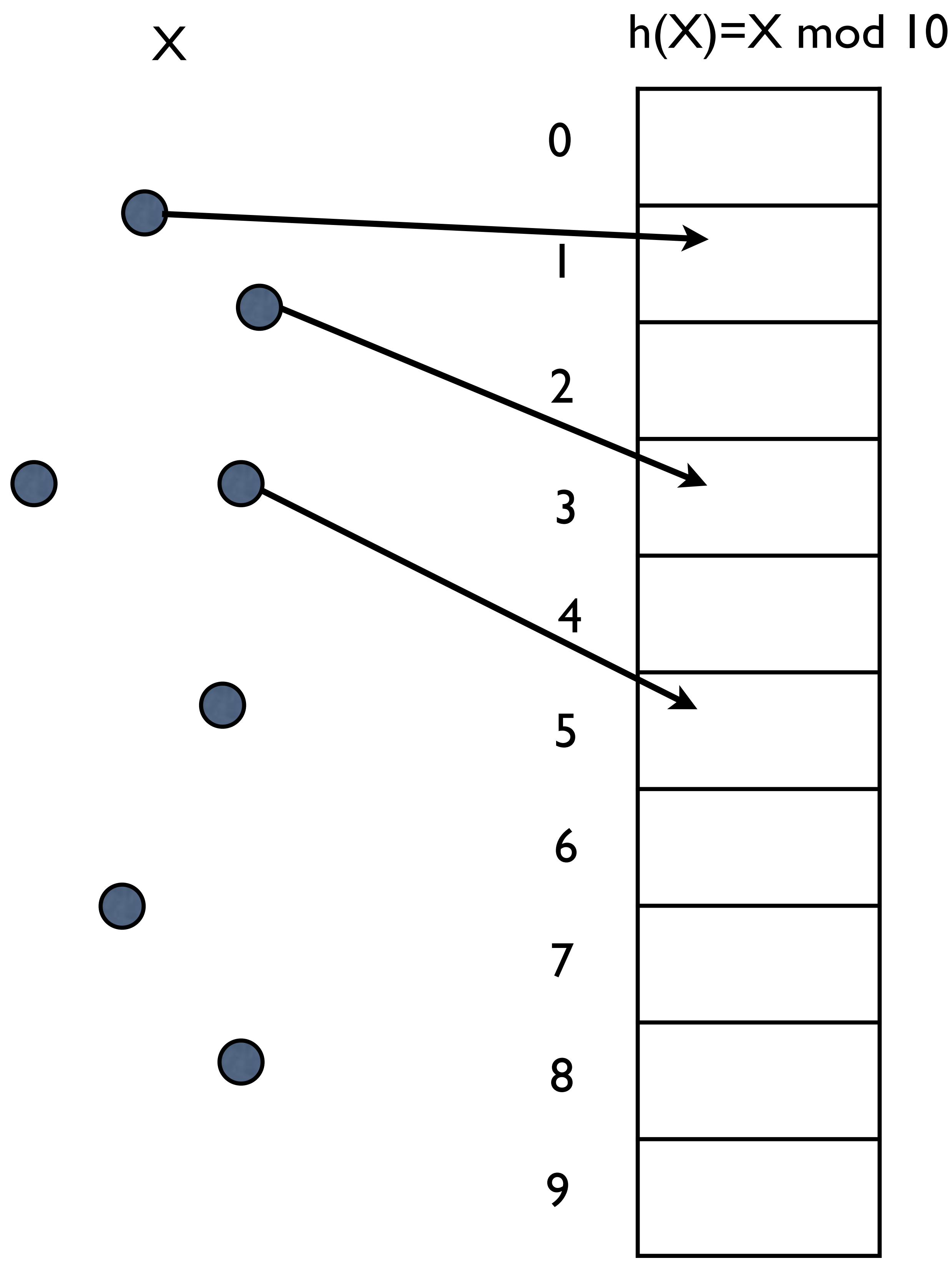
hash functions

- when the key of a record is k, hashing function $h(k)$ assigns a location for the record
- $h(k) = k \bmod m$, m is the number of available location
- because a hashing function is not one-to-one, a collision occurs

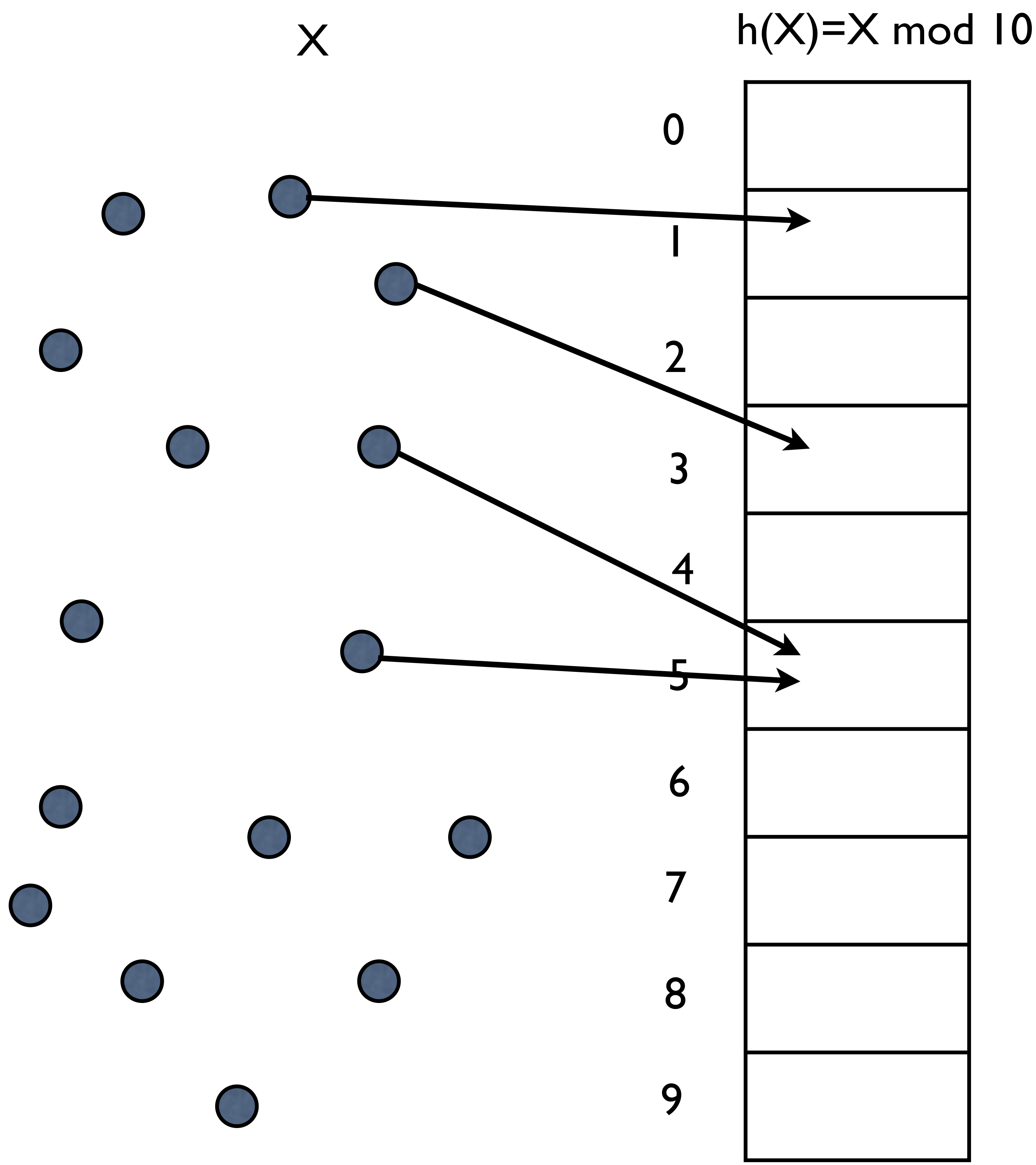
find the memory locations assigned by the hashing function $h(k) = k \bmod 111$ to records of customers with number 064212848?

$h(064212848) = 064212848 \bmod 111 = 14$

hash functions



hash functions

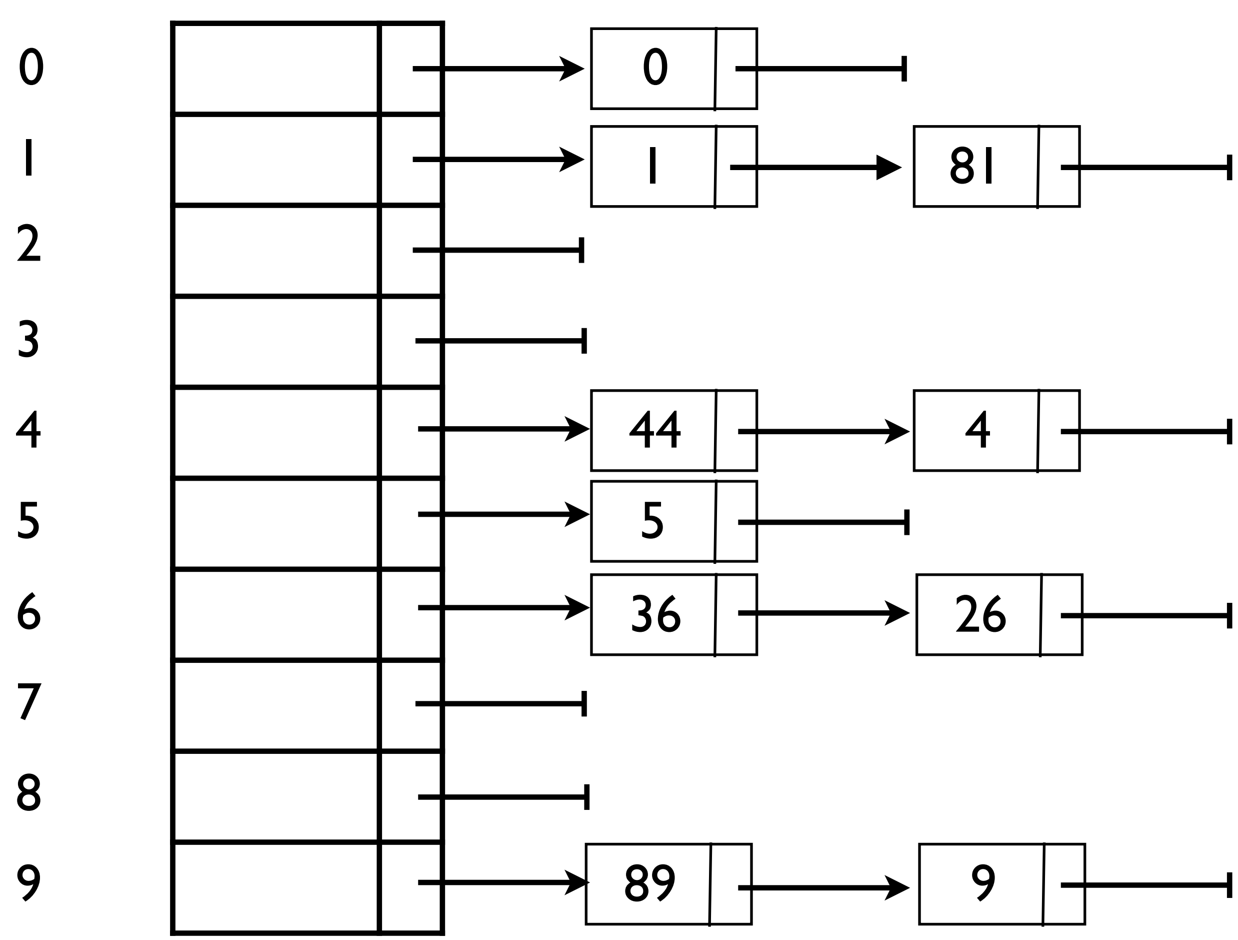


hash functions

- keep a list of all elements that hash to the same value
- operations
  - Find: use hash function to determine which list to traverse
  - Insert: traverse down the list to check whether the element is in the list

    if not, it is inserted at the front (or at the end)

A = {0, 44, 81, 1, 9, 36, 4, 5, 26, 89}



hash functions

DNA sequence:

ACCCTGGTCCGTACCGAACCTCCCTGGTAAACGGTGCCTCCACCGTCG

:		
ACCCT	1	
CCCTG	2	
CCTGG	3	
:		
CCTCC	19	→ 37
:		

classical cryptography: shift cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$f(p) = (p + k) \bmod 26, \quad k=3$

MEET YOU IN THE ZOO

12 4 4 19   24 14 20   8 13   19 7 4   25 14 14

↓ $f(p) = (p + 3) \bmod 26$

15 7 7 22   1 17 23   11 16   22 10 7   2 17 17

PHHW BRX LQ WKH

PHHW BRX LQ WKH

15 7 7 22   1 17 23   11 16   22 10 7   2 17 17

↓ $f(p) = (p - 3) \bmod 26$

12 4 4 19   24 14 20   8 13   19 7 4   25 14 14

MEET YOU IN THE ZOO

Application: Public-key cryptography

- Public-key cryptography
  - Everybody A has his/her key pair: {pubA, priA}.
  - PubA: public key => it is broadcasted to be known to everybody.
  - PriA: private key => it should be kept to be secret.

- Public-key cryptography: it has 3 algorithms.
  - Key generation algorithm G
    - it generates {pubA, priA}.
  - Encryption algorithm
    - $E_{pubA}(m)$: it takes pubA and plaintext msg m to generate the ciphertext c.
  - Decryption algorithm
    - $D_{priA}(c)$: it takes priA and ciphertext m to recover the plaintext m.

- Well known public-key cryptography: RSA, ElGamal, ECC, …

ElGamal Encryption for Zp

- Assumption: $Z_p = \{0, \ldots, p-1\}$ for prime p, g: generator in Zp
  - (generator $g \in Z_p$: $Z_p/\{0\}$ can be generated using $\{g^0 \bmod p = 1, g^1 \bmod p, \ldots, g^{p-1} \bmod p\}$

- Key generation:
  - select a private key $x \in Z_p$,
  - Compute a public key $h = g^x \bmod p$

- Encryption for message $m \in Z_p$ for public key h:
  - Choose $y \in Z_p$. Compute $c1 = g^y \bmod p$.
  - Compute $s = h^y \bmod p$.
  - Compute $c2 = m \cdot s \bmod p$.
  - Ciphertext = (c1, c2)

ElGamal Encryption for Zp

- Decryption for message (c1, c2)
  - Compute $s = c1^x \bmod p$
  - Computes s^{-1} w.r.t mod p
  - Computes $m = c2 \cdot s^{-1} \bmod p$

- Correctness of ElGamal algorithm
  - $c2 \cdot s^{-1} \equiv m \cdot s \cdot s^{-1} \equiv m \pmod p$
  - => $c2 \cdot s^{-1} \bmod p = m \cdot s \cdot s^{-1} \bmod p = m$

- Security of ElGamal algorithm
  - If an attacker successfully decrypts m without knowing x
    => he/she can solve DLP (Discrete Logarithm Problem).
  - DLP : solving $b^k = g$ to get k, where b,g are elements of a finite group. Up to know, there is no efficient algorithms known if the group is carefully chosen.