Integers and division

Integers and division

- **Number theory** is a branch of mathematics that explores integers and their properties.
- **Integers:**
  - **Z integers {…, -2,-1, 0, 1, 2, …}**
  - **Z^+ positive integers {1, 2, …}**

- Number theory has many applications within computer science, including:
  - Indexing - Storage and organization of data
  - Encryption
  - Error correcting codes
  - Random numbers generators

Primes

Definition: A positive integer p that is greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

Primes

Definition: A positive integer p that is greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

What is the next prime after 7?

- 11

Next?

- 13

Primes

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

Examples: 4, 6, 8, 9, …

Why?

2 | 4

Why 6 is a composite?

Primes

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

Examples: 4, 6, 8, 9, …

Why?

2 | 4

3 | 6 or 2 | 6

2 | 8 or 4 | 8

3 | 9

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

  - 12 = ?

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

  - 12 = 2*2*3
  - 21 = 3*7

- Process of finding out factors of the product: **factorization**.

Primes and composites

Factorization of composites to primes:

- $100 = 2*2*5*5 = 2^2*5^2$
- $99 = 3*3*11 = 3^2*11$

Important question:

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

Primes and composites

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

Simple approach (1):

- Let n be a number. To determine whether it is a prime we can test if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.

Primes and composites

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

Simple approach (1):

- Let n be a number. To determine whether it is a prime we can test if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.

- **Example:**
- Assume we want to check if 17 is a prime?
- The approach would require us to check:
- 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

Primes and composites

- **Example approach 1:**
- Assume we want to check if 17 is a prime?
- The approach would require us to check:
- 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

- **Is this the best we can do?**
- **No.** The problem here is that we try to test all the numbers. But this is not necessary.
- **Idea:** Every composite factorizes to a product of primes. So it is sufficient to test only the primes $x < n$ to determine the primality of n.

Primes and composites

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

Approach 2:

- Let n be a number. To determine whether it is a prime we can test if any prime number x < n divides it. If yes it is a composite. If we test all primes $x < n$ and do not find a proper divisor then n is a prime.

Primes and composites

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

Approach 2:

- Let n be a number. To determine whether it is a prime we can test if any prime number x < n divides it. If yes it is a composite. If we test all primes $x < n$ and do not find a proper divisor then n is a prime.

- **Example:** Is 31 a prime?
- Check if 2,3,5,7,11,13,17,23,29 divide it
- It is a prime !!

Primes and composites

Example approach 2:

Is 91 a prime number?

- Easy primes 2,3,5,7,11,13,17,19 ..
- But how many primes are there that are smaller than 91?

Caveat:

- If *n* is relatively small the test is good because we can enumerate (memorize) all small primes
- But if *n* is large there can be larger not obvious primes

Primes and composites

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

Primes and composites

Theorem: If n is a 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 $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $ab > \sqrt{n}\sqrt{n} = n$, which is a contradiction. So either $a \le \sqrt{n}$ *or* $b \le \sqrt{n}$.
- 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 and composites

Theorem: If n is a composite that n has a prime divisor less than or equal to $\sqrt{n}$.

Approach 3:

- Let n be a number. To determine whether it is a prime we can test if any prime number x < $\sqrt{n}$ divides it.

Example 1: Is 101 a prime?

- Primes smaller than $\sqrt{101}$ = 10.xxx are: 2,3,5,7
- 101 is not divisible by any of them
- **Thus 101 is a prime**

Example 2: Is 91 a prime?

- Primes smaller than $\sqrt{91}$ are: 2,3,5,7
- 91 is divisible by 7
- **Thus 91 is a composite**

Primes

Question: How many primes are there?

Theorem: There are infinitely many primes.

Primes

Question: How many primes are there?

Theorem: There are infinitely many primes.

Proof by Euclid.

- Proof by contradiction:
  - Assume there is a finite number of primes: $p_1, p_2, \ldots p_n$
- Let $Q = p_1 p_2 \ldots p_n + 1$ be a number.
- None of the numbers $p_1, p_2, \ldots, p_n$ divides the number Q.
- This is a contradiction since we assumed that we have listed all primes.

Division

Let a be an integer and d a positive integer. Then there are unique integers, q and r, with 0 <= r < d, such that

a = dq + r.

Definitions:

- a is called the **dividend**,
- d is called the **divisor**,
- q is called the **quotient** and
- r the **remainder** of the division.

Example: a= 14, d = 3
14 = 3*4 + 2
14/3=3.666
14 div 3 = 4
14 mod 3 = 2

Relations:

- **q = a div d , r = a mod d**

Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3} \ldots p_k^{ak}$ and $b= p_1^{b1}\ p_2^{b2}\ p_3^{b3} \ldots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)}\ p_2^{\min(a2,b2)}\ p_3^{\min(a3,b3)} \ldots p_k^{\min(ak,bk)}$

Examples:

- gcd(24,36) = ?
- $24 = 2*2*2*3=2^3*3$
- $36= 2*2*3*3=2^2*3^2$
- gcd(24,36) =

Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3} \dots p_k^{ak}$ and $b= p_1^{b1}\ p_2^{b2}\ p_3^{b3} \dots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)}\ p_2^{\min(a2,b2)}\ p_3^{\min(a3,b3)} \dots p_k^{\min(ak,bk)}$

Examples:

- gcd(24,36) = ?
- $24 = 2*2*2*3=2^{3}*3$
- $36= 2*2*3*3=2^{2}*3^{2}$
- $gcd(24,36) =2^{2}*3 =$ **12**

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: …

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: … 12*9= 108
- **Can we find a smaller number?**

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: … 12*9= 108
- **Can we find a smaller number?**
- **Yes.** Try 36. Both 12 and 9 cleanly divide 36.

Least common multiple

A systematic way to find the lcm using factorization:

- Let $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3} \ldots p_k^{ak}$ and $b= p_1^{b1}\ p_2^{b2}\ p_3^{b3} \ldots p_k^{bk}$
- $lcm(a,b)= p_1^{\max(a1,b1)}\ p_2^{\max(a2,b2)}\ p_3^{\max(a3,b3)} \ldots p_k^{\max(ak,bk)}$

Example:

- **What is lcm(12,9) =?**
- $12 = 2*2*3=2^2*3$
- $9=3*3 =3^2$
- **lcm(12,9)** $= 2^2 * 3^2 = 4 * 9 =$ **36**

Euclid algorithm

Finding the greatest common divisor requires factorization

- $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3} \ldots p_k^{ak}$, $b= p_1^{b1}\ p_2^{b2}\ p_3^{b3} \ldots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)}\ p_2^{\min(a2,b2)}\ p_3^{\min(a3,b3)} \ldots p_k^{\min(ak,bk)}$

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

- Luckily a more efficient method for computing the gcd exists:
- It is called **Euclid's algorithm**
  - the method is known from ancient times and named after Greek mathematician Euclid.

Euclid algorithm

Assume two numbers 287 and 91. We want gcd(287,91).

- First divide the larger number (287) by the smaller one (91)
- We get 287 = 3*91 +14

(1) Any divisor of 91 and 287 must also be a divisor of 14:

  - 287 - 3*91 = 14

- Why? [ak – cbk] =r → (a-cb)k = r → (a-cb) = r/k (must be an integer and thus k divides r]

(2) Any divisor of 91 and 14 must also be a divisor of 287

- Why? 287 = 3 b k + dk → 287 = k(3b +d) → 287 /k = (3b +d) ← 287/k must be an integer
- **But then gcd(287,91) = gcd(91,14)**

Euclid algorithm

- **We know that gcd(287,91) = gcd(91,14)**
- But the same trick can be applied again:
  - gcd(91,14)
  - 91 = 14.6 + 7
- and therefore
  - gcd(91,14)=gcd(14,7)
- And one more time:
  - gcd(14,7) = 7
  - trivial
- **The result: gcd(287,91) = gcd(91,14)=gcd(14,7) = 7**

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558) 666=1*558 + 108
  = gcd(558,108) 558=5*108 + 18
  = gcd(108,18) 108=6*18 + 0
  = **18**

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- gcd(503,286) 503=

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- gcd(503,286) 503=1*286 + 217
  =gcd(286, 217) 286=

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- gcd(503,286) 503=1*286 + 217
  =gcd(286, 217) 286=1*217 + 69
  =gcd(217, 69) 217 = 3*69 + 10
  = gcd(69,10) 69 = 6*10 + 9
  =gcd(10,9) 10=1*9 + 1
  = gcd(9,1) =**1**

Modular arithmetic in CS

Modular arithmetic and congruencies are used in CS:

- **Pseudorandom number generators**
- **Hash functions**
- **Cryptology**

Pseudorandom number generators

- **Some problems we want to program need to simulate a random choice.**
- **Examples: flip of a coin, roll of a dice**

We need a way to generate random outcomes

Basic problem:

- assume outcomes: 0, 1, .. N
- generate the random sequences of outcomes

- Pseudorandom number generators let us generate sequences that look random
- **Next:** linear congruential method

Pseudorandom number generators

Linear congruential method

- We choose 4 numbers:
  - the modulus m,
  - multiplier a,
  - increment c, and
  - seed x_0,

  such that $2 =< a < m$, $0 =< c < m$, $0 =< x_0 < m$.

- We generate a sequence of numbers $x_{1,}$ x_2 x_3 ... x_n ... such that $0 =< x_n < m$ for all *n* by successively using the congruence:
  - $x_{n+1} = (a.x_n + c) \bmod m$

Pseudorandom number generators

Linear congruential method:

  - $x_{n+1} = (a.x_n + c) \bmod m$

Example:

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

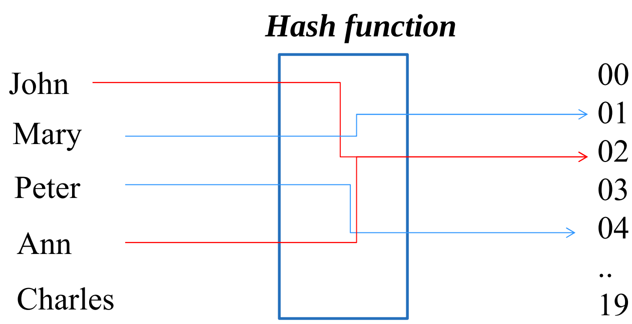
- x_1= 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- x_4= 46 mod 9 =1
- x_5 = 11 mod 9 =2
- x_6 = 18 mod 9 =0
- ....

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.**

Example:



Hash function

An example of a hash function that maps integers (including very large ones) to a subset of integers 0, 1, .. m-1 is:

h(k) = k mod m

Example: Assume we have a database of employes, each with a unique ID – a social security number that consists of 8 digits. We want to store the records in a smaller table with m entries. Using h(k) function we can map a social secutity number in the database of employes to indexes in the table.

Assume: h(k) = k mod 111

Then:

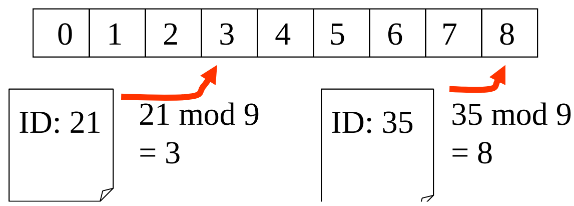
h(064212848) = 064212848 mod 111 = 14

h(037149212) = 037149212 mod 111 = 65

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 function

An example of a hash function that maps integers (including very large ones) to a subset of integers 0, 1, .. m-1 is:

h(k) = k mod m

Example: Assume we have a database of employes, each with a unique ID – a social security number that consists of 8 digits. We want to store the records in a smaller table with m entries. Using h(k) function we can map a social secutity number in the database of employes to indexes in the table.

Assume: h(k) = k mod 111

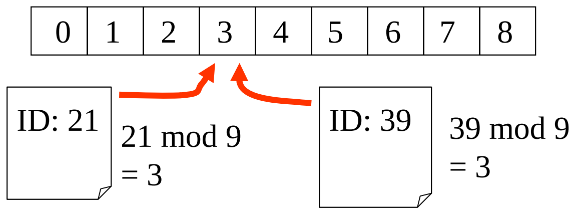
Then:

h(064212848) = 064212848 mod 111 = 14

h(037149212) = 037149212 mod 111 = 65

Hash functions

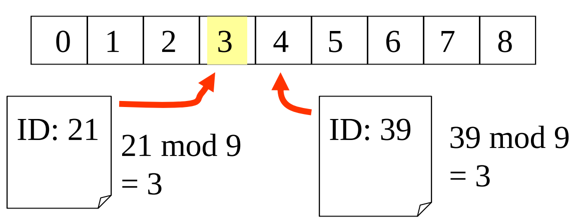
- **Problem:** two documents mapped to the same location



Hash functions

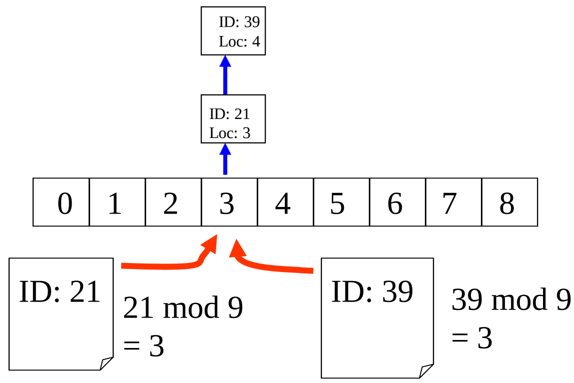
- **Solution 1:** move the next available location
  - Method is represented by a sequence of hash functions to try

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



Hash functions

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



Cryptology

Encryption of messages.

- **Ceasar cipher:**
- Shift letters in the message by 3, last three letters mapped to the first 3 letters, e.g. A is shifted to D, X is shifted to A

How to represent the idea of a shift by 3?

- There are 26 letters in the alphabet. Assign each of them a number from 0,1, 2, 3, .. 25 according to the alphabetical order.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	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

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	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

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  -

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	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

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**

  - **L 0LNH GLYFUHVH PDVK.**