Integers and division

• **Number theory** is a branch of mathematics that explores integers and their properties.

• **Integers:**
  – $\mathbb{Z}$ integers {…, -2, -1, 0, 1, 2, …}
  – $\mathbb{Z}^+$ positive integers {1, 2, …}

• Number theory has many applications within computer science, including:
  – Storage and organization of data
  – Encryption
  – Error correcting codes
  – Random numbers generators
**Division**

**Definition:** Assume 2 integers $a$ and $b$, such that $a \neq 0$ ($a$ is not equal 0). We say that $a$ divides $b$ if there is an integer $c$ such that $b = ac$. If $a$ divides $b$ we say that $a$ is a factor of $b$ and that $b$ is multiple of $a$.

- The fact that $a$ divides $b$ is denoted as $a | b$.

**Examples:**
- $4 | 24$ True or False? **True**
  - $4$ is a factor of $24$
  - $24$ is a multiple of $4$
- $3 | 7$ True or False? **False**

**Primes**

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

**Examples:** $2, 3, 5, 7, \ldots$
- $1 | 2$ and $2 | 2$, $1 | 3$ and $3 | 3$, etc
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:
• $12 = 2 \times 2 \times 3$
• $21 = 3 \times 7$

• Process of finding out factors of the product: factorization.

Primes and composites

• How to determine whether the number is a prime or a composite?
Let $n$ be a number. Then in order to determine whether it is a prime we can test:
• Approach 1: 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.
• Approach 2: 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.
• Approach 3: if any prime number $x < \sqrt{n}$ divides it. If yes it is a composite. If we test all primes $x < \sqrt{n}$ and do not find a proper divisor then $n$ is a prime.
Division

Let $a$ be an integer and $d$ a positive integer. Then there are unique integers, $q$ and $r$, with $0 \leq r < d$, 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.

Relations:
- $q = a \div d$ , $r = a \mod d$

Example: $a= 14$, $d = 3$

\[
14 = 3 \times 4 + 2 \\
14/3=3.666 \\
14 \ div \ 3 = 4 \\
14 \ mod \ 3 = 2
\]

Greatest common divisor

A systematic way to find the gcd using factorization:
- Let $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \ldots p_k^{b_k}$
- $\text{gcd}(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} p_3^{\min(a_3,b_3)} \ldots p_k^{\min(a_k,b_k)}$

Examples:
- $\text{gcd}(24,36) = ?$
- $24 = 2^2*2*3=2^3*3$
- $36= 2^2*3*3=2^2*3^2$
- $\text{gcd}(24,36) = ?$
Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \ldots p_k^{b_k}$
- $\text{gcd}(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} p_3^{\min(a_3,b_3)} \ldots p_k^{\min(a_k,b_k)}$

Examples:

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

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 $\text{lcm}(a,b)$.

Example:

- What is $\text{lcm}(12,9) = ?$
- 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 \( \text{lcm}(a,b) \).

**Example:**

- What is \( \text{lcm}(12,9) \)?
- Give me a common multiple: \( \ldots 12 \times 9 = 108 \)
- 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 \(a=p_1^{a_1}p_2^{a_2}p_3^{a_3} \ldots p_k^{a_k}\) and \(b=p_1^{b_1}p_2^{b_2}p_3^{b_3} \ldots p_k^{b_k}\)
- \(\text{lcm}(a,b)=p_1^{\max(a_1,b_1)}p_2^{\max(a_2,b_2)}p_3^{\max(a_3,b_3)} \ldots p_k^{\max(a_k,b_k)}\)

Example:

- What is \(\text{lcm}(12,9) = ?\)
- \(12 = 2^2 \times 3 = 2^2 \times 3^1\)
- \(9 = 3^2 = 3^2\)
- \(\text{lcm}(12, 9) = 2^2 \times 3^2 = 4 \times 9 = 36\)

Euclid algorithm

Finding the greatest common divisor requires factorization

- \(a=p_1^{a_1}p_2^{a_2}p_3^{a_3} \ldots p_k^{a_k}\), \(b=p_1^{b_1}p_2^{b_2}p_3^{b_3} \ldots p_k^{b_k}\)
- \(\text{gcd}(a,b)=p_1^{\min(a_1,b_1)}p_2^{\min(a_2,b_2)}p_3^{\min(a_3,b_3)} \ldots p_k^{\min(a_k,b_k)}\)

- 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? \[ ak – cbk = r \rightarrow (a-cb)k = r \rightarrow (a-cb) = r/k \] (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 \[ \rightarrow 287 = k(3b + d) \rightarrow 287/k = (3b + d) \]
- 287/k must be an integer
- But then \[ \text{gcd}(287,91) = \text{gcd}(91,14) \]

**Euclid algorithm**

- We know that \[ \text{gcd}(287,91) = \text{gcd}(91,14) \]
- But the same trick can be applied again:
  - \[ \text{gcd}(91,14) \]
  - \[ 91 = 14.6 + 7 \]
  - and therefore
    - \[ \text{gcd}(91,14)=\text{gcd}(14,7) \]

- And one more time:
  - \[ \text{gcd}(14,7) = 7 \]
  - trivial
- **The result**: \[ \text{gcd}(287,91) = \text{gcd}(91,14)=\text{gcd}(14,7) = 7 \]
Euclid algorithm

Example 1:
- Find the greatest common divisor of 666 & 558
  
  \[
  \begin{align*}
  \gcd(666,558) & = 666 = 1 \times 558 + 108 \\
  = \gcd(558,108) & = 558 = 5 \times 108 + 18 \\
  = \gcd(108,18) & = 108 = 6 \times 18 + 0 \\
  = 18
  \end{align*}
  \]

Example 2:
- Find the greatest common divisor of 286 & 503:
  
  \[
  \begin{align*}
  \gcd(503,286) & = 503 = \\
  & =
  \end{align*}
  \]
Euclid algorithm

Example 2:
• Find the greatest common divisor of 286 & 503:

  • \( \gcd(503, 286) \)
  \[
  503 = 1 \times 286 + 217
  \]
  \( = \gcd(286, 217) \)
  \[
  286 = 1 \times 217 + 69
  \]
  \( = \gcd(217, 69) \)
  \[
  217 = 3 \times 69 + 10
  \]
  \( = \gcd(69, 10) \)
  \[
  69 = 6 \times 10 + 9
  \]
  \( = \gcd(10, 9) \)
  \[
  10 = 1 \times 9 + 1
  \]
  \( = \gcd(9, 1) = 1 \)
Modular arithmetic

- In computer science we often care about the remainder of an integer when it is divided by some positive integer.

**Problem:** Assume that it is a midnight. What is the time on the 24 hour clock after 50 hours?

**Answer:** the result is 2am

How did we arrive to the result:
- Divide 50 with 24. The reminder is the time on the 24 hour clock.
  - $50 = 2 \times 24 + 2$
  - so the result is 2am.

Congruency

**Definition:** If $a$ and $b$ are integers and $m$ is a positive integer, then $a$ is congruent to $b$ modulo $n$ if $m$ divides $a-b$. We use the notation $a = b \pmod{m}$ to denote the congruency. If $a$ and $b$ are not congruent we write $a \not\equiv b \pmod{m}$.

**Example:**
- Determine if 17 is congruent to 5 modulo 6?
**Congruency**

**Theorem.** If a and b are integers and m a positive integer. Then a=b (mod m) if and only if a mod m = b mod b.

**Example:**
- Determine if 17 is congruent to 5 modulo 6?
  - 17 mod 6 = 5
  - 5 mod 6 = 5
  - Thus 17 is congruent to 5 modulo 6.

---

**Congruencies**

**Theorem 1.** Let m be a positive integer. The integers a and b are congruent modulo m if and only if there exists an integer k such that a=b+mk.

**Theorem 2.** Let m be a positive integer. If a=b (mod m) and c=d (mod m) then:

\[ a+c = b+d \pmod{m} \]
\[ ac = bd \pmod{m} \]
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 \( 2 \leq a < m, 0 \leq c < m, 0 \leq x_0 < m \).

- We generate a sequence of numbers \( x_1, x_2, x_3, \ldots \) such that \( 0 \leq x_n < m \) for all \( n \) by successively using the congruence:
  - \( x_{n+1} = (a \cdot x_n + c) \mod m \)

Example:
- Assume: \( m = 9, a = 7, c = 4, x_0 = 3 \)
  - \( x_1 = 7 \cdot 3 + 4 \mod 9 = 25 \mod 9 = 7 \)
  - \( x_2 = 53 \mod 9 = 8 \)
  - \( x_3 = 60 \mod 9 = 6 \)
  - \( x_4 = 46 \mod 9 = 1 \)
  - \( x_5 = 11 \mod 9 = 2 \)
  - \( x_6 = 18 \mod 9 = 0 \)
  - \ldots
**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:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Hash Value</th>
<th>Hash Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td></td>
<td>00</td>
</tr>
<tr>
<td>Mary</td>
<td></td>
<td>01</td>
</tr>
<tr>
<td>Peter</td>
<td></td>
<td>02</td>
</tr>
<tr>
<td>Ann</td>
<td></td>
<td>03</td>
</tr>
<tr>
<td>Charles</td>
<td></td>
<td>04</td>
</tr>
<tr>
<td></td>
<td></td>
<td>..</td>
</tr>
<tr>
<td></td>
<td></td>
<td>19</td>
</tr>
</tbody>
</table>

**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 employees, 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 security number in the database of employees to indexes in the table.

**Assume:** h(k) = k mod 111

**Then:**

\[ h(064212848) = 064212848 \mod 111 = 14 \]
\[ h(037149212) = 037149212 \mod 111 = 65 \]