DMA: Properties of integers

Laura Mančinska,
Institut for Matematiske Fag

UNIVERSITY OF COPENHAGEN

Plan for today

- Quotients, remainders, mod-d function
- Divisors and multiples
- Greatest common divisor (GCD)
- Euclidean Algorithm
- Least common multiple (LCM)
- Primes

- Prime factorization
- Base-b expansion

Reading: Section 1.4 from KBR

Quotient and remainder

Thm. Let $m \in \mathbb{Z}$ be an integer and $d \in \mathbb{Z}^+$ be a positive integer. Then there exists $0 \leq r < d$ and $q \in \mathbb{Z}$ such that

$$m = qd + r$$

q is called the quotient

r is called the remainder

Examples

$m = 12, d = 5$

$m = 5, d = 12$

$m = -12, d = 5$

$m = -5, d = 12$

Quotient and remainder

Thm. Let $m \in \mathbb{Z}$ be an integer and $d \in \mathbb{Z}^+$ be a positive integer. Then there exists $0 \leq r < d$ and $q \in \mathbb{Z}$ such that

$$m = qd + r$$

q is called the quotient

r is called the remainder

Examples

$m = 12, d = 5$	$12 = 2 \cdot 5 + 2$
$m = 5, d = 12$	$5 = 0 \cdot 12 + 5$
$m = -12, d = 5$	$-12 = (-3) \cdot 5 + 3$
$m = -5, d = 12$	$-5 = (-1) \cdot 12 + 7$

The mod-d function

Let $m \in \mathbb{Z}^+$, $d \in \mathbb{Z}^+$. Suppose $0 \leq r < d, q \in \mathbb{Z}$ and we have

$$m = qd + r$$

Def. The mod-d function returns the remainder. That is

$$m \bmod d \stackrel{\text{def}}{=} r$$

- mod-d function is implemented in most programming languages
- In F#, python, C: `m % d`
- Functionality for $m, d \leq 0$ can differ

Examples: the mod-d function

Def. The mod-d function returns the remainder. That is

$$m \bmod d \stackrel{\text{def}}{=} r$$

Where $\mathbf{0 \leq r < d}, q \in \mathbb{Z}$ and $m = qd + r$.

Compute the following

- 3 mod 2
- $2n$ mod 2, where $n \in \mathbb{Z}^+$
- Express the solution using the appropriate mod-d function.
  - It is 9:00am. What time will it be in 100 hours?
  - What day of the week will it be in 26 days?

Divisors

Let $m \in \mathbb{Z},\ d \in \mathbb{Z}^+$. Suppose $0 \leq r < d, q \in \mathbb{Z}$ and we have

$$m = qd + r$$

Def. (terminology) If $r = 0$, we say that

- m is a multiple of d and
- d is a divisor of m.
- We write $d|m$; pronounced "d divides m"

- If $r \neq 0$, we write $d \nmid m$; pronounced "d does not divide m"

Properties of divisors

Let $m, n \in \mathbb{Z},\ d \in \mathbb{Z}^+$.

1. $m|m$, $1|m$ and $d|0$
2. If $d|m$ or $d|n$ then $d|(mn)$
3. If $d|m$ and $d|n$ then $d|(m+n)$
4. If $d|m$ and $d|n$ then $d|(m-n)$
5. **(generalizes 3. and 4.)**
   If $d|m$ and $d|n$ then $d|(m-qn)$ for any $q \in \mathbb{Z}$
6. **(transitivity)** If $d|m$ and $m|n$ then $d|n$

Greatest common divisor (GCD)

Let $a, b, d \in \mathbb{Z}^{+}$. Integer d is a common divisor of a and b if $d|a$ and $d|b$.

Def.(GCD) We say that d is the greatest common divisor of a and b, denoted $\mathbf{GCD(}\boldsymbol{a}, \boldsymbol{b}\mathbf{)}$, if d is the largest of the common divisors of a and b.

Determine GCD(36,30)

Euclidean algorithm provides a very efficient method for finding GCD(a, b).

Finding GCD(a, b) (warm-up to Euclidean algorithm)

Let $a, b \in \mathbb{Z}^+$ and $a \geq b$.

- Recall: $a \bmod b = r$, where $a = qb + r$ and $0 \leq r < b$.

- If $d|a$ and $d|b$ then $d|(a \bmod b)$
  - Since $a \bmod b = r = a - qb$ (use Property 5)

- If $d|b$ and $d|(a \bmod b)$ then $d|a$
  - Since $a = qb + (a \bmod b) = (a \bmod b) - (-q)b$ (use Prop. 5)

- Common_divisors(a, b)=Common_divisors($a \bmod b, b$)
  - GCD(a, b)=GCD(b,$a \bmod b$)

Euclidean algorithm

Let $a, b \in \mathbb{Z}^+$ and $a \geq b$.

Step 1: $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, a \bmod b)$ $\quad a = q_1 b + r_1$

Step 2: $\mathrm{GCD}(b, r_1) = \mathrm{GCD}(r_1, b \bmod r_1)$ $\quad b = q_2 r_1 + r_2$

Step 3: $\mathrm{GCD}(r_1, r_2) = \mathrm{GCD}(r_2, r_1 \bmod r_2)$ $\quad r_1 = q_3 r_2 + r_3$

…

Stop when $r_k = 0$

$$\mathbf{GCD}(\boldsymbol{a}, \boldsymbol{b}) = \boldsymbol{r_{k-1}}$$

Properties of GCD

Thm. Let $a, b \in \mathbb{Z}^+$. If $d = \mathrm{GCD}(a, b)$ then there exist $s, t \in \mathbb{Z}$ such that

$$d = sa + tb$$

- Extended version of Euclidean algorithm finds s, t.

Least common multiple (LCM)

Let $a, b, m \in \mathbb{Z}^+$. Integer m is a common multiple of a and b if $a|m$ and $b|m$.

Def.(LCM) We say that m is the least common multiple of a and b, denoted $\mathbf{LCM(a, b)}$, if m is the smallest of all the common multiples of a and b.

Determine LCM(12,15)

Thm. Let $a, b \in \mathbb{Z}^+$. Then

$$\mathrm{LCM}(a, b) = \frac{ab}{\mathrm{GCD}(a, b)}$$

How to find $\mathrm{LCM}(a, b)$?

Primes

Primes

Def. We say that a positive integer $p > 1$ is a prime, if the only divisors of p are p and 1. Otherwise, we say that p is composite.

Determine which ones are primes: 1, 2, 3, 12, 13, 37, 51.

How to test if $m \in \mathbb{Z}^+$ is a prime?

```
Test(m)
    If (m=1) then
        return False
    For  d=2 thru m-1
        if (m % d) = 0 then
            return False
    return True
```

- Worst case complexity $\Theta(m)$.
- If m is not a prime we can factor it as $m = d_1 d_2$, where $d_1 \geq d_2 \geq 2$. Note that $d_2 \leq \sqrt{m}$.

How to test if $m \in \mathbb{Z}^+$ is a prime?

```
Test(m)
    If (m=1) then
        return False
    For d=2 thru Floor(Sqrt(m))
        if (m % d) = 0 then
            return False
    return True
```

- Worst case complexity $\Theta(\sqrt{m})$. Not efficient.
- If $2 \nmid n$, only need to check odd numbers.
- Suffices to check only primes $\leq \sqrt{m}$ (Sieve of Eratosthenes)

How to test if $m \in \mathbb{Z}^+$ is a prime?

- Suffices to check only primes $\leq \sqrt{m}$ (Sieve of Eratosthenes)
  - This requires pre-computation of primes
- There exist efficient probabilistic algorithms based on number-theoretic properties.
  - These can yield inconclusive or potentially wrong answer.
- In 2002, Agrawal, Kayal, and Saxena came up with an efficient deterministic test.
- Not currently used in practice.

Prime factorization

Thm. (prime factorization) Any $m \in \mathbb{Z}^+$ can be uniquely expressed as

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}$$

Where $p_1 < p_2 < \cdots < p_k$ are primes and all the a_i's are positive integers.

Thm. If d is a divisor of m, then $d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where $0 \leq b_i \leq a_i$ for all i.

Prime factorization and GCD/LCM

Thm. Let $a, b \in \mathbb{Z}^+$ and let

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ and } p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

be their prime factorizations* with $a_i, b_i \in \mathbb{Z}$. Then

$$\mathrm{GCD}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$$

$$\mathrm{LCM}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)}$$

Representing integers in different bases

Base-b expansion

- Commonly use decimal (base-10) expansion:

$$726 = 7 \cdot 10^2 + 2 \cdot 10 + 6 \cdot 10^0$$

Thm. Let $b > 1$ be an integer. Any $n \in \mathbb{Z}^+$ can be uniquely expressed as

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_1 b^1 + d_0 b^0$$

where $d_k \neq 0$ and $0 \leq d_i < b$ for all i.

We call

$$\boldsymbol{d_k d_{k-1} \ldots d_1 d_0}$$

the base-b expansion of n.

- Sometimes we write $(d_k d_{k-1} \ldots d_1 d_0)_{\boldsymbol{b}}$ to indicate that base-b is used.

Digits in base-b expansion

- Each of the digits d_i in $(d_k d_{k-1} \dots d_1 d_0)_{\boldsymbol{b}}$ take one out of b different values
- In decimal: $d_i \in \{0,1,2, \dots, 9\}$
- Common bases are 2(binary), 8(octal), 16(**hex**adecimal)
    - In binary: $d_i \in \{0,1\}$
    - In base-3: $d_i \in \{0,1,2\}$
    - In octal (base-8): $d_i \in \{0,1, \dots, 7\}$
    - In hex: $d_i \in \{0,1, \dots, 8,9, a, b, c, d, e, f\}$

Find the decimal expansion of the following

- $(101)_{\mathbf{2}}$
- $(101)_{\mathbf{3}}$
- $(102)_{\mathbf{3}}$
- $(102)_{\mathbf{2}}$
- $(1a)_{\mathbf{16}}$
- $(1f)_{\mathbf{16}}$
- $(1g)_{\mathbf{16}}$

Find the decimal expansion of the following

- $(101)_{\mathbf{2}}$
- $(101)_{\mathbf{3}}$
- $(102)_{\mathbf{3}}$
- $(102)_{\mathbf{2}}$ not valid!
- $(1a)_{\mathbf{16}}$
- $(1f)_{\mathbf{16}}$
- $(1g)_{\mathbf{16}}$ not valid!

Finding base-b expansion

Let $n \in \mathbb{Z}^+$ and $b > 1$.

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_1 b^1 + d_0$$
$$= (d_k b^{k-1} + d_{k-1} b^{k-2} + \cdots + d_1 b^0) b + d_0$$

$$\boldsymbol{d_0 = n \bmod b}$$

$$q_1 = d_k b^{k-1} + d_{k-1} b^{k-2} + \cdots d_2 b^1 + d_1$$
$$= (d_k b^{k-2} + d_{k-1} b^{k-3} + \cdots d_2) b + d_1$$

$$\boldsymbol{d_1 = q_1 \bmod b}$$

…

Keep going until $q_i = 0$

How to find base-b expansion?

```
Expand(n)
    quotient ← n
    k ← 0
    While quotient≠0
        d_k = quotient % B
        quotient ← (quotient - d_k)/B
        k ← k+1
    return [d_{k-1},…,d_1,d_0]
```