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

Reading: Section 1.4 from KBR

Quotient and remainder

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

$$m = qd + r$$

q is called the quotient

r is called the remainder

The mod-d function

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

$$m = qd + r$$

for $0 \leq r < d, q \in \mathbb{Z}$.

Def. The mod-d function returns the remainder r

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

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

The mod-d function: Examples

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

$$m = qd + r$$

for $0 \leq r < d, q \in \mathbb{Z}$.

Def. The mod-d function returns the remainder r

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

Task: 1) Find the quotient, q, and the remainder, r

2) If $m, d > 0$, compute $m \bmod d$

- $m = 12, d = 5$
- $m = 5, d = 12$
- $m = -12, d = 5$
- $m = -5, d = 12$

Terminology: divisors, multiples, $d|m$

Let $d \in \mathbb{Z}^+, m \in \mathbb{Z}$. Write m as
$$m = qd + r$$
for $0 \leq r < d, q \in \mathbb{Z}$.

Def. If $r = 0$, we say that

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

If $r \neq 0$, we write $d \nmid m$ and say "d does not divide m"

Properties of divisors

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

1. $d|d$, $1|m$ 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 $d|(sm+tn)$ for any $s, t \in \mathbb{Z}$
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 $d|b$.

Divisors of 36:

Divisors of 30:

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

Task: Determine GCD(36,30)

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

What does it mean that findGCD(a, b) is an <u>efficient</u> algorithm?

- Suppose $a \geq b$

Answer: findGCD(a, b) has worst-case running time of

1) $O(\text{poly}(\log a))$ i.e. $O((\log a)^k)$ for some $k \in \mathbb{Z}^+$
2) $O(\text{poly}(a))$ i.e. $O(a^k)$ for some $k \in \mathbb{Z}^+$
3) $O(2^a)$

Idea behind the Euclidean algorithm

Thm. Let $a, b \in \mathbb{Z}^+$. Assume $a \geq b$.
Then $\texttt{Common\_divisors}(a, b) = \texttt{Common\_divisors}(a \bmod b, b)$

and thus

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(a \bmod b, b)$$

Euclidean algorithm

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

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

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

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

…

Stop when $r_k = 0$

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

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 $\mathbf{LCM}(\boldsymbol{a}, \boldsymbol{b})$, if m is the smallest of all the common multiples of a and b.

Task: Compute LCM(12,15)

- Multiples of 12:

- Multiples of 15:

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.

Task: Compute LCM(12,15)

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

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

- How can we find LCM(12,15) more efficiently?

Primes and prime factorization

Def. A positive integer $p > 1$ is a prime, if its only divisors are p and 1.

Examples: 2, 5, 7, 13, 47

Non-examples: 0, 1, -2, 4, 12, 51

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

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

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

Prime factorization contains a lot of information

Consider the prime factorization of m:

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

- The divisors of m can be written as

$$d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

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

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

be their prime factorizations* with $a_i, b_i \in \mathbb{Z}^+ \cup \{0\}$. Then

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

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

What we saw today

- Division with remainders: $m = qd + r$
- Mod-d function (Ex: $17 \bmod 5 = 2$)
- (Common) divisors, (common) multiples
- GCD and LCM and how to calculate them
  - Euclidean algorithm
- Primes and prime factorization