CS102A - Auxiliaries for Assignment 3

Greatest common divisor

Hengcheng ZHU

Southern University of Science and Technology
Department of Computer Science and Engineering

March 31, 2019

Acknowledgment & Remark

The content of these slides are based on the materials in

- CS201 Discrete Mathematics for Computer Science
- By Prof. Qi Wang

These content will not be covered by the final exam of CS102A. It is just for you to solve A3Q1.

I'm sorry for not being able to block these out of scope content from being your assignment. What I can do is to help you guys conquer them.

Divisibility

If $a, b \in \mathbb{Z}$ and $a \neq 0$, we say a divides b

- If $\exists c \in \mathbb{Z}$ $s.t.$ $b = ac$
- Or equivalently $\frac{b}{a} \in \mathbb{Z}$

We also say

- a is a divisor/factor of b
- b is a multiple of a

Notations

- a divides b: $a \mid b$
- a does not divide b: $a \nmid b$

Divisibility - Properties

For $a, b, c \in \mathbb{Z}$

1. $a \mid b \wedge a \mid c \implies a \mid (b + c)$
   - Let $b = k_1 a,\ c = k_2 a$ then $b + c = (k_1 + k_2)a$
2. $a \mid b \implies \forall c, a \mid bc$
   - Let $b = k_1 a$ then $bc = k_1 c \cdot a$
3. $a \mid b \wedge b \mid c \implies a \mid c$
   - Let $b = k_1 a,\ c = k_2 b$ then $c = k_1 k_2 \cdot a$

Corollary: For $a, b, c \in \mathbb{Z}$ and $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $\forall m, n \in \mathbb{Z},\ a \mid (mb + nc)$

Greatest Common Divisor (GCD)

For $a, b \in \mathbb{Z}$, The largest integer d such that $d \mid a$ and $d \mid b$ is the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$

For primes $p_1, p_2, \ldots, p_n$
Let $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \ldots \cdot p_n^{\min(a_n, b_n)}$$

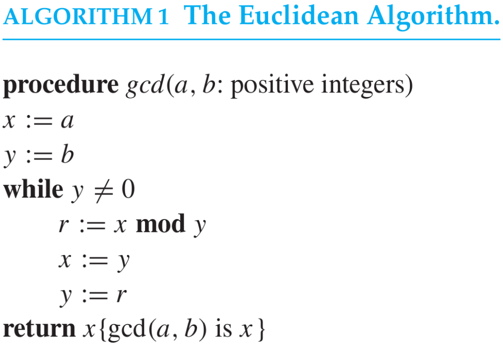
Euclidean Algorithm

Lemma: For $a, b, c \in \mathbb{Z}$ and $a = bq + r$.
Then $\gcd(a, b) = \gcd(b, r)$

Example: $\gcd(287, 91)$

- $287 = 91 \cdot 3 + 14$
- $91 = 14 \cdot 6 + 7$
- $14 = 7 \cdot 2 + 0$

$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$



ALGORITHM 1 The Euclidean Algorithm.

```
procedure gcd($a$, $b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ mod $y$
    $x := y$
    $y := r$
return $x$ {gcd($a$, $b$) is $x$}
```

Euclidean Algorithm - Correctness

Lemma: For $a, b, c \in \mathbb{Z}$ and $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$

Proof.

- Suppose that $d \mid a$ and $d \mid b$. Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be a common divisor of b and r.
- Suppose that $d \mid b$ and $d \mid r$. Then d also divides $bq + r = a$. Hence, any common divisor of b and r must also be a common divisor of a and b.
- Q.E.D.

Euclidean Algorithm in Java

```java
public static int gcd(int a, int b) {
    // Check if a, b are positive here.
    int x = a;
    int y = b;
    while(y != 0) {
        int r = x % y;
        x = y;
        y = r;
    }
    return x;
}
```

Thanks