Number Theory: The Euclidean Algorithm

Ian Ludden

lan Ludden Number Theory: The Euclidean Algorithm

.

< 回 > < 三 > < 三 >

• Recall the definitions of gcd and lcm.

- Recall the definitions of gcd and lcm.
- Describe the Euclidean algorithm and reproduce its pseudocode.

- Recall the definitions of gcd and lcm.
- Describe the Euclidean algorithm and reproduce its pseudocode.
- Apply the Euclidean algorithm to compute the gcd of two larger integers.

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

Definition

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a **greatest common divisor** (gcd) of *a* and *b* if **1** $c \mid a$ and $c \mid b$ (*c* is a common divisor of *a* and *b*), and

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

- 1 $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
- 2 for every common divisor d of a and b, $d \mid c$.

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

- 1 $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
- 2 for every common divisor d of a and b, $d \mid c$.

Definition

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

- 1 $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
- 2 for every common divisor d of a and b, $d \mid c$.

Examples

Definition

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

- 1 $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
- 2 for every common divisor d of a and b, $d \mid c$.

Examples

• gcd(8, 12) = 4

Definition

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

- 1 $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and
- 2 for every common divisor d of a and b, $d \mid c$.

Examples

- gcd(8, 12) = 4
- gcd(-35, 20) = 5

Definition

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

1 $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and

2 for every common divisor d of a and b, $d \mid c$.

Examples

- gcd(8, 12) = 4
- gcd(-35, 20) = 5
- gcd(a, b) = gcd(b, a)

Definition

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

1 $c \mid a$ and $c \mid b$ (c is a common divisor of a and b), and

2 for every common divisor d of a and b, $d \mid c$.

Examples

- gcd(8, 12) = 4
- gcd(-35, 20) = 5
- gcd(a, b) = gcd(b, a)
- For any integer $a \neq 0$, gcd(a, 0) = |a|

YneZ, nO.

0=n.().

・ロト ・ 戸 ト ・ ヨ ト ・ ヨ ト

For any integers *a* and *b*, with $a \neq 0$ or $b \neq 0$, $c \in \mathbb{Z}^+$ is called a *greatest common divisor* (gcd) of *a* and *b* if

1 $c \mid a \text{ and } c \mid b (c \text{ is a common divisor of } a \text{ and } b)$, and

2 for every common divisor d of a and b, $d \mid c$.

Examples

- gcd(8, 12) = 4
- gcd(-35, 20) = 5
- gcd(a, b) = gcd(b, a)
- For any integer $a \neq 0$, gcd(a, 0) = |a|
- gcd(0,0) is undefined

For any *positive* integers *a* and *b*, $c \in \mathbb{Z}^+$ is called a *least common multiple* (lcm) of *a* and *b* if

For any *positive* integers *a* and *b*, $c \in \mathbb{Z}^+$ is called a *least common multiple* (lcm) of *a* and *b* if

1 $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and

For any *positive* integers *a* and *b*, $c \in \mathbb{Z}^+$ is called a *least common multiple* (lcm) of *a* and *b* if

- 1 $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
- 2 for every positive common multiple *d* of *a* and *b*, $c \leq d$.

For any *positive* integers *a* and *b*, $c \in \mathbb{Z}^+$ is called a *least common multiple* (lcm) of *a* and *b* if

- 1 $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
- 2 for every positive common multiple *d* of *a* and *b*, $c \leq d$.

Least Common Multiple

Definition

For any *positive* integers *a* and *b*, $c \in \mathbb{Z}^+$ is called a *least common multiple* (lcm) of *a* and *b* if

- 1 $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
- **2** for every positive common multiple *d* of *a* and *b*, $c \leq d$.

Theorem

For all $a, b \in \mathbb{Z}^+$, $ab = lcm(a, b) \cdot gcd(a, b)$.

・ 同 ト ・ ヨ ト ・ ヨ ト

For any *positive* integers *a* and *b*, $c \in \mathbb{Z}^+$ is called a *least common multiple* (lcm) of *a* and *b* if

- 1 $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
- 2 for every positive common multiple *d* of *a* and *b*, $c \leq d$.

Theorem

For all $a, b \in \mathbb{Z}^+$, $ab = lcm(a, b) \cdot gcd(a, b)$.

Examples • a = 4, b = 7 gcd (4, 7) = 1 "relatively prime" $I_{cm}(4, 7) = \frac{4.7}{1} = 28$

・ロト ・ 四ト ・ ヨト・

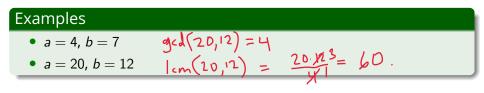
Э

For any *positive* integers *a* and *b*, $c \in \mathbb{Z}^+$ is called a *least common multiple* (lcm) of *a* and *b* if

- 1 $a \mid c$ and $b \mid c$ (c is a common multiple of a and b), and
- 2 for every positive common multiple *d* of *a* and *b*, $c \leq d$.

Theorem

For all $a, b \in \mathbb{Z}^+$, $ab = lcm(a, b) \cdot gcd(a, b)$.



ヘロト 人間 ト 人 ヨト 人 ヨト

By comparing prime factorizations (slow) a = |68, b=228 $a = 2^3 \cdot 3^1 \cdot 7^1 \cdot 1^9$ $b = 2^3 \cdot 3^1 \cdot 7^1 \cdot 1^9$ a = |2

э

- By comparing prime factorizations (slow)
- By the Euclidean algorithm (fast, easy to do by hand)

The Division Algorithm, Revisited

Theorem

For any integers a and b, where b > 0, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

- 1 a = bq + r and
- **2** $0 \le r < b$.

The Division Algorithm, Revisited

Theorem

For any integers a and b, where b > 0, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

- 1 a = bq + r and
- **2** $0 \le r < b$.

Claim

For any integers a, b, q, and r, with b positive, if a = bq + r, then gcd(a, b) = gcd(b, r).

The Division Algorithm, Revisited

Theorem

For any integers a and b, where b > 0, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

- 1 a = bq + r and
- **2** $0 \le r < b$.

Claim

For any integers a, b, q, and r, with b positive, if a = bq + r, then gcd(a, b) = gcd(b, r).

See textbook, Section 4.6, for proof of claim $n \mid \alpha \quad and \quad (h \mid b) \Rightarrow n \mid (b_2) \Rightarrow n \mid (a-b_2) \Rightarrow n \mid -$

The Euclidean algorithm

Repeatedly apply the division algorithm and the claim

< 回 > < 三 > < 三 > >

```
"function"
procedure gcd(a, b) \mathfrak{gl}_{b}
     r := remainder(a, b) \alpha = bq + r
     if r == 0
                                              gcd(a,b) \leq q
qcd(a,b) \leq b
         return b d = b_q + 0
     else
         return gcd(b, r)
 recursion
```

3

何 ト イ ヨ ト イ ヨ ト

```
procedure gcd(a, b)
r := remainder(a, b)
if r == 0
return b
else
return gcd(b, r)
```

Example a = 168, b = 456

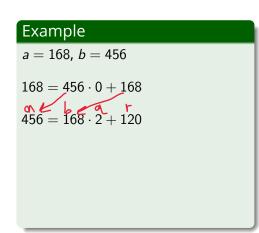
イロト イポト イヨト イヨト

```
procedure gcd(a, b)
r := remainder(a, b)
if r == 0
return b
else
return gcd(b, r)
```

Example a = 168, b = 456 $168 = 456 \cdot 0 + 168$

▲□ ▶ ▲ □ ▶ ▲ □ ▶

```
procedure gcd(a, b)
r := remainder(a, b)
if r == 0
return b
else
return gcd(b, r)
```



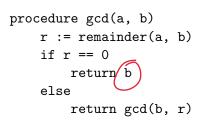
<ロト < 四ト < 回ト < ヨト

```
procedure gcd(a, b)
r := remainder(a, b)
if r == 0
return b
else
return gcd(b, r)
```

Example	
<i>a</i> = 168, <i>b</i> = 456	
$168 = 456 \cdot 0 + 168$	
$456 = 168 \cdot 2 + 120$	
$168 = 120 \cdot 1 + 48$	

```
procedure gcd(a, b)
r := remainder(a, b)
if r == 0
return b
else
return gcd(b, r)
```

Example	
<i>a</i> = 168, <i>b</i> = 456	
$168 = 456 \cdot 0 + 168$	
$456 = 168 \cdot 2 + 120$	
$168 = 120 \cdot 1 + 48$	
$120 = 48 \cdot 2 + 24$	



Example	
<i>a</i> = 168, <i>b</i> = 456	
$168 = 456 \cdot 0 + 168$	
$456 = 168 \cdot 2 + 120$	
$168 = 120 \cdot 1 + 48$	
$120 = 48 \cdot 2 + 24$	
48 = 24 2 + 0	

- Recall the definitions of gcd and lcm.
- Describe the Euclidean algorithm and reproduce its pseudocode.
- Apply the Euclidean algorithm to compute the gcd of two larger integers.