§35 Greatest Common Divisor

Tom Lewis

Fall Term 2010
Outline

1. The gcd

2. The Euclidean algorithm

3. An important theorem
Definition (Common divisor)

Let \( a, b \in \mathbb{Z} \). We call an integer \( d \) a common divisor of \( a \) and \( b \) provided that \( d \mid a \) and \( d \mid b \).

Example

Let \( a = 18 \) and \( b = 60 \). The divisors of 18 are \( \pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18 \).

The divisors of 60 are \( \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60 \).

The common divisors are \( \pm 1, \pm 2, \pm 3, \) and \( \pm 6 \).
The gcd

**Definition (Common divisor)**

Let $a, b \in \mathbb{Z}$. We call an integer $d$ a **common divisor** of $a$ and $b$ provided that $d|a$ and $d|b$.

**Example**

Let $a = 18$ and $b = 60$. The divisors of 18 are

$$\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18.$$  

The divisors of 60 are

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60.$$  

The common divisors are $\pm 1, \pm 2, \pm 3$, and $\pm 6$.  

Tom Lewis ()  
§35 Greatest Common Divisor  
Fall Term 2010  
3 / 10
Definition (Greatest common divisor)

Let $a, b \in \mathbb{Z}$. We call an integer $d$ the greatest common divisor of $a$ and $b$ provided that

The greatest common divisor of $a$ and $b$ is denoted by $\text{gcd}(a, b)$. 

Example

Since the common divisors of 18 and 60 are $\pm 1$, $\pm 2$, $\pm 3$, and $\pm 6$, clearly their $\text{gcd}(18, 60) = 6$. 
Definition (Greatest common divisor)

Let \( a, b \in \mathbb{Z} \). We call an integer \( d \) the greatest common divisor of \( a \) and \( b \) provided that

- \( d \) is a common divisor of \( a \) and \( b \) and

The greatest common divisor of \( a \) and \( b \) is denoted by \( \text{gcd}(a, b) \).
Definition (Greatest common divisor)

Let $a, b \in \mathbb{Z}$. We call an integer $d$ the greatest common divisor of $a$ and $b$ provided that

- $d$ is a common divisor of $a$ and $b$ and
- if $e$ is any common divisor of $a$ and $b$, then $e \leq d$.

The greatest common divisor of $a$ and $b$ is denoted by $\gcd(a, b)$. 

Example

Since the common divisors of 18 and 60 are $\pm 1, \pm 2, \pm 3,$ and $\pm 6$, clearly their $\gcd(18, 60) = 6$. 

Tom Lewis () §35 Greatest Common Divisor Fall Term 2010 4 / 10
Definition (Greatest common divisor)

Let $a, b \in \mathbb{Z}$. We call an integer $d$ the greatest common divisor of $a$ and $b$ provided that

- $d$ is a common divisor of $a$ and $b$ and
- if $e$ is any common divisor of $a$ and $b$, then $e \leq d$.

The greatest common divisor of $a$ and $b$ is denoted by $\gcd(a, b)$.

Example

Since the common divisors of 18 and 60 are

$\pm 1, \pm 2, \pm 3, \text{ and } \pm 6,$

clearly their $\gcd(18, 60) = 6$. 
Theorem

Let $a$ and $b$ be positive integers. Then

$$\gcd(a, b) = \gcd(b, a \mod b)$$
Problem

Find $\gcd(15, 40)$. 
The Euclidean algorithm

Problem

Find \( \gcd(15, 40) \).

Problem

Find \( \gcd(3528, 540) \).
The Euclidean algorithm

§35 Greatest Common Divisor

Fall Term 2010
From Wikipedia

In The Simpsons episode *That 90’s Show*, Homer defines “GRUNGE” as Guitar Rock Utilizing Nihilist Grunge Energy.

---

The Euclidean algorithm

Here is the pseudo-code for Euclid’s algorithm:

```plaintext
Euclid(a, b)
{
    while (b not 0)
    {
        interchange(a, b)
        b := b mod a
    }
    return(a)
}
```
### The Euclidean algorithm

Here is the pseudo-code for Euclid’s algorithm:

```plaintext
Euclid(a, b) {
    while (b not 0) {
        interchange(a, b)
        b := b mod a
    }
    return(a)
}
```

### From Wikipedia

In the Simpsons episode *That 90's Show*, Homer defines “GRUNGE” as Guitar Rock Utilizing Nihilist Grunge Energy.
Theorem

Let $a$ and $b$ be integers, not both zero. The smallest positive integer of the form $ax + by$, where $x$ and $y$ are integers, is $\gcd(a, b)$. 

Problem

Find $x$ and $y$ such that $3528x + 540y = \gcd(3528, 540)$. 

Tom Lewis () §35 Greatest Common Divisor Fall Term 2010 9 / 10
Theorem

Let $a$ and $b$ be integers, not both zero. The smallest positive integer of the form $ax + by$, where $x$ and $y$ are integers, is $\gcd(a, b)$.

Problem

Find $x$ and $y$ such that

$$3528x + 540y = \gcd(3528, 540).$$
Definition

Let $a$ and $b$ be integers. We call $a$ and $b$ relatively prime provided $\gcd(a, b) = 1$. 
Definition
Let $a$ and $b$ be integers. We call $a$ and $b$ \textbf{relatively prime} provided $\gcd(a, b) = 1$.

Corollary
Let $a$ and $b$ be integers. There exist integers $x$ and $y$ such that $ax + by = 1$ if and only if $a$ and $b$ are relatively prime.
Definition
Let $a$ and $b$ be integers. We call $a$ and $b$ relatively prime provided $\gcd(a, b) = 1$.

Corollary
Let $a$ and $b$ be integers. There exist integers $x$ and $y$ such that $ax + by = 1$ if and only if $a$ and $b$ are relatively prime.

Theorem
Let $a$ and $b$ be integers, not both integers. Let $d = \gcd(a, b)$. If $e$ is a common divisor of $a$ and $b$, then $e \mid d$. 