Introduction to Proofs - Number Theory
Euclidean GCD algorithm

Prof Mike Pawliuk

UTM

August 13, 2020

Slides available at: mikepawliuk.ca

Learning Objectives (for this video)

By the end of this video, participants should be able to:

1. Apply the Euclidean GCD algorithm.
2. Find witnesses to Bezout's Identity.

Motivation

In the previous video we explored the definitions of GCD, and now we will see a fast way for computing common factors.

This method can be reversed to solve equations like $84x + 35y = 7$.

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a,b) = \gcd(a-kb, b).$$

a	b	k	$a-kb$	$\gcd(a,b)$	$\gcd(a-kb,b)$
50	15	1		5	
50	15	2		5	
50	15	3		5	

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

a	b	k	$a - kb$	$\gcd(a, b)$	$\gcd(a - kb, b)$
50	15	1	35	5	
50	15	2		5	
50	15	3		5	

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

a	b	k	$a - kb$	$\gcd(a, b)$	$\gcd(a - kb, b)$
50	15	1	35	5	5
50	15	2		5	
50	15	3		5	

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

a	b	k	$a - kb$	$\gcd(a, b)$	$\gcd(a - kb, b)$
50	15	1	35	5	5
50	15	2	20	5	
50	15	3		5	

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

a	b	k	$a - kb$	$\gcd(a, b)$	$\gcd(a - kb, b)$
50	15	1	35	5	5
50	15	2	20	5	5
50	15	3		5	

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

a	b	k	$a - kb$	$\gcd(a, b)$	$\gcd(a - kb, b)$
50	15	1	35	5	5
50	15	2	20	5	5
50	15	3	5	5	

4. Two GCD lemmas

Lemma 1

Let a, b be integers. If $d|a$ and $d|b$ then $d|(a-b)$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

a	b	k	$a - kb$	$\gcd(a, b)$	$\gcd(a - kb, b)$
50	15	1	35	5	5
50	15	2	20	5	5
50	15	3	5	5	5

4. Two GCD lemmas

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

Proof.

We show that a, b and $a - kb, b$ have the same set of divisors (and hence the same greatest common divisor.

4. Two GCD lemmas

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

Proof.

We show that a, b and $a - kb, b$ have the same set of divisors (and hence the same greatest common divisor.

Suppose $d|a$ and $d|b$.

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

Proof.

We show that a, b and $a - kb, b$ have the same set of divisors (and hence the same greatest common divisor.

Suppose $d|a$ and $d|b$. So there are integers x, y with $a = dx$ and $b = dy$.

4. Two GCD lemmas

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

Proof.

We show that a, b and $a - kb, b$ have the same set of divisors (and hence the same greatest common divisor.

Suppose $d|a$ and $d|b$. So there are integers x, y with $a = dx$ and $b = dy$. Note that

$$a - kb = dx - kdy = d(x - kb)$$

So d also divides $a - kb$.

4. Two GCD lemmas

Lemma 2

Let a, b, k be integers with a, b not both 0. Then

$$\gcd(a, b) = \gcd(a - kb, b).$$

Proof.

We show that a, b and $a - kb, b$ have the same set of divisors (and hence the same greatest common divisor.

Suppose $d|a$ and $d|b$. So there are integers x, y with $a = dx$ and $b = dy$. Note that

$$a - kb = dx - kdy = d(x - kb)$$

So d also divides $a - kb$.

Exercise. Conversely, show that if $d|(a - kb)$ and $d|b$, then $d|a$. □

5. Euclidean Algorithm

Major idea

Repeated applications of the division algorithm on the quotients can find the GCD quickly.

5. Euclidean Algorithm

Major idea

Repeated applications of the division algorithm on the quotients can find the GCD quickly.

Example 1. $a = 84, b = 35$

$$84 = 2 \cdot 35 + 14$$

5. Euclidean Algorithm

Major idea

Repeated applications of the division algorithm on the quotients can find the GCD quickly.

Example 1. $a = 84, b = 35$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$

5. Euclidean Algorithm

Major idea

Repeated applications of the division algorithm on the quotients can find the GCD quickly.

Example 1. $a = 84, b = 35$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7$$

5. Euclidean Algorithm

Major idea

Repeated applications of the division algorithm on the quotients can find the GCD quickly.

Example 1. $a = 84, b = 35$

$$
\begin{aligned}
84 &= 2 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7 \qquad \text{STOP}
\end{aligned}
$$

5. Euclidean Algorithm

Major idea

Repeated applications of the division algorithm on the quotients can find the GCD quickly.

Example 1. $a = 84, b = 35$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7 \qquad \text{STOP}$$

So $\gcd(84, 35) = 7$.

Example 2. $a = 1071, b = 462$

$$1071 = 2 \cdot 462 + 147$$

Example 2. $a = 1071, b = 462$

$$1071 = 2 \cdot 462 + 147$$
$$462 = 3 \cdot 147 + 21$$

Example 2. $a = 1071, b = 462$

$$\begin{aligned} 1071 &= 2 \cdot 462 + 147 \\ 462 &= 3 \cdot 147 + 21 \\ 147 &= 7 \cdot 21 \end{aligned}$$

5. Euclidean Algorithm

Example 2. $a = 1071, b = 462$

$$\begin{aligned} 1071 &= 2 \cdot 462 + 147 \\ 462 &= 3 \cdot 147 + 21 \\ 147 &= 7 \cdot 21 \qquad \text{STOP} \end{aligned}$$

5. Euclidean Algorithm

Example 2. $a = 1071, b = 462$

$$1071 = 2 \cdot 462 + 147$$
$$462 = 3 \cdot 147 + 21$$
$$147 = 7 \cdot 21 \qquad \text{STOP}$$

So $\gcd(1071, 462) = 21$.

6. Going backwards

The Euclidean Algorithm actually gives us a way to solve equations like this:

Theorem (Bezout's Identity)

Let a, b be integers (not both 0). There are integers x, y such that

$$ax + by = \gcd(a, b).$$

6. Going backwards

The Euclidean Algorithm actually gives us a way to solve equations like this:

Theorem (Bezout's Identity)

Let a, b be integers (not both 0). There are integers x, y such that

$$ax + by = \gcd(a, b).$$

The idea is to use back-substitution after applying the Euclidean algorithm

7. Bezout's Identity Example

$a = 84, b = 35, \gcd(84, 35) = 7$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7$$

7. Bezout's Identity Example

$a = 84, b = 35, \gcd(84, 35) = 7$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7$$

Example 1. Solve $7 = 35x + 84y$.

7. Bezout's Identity Example

$a = 84, b = 35, \gcd(84, 35) = 7$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7$$

Example 1. Solve $7 = 35x + 84y$.

$$\begin{aligned} 7 &= 35 - 2 \cdot \boxed{14} \\ &= \\ &= \\ &= \end{aligned}$$

7. Bezout's Identity Example

$a = 84, b = 35, \gcd(84, 35) = 7$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7$$

Example 1. Solve $7 = 35x + 84y$.

$$\begin{aligned} 7 &= 35 - 2 \cdot \boxed{14} \\ &= 35 - 2 \cdot (84 - 2 \cdot 35) \\ &= \\ &= \end{aligned}$$

7. Bezout's Identity Example

$a = 84, b = 35, \gcd(84, 35) = 7$

$$\begin{aligned}
84 &= 2 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7
\end{aligned}$$

Example 1. Solve $7 = 35x + 84y$.

$$\begin{aligned}
7 &= 35 - 2 \cdot \boxed{14} \\
&= 35 - 2 \cdot (84 - 2 \cdot 35) \\
&= 35 - 2 \cdot 84 + 4 \cdot 35 \\
&=
\end{aligned}$$

7. Bezout's Identity Example

$a = 84, b = 35, \gcd(84, 35) = 7$

$$
\begin{aligned}
84 &= 2 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7
\end{aligned}
$$

Example 1. Solve $7 = 35x + 84y$.

$$
\begin{aligned}
7 &= 35 - 2 \cdot \boxed{14} \\
&= 35 - 2 \cdot (84 - 2 \cdot 35) \\
&= 35 - 2 \cdot 84 + 4 \cdot 35 \\
&= (5)35 + (-1)84
\end{aligned}
$$

7. Bezout's Identity Example

$a = 84, b = 35, \gcd(84, 35) = 7$

$$84 = 2 \cdot 35 + 14$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7$$

Example 1. Solve $7 = 35x + 84y$.

$$\begin{aligned} 7 &= 35 - 2 \cdot \boxed{14} \\ &= 35 - 2 \cdot (84 - 2 \cdot 35) \\ &= 35 - 2 \cdot 84 + 4 \cdot 35 \\ &= (5)35 + (-1)84 \end{aligned}$$

So $x = 5$ and $y = -1$ solves $7 = 35x + 84y$.

7. Bezout's Identity Example

Example 2. Solve $21 = 35x + 84y$.

7. Bezout's Identity Example

Example 2. Solve $21 = 35x + 84y$.

$$\begin{aligned} 7 &= (5)35 + (-1)84 \\ \implies 3 \cdot 7 &= (3 \cdot 5)35 + (3 \cdot -1)84 \\ \implies 21 &= (15)35 + (-3)84 \end{aligned}$$

7. Bezout's Identity Example

Example 2. Solve $21 = 35x + 84y$.

$$\begin{aligned} 7 &= (5)35 + (-1)84 \\ \implies 3 \cdot 7 &= (3 \cdot 5)35 + (3 \cdot -1)84 \\ \implies 21 &= (15)35 + (-3)84 \end{aligned}$$

So $x = 15$ and $y = -3$ solves $21 = 35x + 84y$.

Reflection

- What is a proof that the Euclidean algorithm always works?
- Are the solutions x, y to Bezout's identity always unique? Can there be other solutions?
- Write code that runs the Euclidean algorithm. Is it fast?
- Apply the Euclidean algorithm to two consecutive Fibonacci numbers (like 55 and 34). What happens and why?