Number Theory with python PROGRAMMING

Euclidean Algorithm

Lecture 3

Justin Stevens

Outline

1. Euclidean Algorithm
   - Greatest Common Divisor
   - Proof
   - GCD of 3 Numbers
   - Euclidean Algorithm Challenges
2. Bezout's Identity
3. Linear Congruences

Greatest Common Divisor

We can find the set of all positive divisors of the number n, denoted $D(n)$:

Greatest Common Divisor

We can find the set of all positive divisors of the number n, denoted $D(n)$:

$$D(12) = \{1, 2, 3, 4, 6, 12\}$$
$$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

Greatest Common Divisor

We can find the set of all positive divisors of the number n, denoted $D(n)$:

$$D(12) = \{1, 2, 3, 4, 6, 12\}$$
$$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

The set of common divisors of 12 and 30 is $D(12) \cap D(30) = \{1, 2, 3, 6\}$. The max is 6. We say that this is the greatest common divisor of 12 and 30.

Greatest Common Divisor

We can find the set of all positive divisors of the number n, denoted $D(n)$:

$$D(12) = \{1, 2, 3, 4, 6, 12\}$$
$$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

The set of common divisors of 12 and 30 is $D(12) \cap D(30) = \{1, 2, 3, 6\}$. The max is 6. We say that this is the greatest common divisor of 12 and 30.

Definition. For two integers a and b the set of common divisors of a and b is $D(a) \cap D(b)$. The maximum element in this set is the **greatest common divisor** of a and b, $\gcd(a, b)$.

By definition, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ since it is a divisor of both. We do not define $\gcd(0, 0)$ since every positive integer divides 0.

Theorem. When $a \mid b$, $\gcd(a, b) = a$.

Euclid's Elements

Around the time of 300 BC, a great Greek mathematician rose from Alexandria by the name of Euclid. He wrote a series of 13 books known as *Elements*. Elements is thought by many to be the most successful and influential textbook ever written. It has been published the second most of any book, next to the Bible.

The book covers both Euclidean geometry and elementary number theory. This chapter will focus solely on **Book VII, Proposition 1.**

Euclidean Algorithm I

In a previous example, we saw that when $a = 25$ and $b = 15$, then

$$D(25) = \{1, 5, 25\},\ D(15) = \{1, 3, 5, 15\}.$$

Euclidean Algorithm I

In a previous example, we saw that when $a = 25$ and $b = 15$, then

$$D(25) = \{1, 5, 25\},\ D(15) = \{1, 3, 5, 15\}.$$

Their difference is $a - b = 25 - 15 = 10$. Note that $D(10) = \{1, 2, 5, 10\}$.

Euclidean Algorithm I

In a previous example, we saw that when $a = 25$ and $b = 15$, then

$$D(25) = \{1, 5, 25\},\ D(15) = \{1, 3, 5, 15\}.$$

Their difference is $a - b = 25 - 15 = 10$. Note that $D(10) = \{1, 2, 5, 10\}$.

$$D(25) \cap D(15) = D(15) \cap D(10) = \{1, 5\}.$$

Hence, $\gcd(25, 15) = \gcd(15, 10) = 5$.

Euclidean Algorithm II

"When two unequal numbers are set out, and the less is continually subtracted in turn from the greater, if the number which is left never measures the one before it until a unit is left, then the original numbers are relatively prime." - Euclid

Theorem. If $n = dq + r$ where $0 \leq r < d$, then $\gcd(n, d) = \gcd(d, r)$.

Proof of Euclidean Algorithm

Theorem. If $n = dq + r$ where $0 \leq r < d$, then $\gcd(n, d) = \gcd(d, r)$.

Proof. I claim that the set of common divisors between n and d is the same as the set of common divisors between d and r.

Proof of Euclidean Algorithm

Theorem. If $n = dq + r$ where $0 \leq r < d$, then $\gcd(n, d) = \gcd(d, r)$.

Proof. I claim that the set of common divisors between n and d is the same as the set of common divisors between d and r.

If l is a common divisor of n and d, then since $l \mid n$ and $l \mid d$, l divides all linear combinations of n and d. Therefore, $l \mid n - dq = r$, meaning that l is also a common divisor of n and r.

Proof of Euclidean Algorithm

Theorem. If $n = dq + r$ where $0 \leq r < d$, then $\gcd(n, d) = \gcd(d, r)$.

Proof. I claim that the set of common divisors between n and d is the same as the set of common divisors between d and r.

If l is a common divisor of n and d, then since $l \mid n$ and $l \mid d$, l divides all linear combinations of n and d. Therefore, $l \mid n - dq = r$, meaning that l is also a common divisor of n and r.

Conversely, if k is a common divisor of d and r, then since $k \mid d$ and $k \mid r$, k is a common divisor of all linear combinations of d and r, therefore, $k \mid dq + r = n$. Hence, k is also a common divisor of n and d.

Proof of Euclidean Algorithm

Theorem. If $n = dq + r$ where $0 \leq r < d$, then $\gcd(n, d) = \gcd(d, r)$.

Proof. I claim that the set of common divisors between n and d is the same as the set of common divisors between d and r.

If l is a common divisor of n and d, then since $l \mid n$ and $l \mid d$, l divides all linear combinations of n and d. Therefore, $l \mid n - dq = r$, meaning that l is also a common divisor of n and r.

Conversely, if k is a common divisor of d and r, then since $k \mid d$ and $k \mid r$, k is a common divisor of all linear combinations of d and r, therefore, $k \mid dq + r = n$. Hence, k is also a common divisor of n and d.

We have established that the two sets of common divisors are equivalent, therefore, the greatest common divisor must be equivalent.

Example. Compute $\gcd(60, 8)$ and $\gcd(490, 110)$.

Practice Euclidean Algorithm

Example. Compute $\gcd(60, 8)$ and $\gcd(490, 110)$.

We see that $60 = 8 \cdot 7 + 4$, hence, $\gcd(60, 8) = \gcd(8, 4) = 4$.

Practice Euclidean Algorithm

Example. Compute $\gcd(60, 8)$ and $\gcd(490, 110)$.

We see that $60 = 8 \cdot 7 + 4$, hence, $\gcd(60, 8) = \gcd(8, 4) = 4$.

For the second problem, we use the division algorithm twice:

$$\begin{aligned} 490 &= 110 \cdot 4 + 50 \\ 110 &= 50 \cdot 2 + 10 \\ 50 &= 10 \cdot 5. \end{aligned}$$

Therefore, $\gcd(490, 110) = \gcd(110, 50) = 10$. We can verify that

$$\begin{aligned} D(490) &= \{1, 2, 5, 7, 10, 14, 35, 49, 70, 98, 245, 490\} \\ D(110) &= \{1, 2, 5, 10, 11, 22, 55, 110\} \\ D(50) &= \{1, 2, 5, 10, 25, 50\}. \end{aligned}$$

Hence, $D(490) \cap D(110) = D(110) \cap D(50) = \{1, 2, 5, 10\}$.

Extended Euclidean Algorithm

Theorem. For two natural a, b, $a > b$, to find $\gcd(a, b)$ we use the division algorithm repeatedly

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ \dots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Then we have $\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n$.

Notice the greatest common divisor is the final **non-zero remainder**.

Examples of Euclidean Algorithm

Example 1.

(a) Find $\gcd(603, 301)$.

(b) Find $\gcd(289, 153)$.

(c) Find $\gcd(2627, 481)$.

(d) Find $\gcd(8774, 1558)$.

Example (a) Solution

Example. Find $\gcd(603, 301)$.

Note that

$$603 = 301 \cdot 2 + 1.$$

Therefore, by the Euclidean Algorithm, we have

$$\gcd(603, 301) = \gcd(1, 301) = \boxed{1}.$$

Example (b) Solution

Example. Find $\gcd(289, 153)$.

We repeatedly use the division algorithm as follows:

$$\begin{aligned} 289 &= 153 \cdot 1 + 136 \\ 153 &= 136 \cdot 1 + \boxed{17} \\ 136 &= 17 \cdot 8 + 0. \end{aligned}$$

Therefore $\gcd(153, 289) = \boxed{17}$.

Example (c) Solution

Example. Find $\gcd(2627, 481)$.

We repeatedly use the division algorithm as follows:

$$\begin{aligned} 2627 &= 481 \cdot 5 + 222 \\ 481 &= 222 \cdot 2 + \boxed{37} \\ 222 &= 37 \cdot 6 + 0 \end{aligned}$$

Therefore $\gcd(2627, 481) = 37$.

Notice that we only use remainders in the Euclidean algorithm. For instance, in the previous example, $2627 \equiv 222 \pmod{481}$. For larger numbers, we use computers to calculate the remainders.

Example (d) Solution

Example. Find $\gcd(8774, 1558)$.

With the help of a computer:

$$\begin{aligned} 8774 &\equiv 984 \pmod{1558} \\ 1558 &\equiv 574 \pmod{948} \\ 948 &\equiv 410 \pmod{574} \\ 574 &\equiv 164 \pmod{410} \\ 410 &\equiv \boxed{82} \pmod{164} \\ 164 &\equiv 0 \pmod{82} \end{aligned}$$

Since we desire the last non-zero remainder, $\gcd(8774, 1558) = 82$.

More than 2 Numbers

The greatest common divisor of more than 2 numbers is defined similarly.

For example, to calculate $\gcd(21, 35, 49)$, we see that

More than 2 Numbers

The greatest common divisor of more than 2 numbers is defined similarly.

For example, to calculate $\gcd(21, 35, 49)$, we see that

$$D(21) = \{1, 3, 7, 21\},\ D(35) = \{1, 5, 7, 35\},\ D(49) = \{1, 7, 49\}.$$

More than 2 Numbers

The greatest common divisor of more than 2 numbers is defined similarly.

For example, to calculate $\gcd(21, 35, 49)$, we see that

$$D(21) = \{1, 3, 7, 21\},\ D(35) = \{1, 5, 7, 35\},\ D(49) = \{1, 7, 49\}.$$

Therefore, $D(21) \cap D(35) \cap D(49) = \{1, 7\}$. Hence, $\gcd(21, 35, 49) = 7$.

More than 2 Numbers

The greatest common divisor of more than 2 numbers is defined similarly.

For example, to calculate $\gcd(21, 35, 49)$, we see that

$$D(21) = \{1, 3, 7, 21\},\ D(35) = \{1, 5, 7, 35\},\ D(49) = \{1, 7, 49\}.$$

Therefore, $D(21) \cap D(35) \cap D(49) = \{1, 7\}$. Hence, $\gcd(21, 35, 49) = 7$.

Caution: When calculating $\gcd(6, 10, 15)$, we may be tempted to say 2 or 3 since $\gcd(6, 10) = 2$ or $\gcd(6, 15) = 3$. However, $2 \nmid 15$ and $3 \nmid 10$. Indeed,

$$D(6) = \{1, 2, 3, 6\},\ D(10) = \{1, 2, 5, 10\},\ D(15) = \{1, 3, 5, 15\}.$$

The only common divisor of all three numbers is 1.

More than 2 Numbers

The greatest common divisor of more than 2 numbers is defined similarly.

For example, to calculate $\gcd(21, 35, 49)$, we see that

$$D(21) = \{1, 3, 7, 21\},\ D(35) = \{1, 5, 7, 35\},\ D(49) = \{1, 7, 49\}.$$

Therefore, $D(21) \cap D(35) \cap D(49) = \{1, 7\}$. Hence, $\gcd(21, 35, 49) = 7$.

Caution: When calculating $\gcd(6, 10, 15)$, we may be tempted to say 2 or 3 since $\gcd(6, 10) = 2$ or $\gcd(6, 15) = 3$. However, $2 \nmid 15$ and $3 \nmid 10$. Indeed,

$$D(6) = \{1, 2, 3, 6\},\ D(10) = \{1, 2, 5, 10\},\ D(15) = \{1, 3, 5, 15\}.$$

The only common divisor of all three numbers is 1.

Using our set notation, we can show the following theorem:

Theorem. For three positive integers a, b, c,

$$\gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b).$$

Example 2. Compute $\gcd(3^{64}-1, 3^{40}-1)$ and $\gcd(3^{64}-1, 3^{20}-1)$.

Example 3. Compute $\gcd(2002+2, 2002^2+2, 2002^3+2, \cdots)$. *

* Source: 2002 HMMT

Exponent GCD

Example. Compute $\gcd(3^{64}-1, 3^{40}-1)$.

We reduce the exponents using the Euclidean algorithm:

$$\begin{aligned}
3^{64}-1 &= \left(3^{40}-1\right)3^{24} + \left(3^{24}-1\right) &&\implies \gcd(3^{64}-1, 3^{40}-1) = \gcd(3^{40}-1, 3^{24}-1)\\
3^{40}-1 &= \left(3^{24}-1\right)3^{16} + \left(3^{16}-1\right) &&\implies \gcd(3^{24}-1, 3^{40}-1) = \gcd(3^{24}-1, 3^{16}-1)\\
3^{24}-1 &= \left(3^{16}-1\right)3^{8} + \left(3^{8}-1\right) &&\implies \gcd(3^{24}-1, 3^{16}-1) = \gcd(3^{16}-1, 3^{8}-1)\\
3^{16}-1 &= \left(3^{8}-1\right)\left(3^{8}+1\right) &&\implies \gcd(3^{8}-1, 3^{16}-1) = \boxed{3^{8}-1}.
\end{aligned}$$

Note the parallel between the above equations and computing $\gcd(64, 40)$:

$$\gcd(64, 40) = \gcd(40, 24) = \gcd(24, 16) = \gcd(16, 8) = 8.$$

Exponent GCD II

Example. Compute $\gcd(3^{64}-1, 3^{20}-1)$.

We reduce the exponents using the Euclidean algorithm:

$$\begin{aligned}
3^{64}-1 &= \left(3^{20}-1\right)3^{44} + \left(3^{44}-1\right) &&\implies \gcd(3^{64}-1, 3^{20}-1) = \gcd(3^{44}-1, 3^{20}-1)\\
3^{44}-1 &= \left(3^{20}-1\right)3^{24} + \left(3^{24}-1\right) &&\implies \gcd(3^{44}-1, 3^{20}-1) = \gcd(3^{24}-1, 3^{20}-1)\\
3^{24}-1 &= \left(3^{20}-1\right)3^{4} + \left(3^{4}-1\right) &&\implies \gcd(3^{24}-1, 3^{20}-1) = \gcd(3^{20}-1, 3^{4}-1)
\end{aligned}$$

Note that $3^4-1 \mid \left(3^4\right)^5-1$, hence $\gcd(3^{20}-1, 3^4-1) = 3^4-1$.

Notice the parallel with the division algorithm:

$$\begin{aligned}
64 &= 20\cdot 3+4\\
20 &= 4\cdot 5.
\end{aligned}$$

Therefore, $\gcd(64, 20) = \gcd(4, 20) = 4$.

Generalized Exponent GCD

Theorem. For natural numbers, $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

2002 GCD Sequence

Example. Compute $\gcd(2002 + 2, 2002^2 + 2, 2002^3 + 2, \cdots)$.

We compute the gcd of the first two terms. By difference of squares,

2002 GCD Sequence

Example. Compute $\gcd(2002+2, 2002^2+2, 2002^3+2, \cdots)$.

We compute the gcd of the first two terms. By difference of squares,

$$2002^2 - 4 = (2002+2)(2002-2) \implies 2002^2 + 2 = (2002+2)(2002-2) + 6.$$

2002 GCD Sequence

Example. Compute $\gcd(2002+2, 2002^2+2, 2002^3+2, \cdots)$.

We compute the gcd of the first two terms. By difference of squares,

$$2002^2 - 4 = (2002+2)(2002-2) \implies 2002^2+2 = (2002+2)(2002-2)+6.$$

Hence, by the Euclidean Algorithm,

$$\gcd(2002+2, 2002^2+2) = \gcd(2002+2, 6) = \gcd(2004, 6) = 6.$$

2002 GCD Sequence

Example. Compute $\gcd(2002+2, 2002^2+2, 2002^3+2, \cdots)$.

We compute the gcd of the first two terms. By difference of squares,

$$2002^2 - 4 = (2002+2)(2002-2) \implies 2002^2 + 2 = (2002+2)(2002-2) + 6.$$

Hence, by the Euclidean Algorithm,

$$\gcd(2002+2, 2002^2+2) = \gcd(2002+2, 6) = \gcd(2004, 6) = 6.$$

Therefore, the greatest common divisor of the sequence can be at most 6.

2002 GCD Sequence

Example. Compute $\gcd(2002+2, 2002^2+2, 2002^3+2, \cdots)$.

We compute the gcd of the first two terms. By difference of squares,

$$2002^2 - 4 = (2002+2)(2002-2) \implies 2002^2+2 = (2002+2)(2002-2)+6.$$

Hence, by the Euclidean Algorithm,

$$\gcd(2002+2, 2002^2+2) = \gcd(2002+2, 6) = \gcd(2004, 6) = 6.$$

Therefore, the greatest common divisor of the sequence can be at most 6.

Every term in the sequence is even. Furthermore, since $2002 \equiv 1 \pmod 3$,

$$2002^k + 2 \equiv 1^k + 2 \equiv 1 + 2 \equiv 0 \pmod 3.$$

2002 GCD Sequence

Example. Compute $\gcd(2002+2, 2002^2+2, 2002^3+2, \cdots)$.

We compute the gcd of the first two terms. By difference of squares,

$$2002^2 - 4 = (2002+2)(2002-2) \implies 2002^2 + 2 = (2002+2)(2002-2) + 6.$$

Hence, by the Euclidean Algorithm,

$$\gcd(2002+2, 2002^2+2) = \gcd(2002+2, 6) = \gcd(2004, 6) = 6.$$

Therefore, the greatest common divisor of the sequence can be at most 6.

Every term in the sequence is even. Furthermore, since $2002 \equiv 1 \pmod 3$,

$$2002^k + 2 \equiv 1^k + 2 \equiv 1 + 2 \equiv 0 \pmod 3.$$

Hence, every term in the sequence is divisible by both 2 and 3, and therefore 6. The greatest common divisor of the sequence is $\boxed{6}$.

Outline

1 Euclidean Algorithm

2 Bezout's Identity
- Euclidean Algorithm Recap
- Proof
- Bezout's Identity Puzzles

3 Linear Congruences

Euclidean Algorithm Recap

Theorem. For two natural a, b, $a > b$, to find $\gcd(a, b)$ we use the division algorithm repeatedly

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
\cdots & \\
r_{n-2} &= r_{n-1} q_n + r_n \\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

Then we have $\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n$.

Notice the greatest common divisor is the final **non-zero remainder**.

Linear Combinations

Definition. A linear combination of two integers n_1 and n_2 is of the form $n_1x_1 + n_2x_2$ where x_1 and x_2 are integers.

Theorem. If $d \mid n_1$ and $d \mid n_2$, then $d \mid n_1x_1 + n_2x_2$ for integers x_1 and x_2.

Example 4. Express 5 as a linear combination of 45 and 65.

Example 5. Express 10 as a linear combination of 110 and 380.

Express 5 as Linear Combination

Example. Express 5 as a linear combination of 45 and 65.

Notice $\gcd(65, 45) = 5$. Using the Euclidean Algorithm,

$$\begin{aligned} 65 &= 45 \cdot 1 + 20 \\ 45 &= 20 \cdot 2 + 5 \\ 20 &= 5 \cdot 4 \end{aligned}$$

Running the process in reverse:

$$\begin{aligned} 5 &= 45 - 20 \cdot 2 \\ &= 45 - (65 - 45 \cdot 1)2 \\ &= 45 \cdot 3 - 65 \cdot 2. \end{aligned}$$

Express 5 as Linear Combination

Example. Express 5 as a linear combination of 45 and 65.

Notice $\gcd(65, 45) = 5$. Using the Euclidean Algorithm,

$$\begin{aligned} 65 &= 45 \cdot 1 + 20 \\ 45 &= 20 \cdot 2 + 5 \\ 20 &= 5 \cdot 4 \end{aligned}$$

Running the process in reverse:

$$\begin{aligned} 5 &= 45 - 20 \cdot 2 \\ &= 45 - (65 - 45 \cdot 1)2 \\ &= 45 \cdot 3 - 65 \cdot 2. \end{aligned}$$

Express 10 as Linear Combination

Example. Express 10 as a linear combination of 110 and 380.

Solution. We again, use the Euclidean Algorithm to arrive at

$$\begin{aligned} 380 &= 110 \cdot 3 + 50 \\ 110 &= 50 \cdot 2 + \boxed{10} \\ 50 &= 10 \cdot 5 \end{aligned}$$

Using the Euclidean Algorithm in reverse:

$$\begin{aligned} 10 &= 110 - 50 \cdot 2 \\ &= 110 - (380 - 110 \cdot 3) \cdot 2 \\ &= 7 \cdot 110 - 2 \cdot 380. \end{aligned}$$

Bezout's Identity

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

Proof 1: Run the Euclidean Algorithm backwards.

Bezout's Identity

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

Proof 1: Run the Euclidean Algorithm backwards.

Proof 2: Consider the set $S = \{ax + by > 0 \text{ with } x, y \text{ integers}\}$.

For instance, if $a = 4$ and $b = 6$, then which values would be in the set?

(i) 10 (ii) 7 (iii) 2 (iv) -8

Bezout's Identity

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

Proof 1: Run the Euclidean Algorithm backwards.

Proof 2: Consider the set $S = \{ax + by > 0 \text{ with } x, y \text{ integers}\}$.

For instance, if $a = 4$ and $b = 6$, then which values would be in the set?

(i) 10 (ii) 7 (iii) 2 (iv) -8

The answer is (i) and (iii) since $4 \cdot 1 + 6 \cdot 1 = 10$ and $4 \cdot (-1) + 6 \cdot 1 = 2$.

Bezout's Identity

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

Proof 1: Run the Euclidean Algorithm backwards.

Proof 2: Consider the set $S = \{ax + by > 0 \text{ with } x, y \text{ integers}\}$.

For instance, if $a = 4$ and $b = 6$, then which values would be in the set?

(i) 10 (ii) 7 (iii) 2 (iv) -8

The answer is (i) and (iii) since $4 \cdot 1 + 6 \cdot 1 = 10$ and $4 \cdot (-1) + 6 \cdot 1 = 2$.

The **well-ordering principle** states that every non-empty subset of positive integers has a least element. Let this minimum be $d = \min(S)$.

Bezout's Identity

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

Proof 1: Run the Euclidean Algorithm backwards.

Proof 2: Consider the set $S = \{ax + by > 0 \text{ with } x, y \text{ integers}\}$.

For instance, if $a = 4$ and $b = 6$, then which values would be in the set?

(i) 10 (ii) 7 (iii) 2 (iv) -8

The answer is (i) and (iii) since $4 \cdot 1 + 6 \cdot 1 = 10$ and $4 \cdot (-1) + 6 \cdot 1 = 2$.

The **well-ordering principle** states that every non-empty subset of positive integers has a least element. Let this minimum be $d = \min(S)$.

Since d is a member of the set, there exists integers x_1 and y_1 such that $d = ax_1 + by_1$. Now, we must prove $d = \gcd(a, b)$. How can we do this?

Bezout's Identity Proof I

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

$S = \{ax + by > 0,\ x, y \in \mathbb{Z}\}$ and $d = \min(S) = ax_1 + by_1 \stackrel{?}{=} \gcd(a, b)$.

Bezout's Identity Proof I

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

$S = \{ax + by > 0,\ x, y \in \mathbb{Z}\}$ and $d = \min(S) = ax_1 + by_1 \stackrel{?}{=} \gcd(a, b)$.

To begin, we show that d is a common divisor a and b. Assume for the sake of contradiction that d doesn't divide a. By the division algorithm, we have

Bezout's Identity Proof I

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

$S = \{ax + by > 0,\ x, y \in \mathbb{Z}\}$ and $d = \min(S) = ax_1 + by_1 \stackrel{?}{=} \gcd(a, b)$.

To begin, we show that d is a common divisor a and b. Assume for the sake of contradiction that d doesn't divide a. By the division algorithm, we have

$$a = dq + r, \quad 0 \leq r < d.$$

We substitute $d = ax_1 + by_1$ into this equation:

$$a = dq + r = (ax_1 + by_1)\, q + r \implies r = a\,(1 - qx_1) + b\,(-qy_1)\,.$$

Bezout's Identity Proof I

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

$S = \{ax + by > 0,\ x, y \in \mathbb{Z}\}$ and $d = \min(S) = ax_1 + by_1 \stackrel{?}{=} \gcd(a, b)$.

To begin, we show that d is a common divisor a and b. Assume for the sake of contradiction that d doesn't divide a. By the division algorithm, we have

$$a = dq + r, \quad 0 \leq r < d.$$

We substitute $d = ax_1 + by_1$ into this equation:

$$a = dq + r = (ax_1 + by_1)\, q + r \implies r = a\,(1 - qx_1) + b\,(-qy_1)\,.$$

If r is positive, then $r \in S$ since it satisfies the two conditions, however this contradicts the minimality of d. Therefore, we must have $r = 0$ and $d \mid a$.

We can similarly show $d \mid b$. Hence, d is a common divisor of a and b.

Bezout's Identity Proof II

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

$S = \{ax + by > 0,\ x, y \in \mathbb{Z}\}$ and $d = \min(S) = ax_1 + by_1 \stackrel{?}{=} \gcd(a, b)$.

It is now left to show that d is the *greatest* common divisor of a and b.

Bezout's Identity Proof II

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

$S = \{ax + by > 0,\ x, y \in \mathbb{Z}\}$ and $d = \min(S) = ax_1 + by_1 \stackrel{?}{=} \gcd(a, b)$.

It is now left to show that d is the *greatest* common divisor of a and b.

Let d_1 be another common divisor of a and b. By the linear combination theorem, d_1 divides all linear combinations of a and b. Specifically,

$$d_1 \mid ax_1 + by_1 = d.$$

Therefore, every common divisor of a and b divides d, hence, $d = \gcd(a, b)$.

Corollary. If $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.

Bezout's Identity Proof II

Theorem. For a, b natural, there exist $x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

$S = \{ax + by > 0,\ x, y \in \mathbb{Z}\}$ and $d = \min(S) = ax_1 + by_1 \stackrel{?}{=} \gcd(a, b)$.

It is now left to show that d is the *greatest* common divisor of a and b.

Let d_1 be another common divisor of a and b. By the linear combination theorem, d_1 divides all linear combinations of a and b. Specifically,

$$d_1 \mid ax_1 + by_1 = d.$$

Therefore, every common divisor of a and b divides d, hence, $d = \gcd(a, b)$.

Corollary. If $c \mid a$ and $c \mid b$, then $c \mid \gcd(a, b)$.

Example. Express 3 as a linear combination of 1011 and $11,202$.

Linear Combination of 1011 and $11,202$.

Example. Express 3 as a linear combination of 1011 and $11,202$.

Solution. We use the Euclidean Algorithm to arrive at

$$\begin{aligned} 11202 &= 1011 \cdot 11 + 81 \\ 1011 &= 81 \cdot 12 + 39 \\ 81 &= 39 \cdot 2 + \boxed{3} \\ 39 &= 3 \cdot 13 \end{aligned}$$

Using the Euclidean Algorithm in reverse

$$\begin{aligned} 3 &= 81 - 39 \cdot 2 \\ &= 81 - (1011 - 81 \cdot 12) \cdot 2 \\ &= 81 \cdot 25 - 1011 \cdot 2 \\ &= (11202 - 1011 \cdot 11) \cdot 25 - 1011 \cdot 2 \\ &= 11202 \cdot 25 - 1011 \cdot 277. \end{aligned}$$

Linear Combination of 1011 and $11,202$.

Example. Express 3 as a linear combination of 1011 and $11,202$.

Solution. We use the Euclidean Algorithm to arrive at

$$\begin{aligned} 11202 &= 1011 \cdot 11 + 81 \\ 1011 &= 81 \cdot 12 + 39 \\ 81 &= 39 \cdot 2 + \boxed{3} \\ 39 &= 3 \cdot 13 \end{aligned}$$

Using the Euclidean Algorithm in reverse

$$\begin{aligned} 3 &= 81 - 39 \cdot 2 \\ &= 81 - (1011 - 81 \cdot 12) \cdot 2 \\ &= 81 \cdot 25 - 1011 \cdot 2 \\ &= (11202 - 1011 \cdot 11) \cdot 25 - 1011 \cdot 2 \\ &= 11202 \cdot 25 - 1011 \cdot 277. \end{aligned}$$

Bezout's Identity Puzzles

Example 6. Suppose you have a 5 litre jug and a 7 litre jug. We can perform any of the following moves:

- Fill a jug completely with water.
- Transfer water from one jug to another, stopping if the other jug is filled.
- Empty a jug of water.

The goal is to end up with one jug having exactly 1 litre of water. How do we do this?

Jug Puzzle

Note that at every stage, the jugs will contain a linear combination of 5 and 7 litres of water. We find that $1 = 5 \cdot 3 + 7 \cdot (-2)$, therefore, we want to fill the jug with 5 litres 3 times, and empty the one with 7 litres twice.

Jug Puzzle

Note that at every stage, the jugs will contain a linear combination of 5 and 7 litres of water. We find that $1 = 5 \cdot 3 + 7 \cdot (-2)$, therefore, we want to fill the jug with 5 litres 3 times, and empty the one with 7 litres twice.

In order to keep track of how much water we have in each step, we use an ordered pair (a, b), where a is the amount in the 5 litre jug and b is the amount in the 7 litre jug:

$$(0,0) \overset{\text{Fill}}{\to} (5,0) \overset{\text{Transfer}}{\to} (0,5) \overset{\text{Transfer}}{\to} (5,5) \overset{\text{Transfer}}{\to} (3,7) \overset{\text{Empty}}{\to} (3,0)$$

$$(3,0) \overset{\text{Transfer}}{\to} (0,3) \overset{\text{Fill}}{\to} (5,3) \overset{\text{Transfer}}{\to} (1,7) \overset{\text{Empty}}{\to} (1,0).$$

Jug Puzzle

Note that at every stage, the jugs will contain a linear combination of 5 and 7 litres of water. We find that $1 = 5 \cdot 3 + 7 \cdot (-2)$, therefore, we want to fill the jug with 5 litres 3 times, and empty the one with 7 litres twice.

In order to keep track of how much water we have in each step, we use an ordered pair (a, b), where a is the amount in the 5 litre jug and b is the amount in the 7 litre jug:

$$(0,0) \overset{\text{Fill}}{\rightarrow} (5,0) \overset{\text{Transfer}}{\rightarrow} (0,5) \overset{\text{Transfer}}{\rightarrow} (5,5) \overset{\text{Transfer}}{\rightarrow} (3,7) \overset{\text{Empty}}{\rightarrow} (3,0)$$
$$(3,0) \overset{\text{Transfer}}{\rightarrow} (0,3) \overset{\text{Fill}}{\rightarrow} (5,3) \overset{\text{Transfer}}{\rightarrow} (1,7) \overset{\text{Empty}}{\rightarrow} (1,0).$$

Proving Important Theorems

Example 7. Prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

Example 8. Prove that if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

⋆ Exponent GCD Theorem

Example. Prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

Let $d = \gcd(a^m - 1, a^n - 1)$. We show $d \mid a^{\gcd(m,n)} - 1$ and $a^{\gcd(m,n)} - 1 \mid d$.

$\star$ Exponent GCD Theorem

Example. Prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

Let $d = \gcd(a^m - 1, a^n - 1)$. We show $d \mid a^{\gcd(m,n)} - 1$ and $a^{\gcd(m,n)} - 1 \mid d$.

Since $d \mid a^m - 1 \implies a^m \equiv 1 \pmod{d}$. Similarly, $a^n \equiv 1 \pmod{d}$.

$\star$ Exponent GCD Theorem

Example. Prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

Let $d = \gcd(a^m - 1, a^n - 1)$. We show $d \mid a^{\gcd(m,n)} - 1$ and $a^{\gcd(m,n)} - 1 \mid d$.

Since $d \mid a^m - 1 \implies a^m \equiv 1 \pmod{d}$. Similarly, $a^n \equiv 1 \pmod{d}$.

By Bezout's identity, let $\gcd(m, n) = mx + ny$. Then,

$$a^{\gcd(m,n)} \equiv a^{mx+ny} \equiv a^{mx} a^{ny} \equiv 1 \pmod{d}.$$

Therefore, $d \mid a^{\gcd(m,n)} - 1$. We now show that $a^{\gcd(m,n)} - 1 \mid d$.

Since $\gcd(m, n) \mid m$ and $\gcd(m, n) \mid n$, we have

$$\begin{cases} a^{\gcd(m,n)} - 1 \mid a^m - 1 \\ a^{\gcd(m,n)} - 1 \mid a^n - 1 \end{cases} \implies a^{\gcd(m,n)} - 1 \mid \gcd(a^m - 1, a^n - 1).$$

From $d \mid a^{\gcd(m,n)} - 1$ and $a^{\gcd(m,n)} - 1 \mid d$, we have

$$d = \gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1.$$

Euclid's Lemma

Example. If $a \mid bc$ and $\gcd(a, b) = 1$, prove that $a \mid c$.

Proof. By Bezout's identity, $\gcd(a, b) = 1$ implies that there exist x, y such that $ax + by = 1$. Next, multiply this equation by c to arrive at

$$c(ax) + c(by) = c.$$

Finally, since $a \mid c(ax)$ and $a \mid bc$ (given), we have $a \mid ac(x) + bc(y) = c$.

Outline

1. Euclidean Algorithm
2. Bezout's Identity
3. Linear Congruences
   - Diophantine Equations
   - Modular Inverses

Linear Diophantine Equation

Example 9. How many ways are there to make $3.00 using dimes and quarters?

Example 10. Find **all** pairs of integers x, y such that $5x + 7y = 1$.

Parametizing

Example. How many ways are there to make \$3.00 using dimes and quarters?

Let the number of dimes be d and quarters be q. Then,

$$10d + 25q = 300 \implies 2d + 5q = 60.$$

Note that the number of dimes must be divisible by 5. Hence, $d = 0, 5, 10, 15, 20, 25, 30$ gives the solutions

$$(d, q) = (0, 12), (5, 10), (10, 8), (15, 6), (20, 4), (25, 2), (30, 0).$$

There are a total of **7** solutions.

Pairs of Integers

Example. Find **all** pairs of integers x, y such that $5x + 7y = 1$.

We see that $(x, y) = (3, -2)$ is a solution. All such solutions are given by $(x, y) = (3 + 5t, -2 - 7t)$.

Division in Modulos

Consider the multiplication table below for mod 7:

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Find values of x and y such that $3x \equiv 1 \pmod 7$ and $2y \equiv 1 \pmod 7$.

Division in Modulos

Consider the multiplication table below for mod 7:

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Find values of x and y such that $3x \equiv 1 \pmod 7$ and $2y \equiv 1 \pmod 7$.

We see that $x \equiv 5 \pmod 7$ and $y \equiv 4 \pmod 7$. These are called inverses.

Definition. The **inverse** of a mod m is the value x with $ax \equiv 1 \pmod m$. This is denoted $a^{-1} \pmod m$ and is analogous to division.

Example 11. Solve the congruences $8y \equiv 1 \mod 39$ and $9z \equiv 1 \mod 41$.

Example 12. Are there values of x such that $2x \equiv 1 \pmod{6}$?

Example 13. Solve the congruence $13x \equiv 1 \pmod{71}$.

Example. Solve the congruences $8y \equiv 1 \pmod{39}$ and $9z \equiv 1 \pmod{41}$.

We see that $8 \cdot 5 = 40 \equiv 1 \pmod{39} \implies y \equiv 5 \pmod{39}$.

Example. Solve the congruences $8y \equiv 1 \pmod{39}$ and $9z \equiv 1 \pmod{41}$.

We see that $8 \cdot 5 = 40 \equiv 1 \pmod{39} \implies y \equiv 5 \pmod{39}$.

For the second problem,

$$9 \cdot 9 = 81 \equiv -1 \pmod{41} \implies z \equiv -9 \equiv 32 \pmod{41}.$$

When Division Fails

Example. Are there values of x such that $2x \equiv 1 \pmod 6$?

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 1: Multiplication Table Mod 6.

We see that only $2x \equiv 0, 2, 4 \pmod 6$. Therefore, the answer is no.

Mod 71 Congruence

Example. Solve the congruence $13x \equiv 1 \pmod{71}$.

Using the Euclidean algorithm

$$\begin{aligned} 71 &= 13 \cdot 5 + 6 \\ 13 &= 6 \cdot 2 + 1 \end{aligned}$$

In reverse:

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 \\ &= 13 - (71 - 13 \cdot 5) \cdot 2 \\ &= 13 \cdot 11 - 71 \cdot 2. \end{aligned}$$

Hence, $x \equiv 11 \pmod{71}$.