MTH314: Discrete Mathematics for Engineers

Lecture 6: Divisibility

Dr Ewa Infeld

Ryerson University

Divisibility: Definition

Definition

Let $a,\ b \in \mathbb{Z}$. We say that a divides b if there exists an integer q such that $aq = b$.

- Does 6 divide 0?
- What numbers divide 4?
- Does 0 divide 6?
- Does 1 divide 1?
- Does 5 divide 12?
- Does 12 divide 6?

Divisibility: Definition

Definition

Let $a,\ b \in \mathbb{Z}$. We say that a divides b if there exists an integer q such that $a \cdot q = b$.

- Does 6 divide 0? YES. Take $q = 0$, then $6 \cdot 0 = 0$
- What numbers divide 4? -4, -2, -1, 1, 2, 4
- Does 0 divide 6? NO. There's $q \in \mathbb{Z}$ such that $0 \cdot q = 6$.
- Does 1 divide 1? YES. Take $q = 1$, get $1 \cdot 1 = 1$.
- Does 5 divide 12? NO. There is no $q \in \mathbb{Z}$ such that $12 \cdot q = 5$.
- Does 12 divide 6? NO. There is no $q \in \mathbb{Z}$ such that $12 \cdot q = 6$.

Divisibility: Notation

Definition

Let $a,\ b \in \mathbb{Z}$. We say that a divides b and write $a|b$ if there exists an integer q such that $a \cdot q = b$. If a does not divide b, we write $a \not| b$.

- $6|0$
- $-4|4,\ -2|4,\ -1|4,\ 1|4,\ 2|4,\ 4|4$
- $0 \not| 6$
- $1|1$
- $5 \not| 12$
- $12 \not| 6$

Divisibility: Notation

Definition (Divisibility, in words)

Let $a,\ b \in \mathbb{Z}$. We say that a divides b and write $a|b$ if there exists an integer q such that $a \cdot q = b$. If a does not divide b, we write $a \not| b$.

Definition (Divisibility, in symbols)

Let $a,\ b \in \mathbb{Z}$. Then:

$$a|b \ \leftrightarrow \ \exists q \in \mathbb{Z},\ b = q \cdot a$$

Divisibility: Notation

Theorem

$\forall a, b, c \in \mathbb{Z}$:

$$(a|b) \land (b|c) \rightarrow \ a|c$$

Divisibility: Notation

Theorem

$\forall a, b, c \in \mathbb{Z}$:

$$(a|b) \land (b|c) \to \; a|c$$

Proof: We know that $a|b$ and $b|c$. So there exist some integers $q_1, \; q_2$ such that:

$$a \cdot q_1 = b$$

$$b \cdot q_2 = c.$$

Divisibility: Notation

Theorem

$\forall a, b, c \in \mathbb{Z}$:

$$(a|b) \land (b|c) \to \; a|c$$

Proof: We know that $a|b$ and $b|c$. So there exist some integers $q_1,\ q_2$ such that:

$$a \cdot q_1 = b$$

$$b \cdot q_2 = c.$$

Then $c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2)$.

Divisibility: Notation

Theorem

$\forall a, b, c \in \mathbb{Z}$:

$$(a|b) \wedge (b|c) \rightarrow \ a|c$$

Proof: We know that $a|b$ and $b|c$. So there exist some integers $q_1,\ q_2$ such that:

$$a \cdot q_1 = b$$

$$b \cdot q_2 = c.$$

Then $c = b \cdot q_2 = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2)$. Since the product $q_1 \cdot q_2$ is an integer, we get $a|c$. $\square$

Integer combination

Definition

Let $a, b \in \mathbb{Z}$. Then for all $x, y \in \mathbb{Z}$,

$$x \cdot a + y \cdot b$$

is an integer, and it is called an integer combination of a and b.

Example: for any $x, y \in \mathbb{Z}$,

$$x \cdot 5 + y \cdot 6$$

is an integer combination of 5 and 6.
Any integers acan be plugged in for x and y, for example:

$$0 \cdot 5 + 1 \cdot 6, \qquad -14 \cdot 5 + 23861 \cdot 6, \qquad 10 \cdot 5 - 90 \cdot 6 \ldots$$

Integer combination

Definition

Let $a, b \in \mathbb{Z}$. Then for all $x, y \in \mathbb{Z}$,

$$x \cdot a + y \cdot b$$

is an integer, and it is called an integer combination of a and b.

Example: for any $x, y \in \mathbb{Z}$,

$$x \cdot 5 + y \cdot 6$$

is an integer combination of 5 and 6.
If $c \in \mathbb{Z}$ divides both a and b, then c divides any integer combination of a and b.

Theorem

$\forall a, b, c \in \mathbb{Z}$, *if* c *divides both* a *and* b*, then* c *divides any integer combination of* a *and* b*.*

Proof:

Theorem

$\forall a, b, c \in \mathbb{Z}$, if c divides both a and b, then c divides any integer combination of a and b.

Proof: We know that $c|a$ and $c|b$. So there exist some integers $q_1,\ q_2$ such that

$$c \cdot q_1 = a,$$

$$c \cdot q_2 = b.$$

Theorem

$\forall a, b, c \in \mathbb{Z}$, if c divides both a and b, then c divides any integer combination of a and b.

Proof: We know that $c|a$ and $c|b$. So there exist some integers $q_1,\ q_2$ such that

$$c \cdot q_1 = a,$$

$$c \cdot q_2 = b.$$

Then for any integer combination $x \cdot a + y \cdot b$ we have:

$$x \cdot c \cdot q_1 + y \cdot c \cdot q_2 = c \cdot (x \cdot q_1 + y \cdot q_2)$$

And so, since $x \cdot q_1 + y \cdot q_2 \in \mathbb{Z}$, c divides $x \cdot a + y \cdot b$. $\square$

Remainders

Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q, r with $0 \leq r < b$ such that:

$$a = b \cdot q + r.$$

Remainders

Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q, r with $0 \leq r < b$ such that:

$$a = b \cdot q + r.$$

- If $0 \leq a < b$, what is q? What is r?
- If $a = -1$, what are q and r?
- Can you explain how we find q and r in general?

Induction and divisibility

Prove by induction that:

$$\forall n \in \mathbb{N},\ 3|(2^{2n} - 1).$$

Induction and divisibility

Prove by induction that:

$$\forall n \in \mathbb{N},\ 3|(2^{2n} - 1).$$

Base case: $n = 0$.

$$2^{2 \cdot 0} - 1 = 1 - 1 = 0 \checkmark$$

Induction and divisibility

Prove by induction that:

$$\forall n \in \mathbb{N},\ 3|(2^{2n} - 1).$$

Base case: $n = 0$.

$$2^{2\cdot 0} - 1 = 1 - 1 = 0 \checkmark$$

Inductive step: assume that $3|(2^{2n} - 1)$.
Want to show that $3|(2^{2(n+1)} - 1)$.

$$2^{2(n+1)} - 1 =$$

Induction and divisibility

Prove by induction that:

$$\forall n \in \mathbb{N},\ 3|(2^{2n} - 1).$$

Base case: $n = 0$.

$$2^{2\cdot 0} - 1 = 1 - 1 = 0 \checkmark$$

Inductive step: assume that $3|(2^{2n} - 1)$.
Want to show that $3|(2^{2(n+1)} - 1)$.

$$2^{2(n+1)} - 1 = 2^{2n+2} - 1 =$$

Induction and divisibility

Prove by induction that:

$$\forall n \in \mathbb{N},\ 3|(2^{2n} - 1).$$

Base case: Let $n = 0$.

$$2^{2\cdot 0} - 1 = 1 - 1 = 0 \checkmark$$

Inductive step: assume that for some $k \in \mathbb{N}$, $3|(2^{2k} - 1)$.
Want to show that $3|(2^{2(k+1)} - 1)$.

$$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4 \cdot 2^{2k} - 1 =$$

Induction and divisibility

Prove by induction that:

$$\forall n \in \mathbb{N},\ 3|(2^{2n} - 1).$$

Base case: $n = 0$.

$$2^{2\cdot 0} - 1 = 1 - 1 = 0 \checkmark$$

Inductive step: assume that for some $k \in \mathbb{N}$, $3|(2^{2k} - 1)$.
Want to show that $3|(2^{2(k+1)} - 1)$.

$$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4 \cdot 2^{2k} - 1 = 3 \cdot 2^{2k} + 2^{2k} - 1$$

Induction and divisibility

Prove by induction that:

$$\forall n \in \mathbb{N},\ 3|(2^{2n}-1).$$

Base case: $n = 0$.

$$2^{2\cdot 0} - 1 = 1 - 1 = 0 \checkmark$$

Inductive step: assume that for some $k \in \mathbb{N}$, $3|(2^{2k}-1)$.
Want to show that $3|(2^{2(k+1)}-1)$.

$$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4 \cdot 2^{2k} - 1 = 3 \cdot 2^{2k} + 2^{2k} - 1$$

$3 \cdot 2^{2k}$ has to be divisible by 3, since it's 3 times 2^{2k}, an integer.
$2^{2k} - 1$ is divisible by 3 by inductive hypothesis.
By the principle of mathematical induction, we conclude that $\forall n \in \mathbb{N},\ 3|(2^{2n}-1)$. $\square$

Set of divisors

Definition (divisor)

If $a, b \in \mathbb{Z}$ and $a|b$ then a is a divisor or b.

Definition (set of divisors)

We will denote the set of all divisors of b by D_b, with $a \in D_b$ if and only if a is a divisor of b.

Set of divisors

Definition (divisor)

If $a, b \in \mathbb{Z}$ and $a|b$ then a is a divisor or b.

Definition (set of divisors)

We will denote the set of all divisors of b by D_b, with $a \in D_b$ if and only if a is a divisor of b.

Examples:

$$D_4 = \{-4, -2, -1, 1, 2, 4\}$$

Common divisors

Definition (divisor)

If $a, b \in \mathbb{Z}$ and $a|b$ then a is a divisor or b.

Definition (set of divisors)

We will denote the set of all divisors of b by D_b, with $a \in D_b$ if and only if a is a divisor of b.

Examples:

$$D_4 = \{-4, -2, -1, 1, 2, 4\} = D_4 = \{\pm 1, \pm 2, \pm 4\}$$

Common divisors

Definition (divisor)

If $a, b \in \mathbb{Z}$ and $a|b$ then a is a divisor or b.

Definition (set of divisors)

We will denote the set of all divisors of b by D_b, with $a \in D_b$ if and only if a is a divisor of b.

Examples:

$$D_4 = \{-4, -2, -1, 1, 2, 4\} = D_4 = \{\pm 1, \pm 2, \pm 4\}$$

$$D_{15} = \{ \qquad\qquad\qquad \}$$

Set of divisors

Definition (divisor)

If $a, b \in \mathbb{Z}$ and $a|b$ then a is a divisor or b.

Definition (set of divisors)

We will denote the set of all divisors of b by D_b, with $a \in D_b$ if and only if a is a divisor of b.

Examples:

$$D_4 = \{-4, -2, -1, 1, 2, 4\} = D_4 = \{\pm 1, \pm 2, \pm 4\}$$

$$D_{15} = \{\pm 1, \pm 3, \pm 5, \pm 15\}$$

Set of divisors

Definition (divisor)

If $a, b \in \mathbb{Z}$ and $a|b$ then a is a divisor or b.

Definition (set of divisors)

We will denote the set of all divisors of b by D_b, with $a \in D_b$ if and only if a is a divisor of b.

Examples:

$$D_4 = \{-4, -2, -1, 1, 2, 4\} = D_4 = \{\pm 1, \pm 2, \pm 4\}$$

$$D_{15} = \{\pm 1, \pm 3, \pm 5, \pm 15\}$$

$$D_7 =$$

Set of divisors

Definition (divisor)

If $a, b \in \mathbb{Z}$ and $a|b$ then a is a divisor or b.

Definition (set of divisors)

We will denote the set of all divisors of b by D_b, with $a \in D_b$ if and only if a is a divisor of b.

Examples:

$$D_4 = \{-4, -2, -1, 1, 2, 4\} = D_4 = \{\pm 1, \pm 2, \pm 4\}$$

$$D_{15} = \{\pm 1, \pm 3, \pm 5, \pm 15\}$$

$$D_7 = \{\pm 1, \pm 7\}$$

Set of divisors: Exercise

List all (integer) divisors of these numbers:

- -12
- 113
- 100
- 112

Can you think of an efficient way to do this?

Set of divisors: Exercise

List all (integer) divisors of these numbers:

- -12 $D_{-12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$
- 113 $D_{113} = \{\pm 1, \pm 113\}$
- 100 $D_{100} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100\}$
- 112 $D_{112} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 16, \pm 28, \pm 56, \pm 112\}$

Can you think of an efficient way to do this?

Set of divisors: Exercise

List all (integer) divisors of these numbers:

- -12 $D_{-12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$
- 113 $D_{113} = \{\pm 1, \pm 113\}$
- $D_{100} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100\}$
- 112 $D_{112} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 16, \pm 28, \pm 56, \pm 112\}$

Can you think of an efficient way to do this?

$$112 = 2 \times 56$$

Set of divisors: Exercise

List all (integer) divisors of these numbers:

- -12 $D_{-12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$
- 113 $D_{113} = \{\pm 1, \pm 113\}$
- 100 $D_{100} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100\}$
- 112 $D_{112} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 16, \pm 28, \pm 56, \pm 112\}$

Can you think of an efficient way to do this?

$$112 = 2 \times 56$$

$$= 2 \times 2 \times 28$$

Set of divisors: Exercise

List all (integer) divisors of these numbers:

- -12 $D_{-12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$
- 113 $D_{113} = \{\pm 1, \pm 113\}$
- 100 $D_{100} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100\}$
- 112 $D_{112} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 16, \pm 28, \pm 56, \pm 112\}$

Can you think of an efficient way to do this?

$$112 = 2 \times 56$$

$$= 2 \times 2 \times 28$$

$$= 2 \times 2 \times 2 \times 2 \times 14$$

Set of divisors: Exercise

List all (integer) divisors of these numbers:

- -12 $D_{-12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$
- 113 $D_{113} = \{\pm 1, \pm 113\}$
- 100 $D_{100} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100\}$
- 112 $D_{112} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 16, \pm 28, \pm 56, \pm 112\}$

Can you think of an efficient way to do this?

$$112 = 2 \times 56$$

$$= 2 \times 2 \times 28$$

$$= 2 \times 2 \times 2 \times 2 \times 14$$

$$= 2 \times 2 \times 2 \times 2 \times 2 \times 7$$

Set of divisors: Exercise

List all (integer) divisors of these numbers:

- -12 $D_{-12} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$
- 113 $D_{113} = \{\pm 1, \pm 113\}$
- 100 $D_{100} = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20, \pm 25, \pm 50, \pm 100\}$
- 112 $D_{112} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 16, \pm 28, \pm 56, \pm 112\}$

Can you think of an efficient way to do this?

$$112 = 2 \times 56$$

$$= 2 \times 2 \times 28$$

$$= 2 \times 2 \times 2 \times 2 \times 14$$

$$= 2 \times 2 \times 2 \times 2 \times 2 \times 7$$

This is called the PRIME FACTORIZATION

Set of divisors

For any $b \in \mathbb{Z}$ such that $b \neq 0$, the set D_b is always finite.

$$D_b \subseteq \{\pm 1, \pm 2, \ldots, \pm b\}$$

Set of divisors

For any $b \in \mathbb{Z}$ such that $b \neq 0$, the set D_b is always finite.

$$D_b \subseteq \{\pm 1, \pm 2, \ldots, \pm b\}$$

± 1 and $\pm b$ are always in the set.

Set of divisors

For any $b \in \mathbb{Z}$ such that $b \neq 0$, the set D_b is always finite.

$$D_b \subseteq \{\pm 1, \pm 2, \ldots, \pm b\}$$

± 1 and $\pm b$ are always in the set D_b.
± 2 are in the set D_b if and only if b is even.

Set of divisors

For any $b \in \mathbb{Z}$ such that $b \neq 0$, the set D_b is always finite.

$$D_b \subseteq \{\pm 1, \pm 2, \ldots, \pm b\}$$

± 1 and $\pm b$ are always in the set D_b.
± 2 are in the set D_b if and only if b is even.

When $D_b = \{\pm 1, \ldots, \pm b\}$?

Set of divisors

For any $b \in \mathbb{Z}$ such that $b \neq 0$, the set D_b is always finite.

$$D_b \subseteq \{\pm 1, \pm 2, \ldots, \pm b\}$$

± 1 and $\pm b$ are always in the set D_b.
± 2 are in the set D_b if and only if b is even.

Proposition: $D_b = \{\pm 1, \ldots, \pm b\}$ is and only if $b \in \{\pm 1, \pm 2\}$.

Set of divisors

For any $b \in \mathbb{Z}$ such that $b \neq 0$, the set D_b is always finite.

$$D_b \subseteq \{\pm 1, \pm 2, \dots, \pm b\}$$

± 1 and $\pm b$ are always in the set D_b.
± 2 are in the set D_b if and only if b is even.

Proposition: $D_b = \{\pm 1, \dots, \pm b\}$ is and only if $b \in \{\pm 1, \pm 2\}$.

Proof outline: First the "if" part, i.e.
$b \in \{\pm 1, \pm 2\} \Rightarrow D_b = \{\pm 1, \dots, \pm b\}$:

$$D_1 = D_{-1} = \{\pm 1\}$$

$$D_2 = D_{-2} = \{\pm 1, \pm 2\}$$

Set of divisors

For any $b \in \mathbb{Z}$ such that $b \neq 0$, the set D_b is always finite.

$$D_b \subseteq \{\pm 1, \pm 2, \dots, \pm b\}$$

± 1 and $\pm b$ are always in the set D_b.
± 2 are in the set D_b if and only if b is even.

Proposition: $D_b = \{\pm 1, \dots, \pm b\}$ is and only if $b \in \{\pm 1, \pm 2\}$.

Proof outline: First the "if" part, i.e.
$b \in \{\pm 1, \pm 2\} \Rightarrow D_b = \{\pm 1, \dots, \pm b\}$:

$$D_1 = D_{-1} = \{\pm 1\} \checkmark$$

$$D_2 = D_{-2} = \{\pm 1, \pm 2\} \checkmark$$

Set of divisors

Proposition: $D_b = \{\pm 1, \ldots, \pm b\}$ is and only if $b \in \{\pm 1, \pm 2\}$.

Proof outline: First the "if" part, i.e.
$b \in \{\pm 1, \pm 2\} \Rightarrow D_b = \{\pm 1, \ldots, \pm b\}$:

$$D_1 = D_{-1} = \{\pm 1\} \checkmark$$

$$D_2 = D_{-2} = \{\pm 1, \pm 2\} \checkmark$$

Now the "only if" part, i.e. $D_b = \{\pm 1, \ldots, \pm b\} \Rightarrow b \in \{\pm 1, \pm 2\}$.

Suppose for contratiction that this is also true for some b, where $|b| \geq 3$. Let's split it up two cases: $b > 0$ and $b < 0$. In the first case, $b \geq 3$. Then if $D_b = \{\pm 1, \ldots, \pm b\} \Rightarrow b \in \{\pm 1, \pm 2\}$, we have $b - 1 | b$, so for some integer $q > 1$, $q \cdot (b-1) = b$. But if $q \geq 2$, $b \geq 3$, then $q \cdot (b-1) \geq 2b - 2 > b$. The other case is analogous.

Common divisors

If $a, b \in \mathbb{Z}$, and their sets of divisors are respectively D_a and D_b, then their common divisors are the elements of:

$$D_a \cap D_b$$

In other words, $d \in \mathbb{Z}$ is a common divisor of a and b if it divides both a and b.

Common divisors

If $a, b \in \mathbb{Z}$, and their sets of divisors are respectively D_a and D_b, then their common divisors are the elements of:

$$D_a \cap D_b$$

In other words, $d \in \mathbb{Z}$ is a common divisor of a and b if it divides both a and b.

For any $a, b \in \mathbb{Z}$, there exists a greatest common divisor, $GCD(a, b)$. It's the integer d that is the largest element of $D_a \cap D_b$.

Common divisors

If $a, b \in \mathbb{Z}$, and their sets of divisors are respectively D_a and D_b, then their common divisors are the elements of:

$$D_a \cap D_b$$

In other words, $d \in \mathbb{Z}$ is a common divisor of a and b if it divides both a and b.

Common divisors

If $a, b \in \mathbb{Z}$, and their sets of divisors are respectively D_a and D_b, then their common divisors are the elements of:

$$D_a \cap D_b$$

In other words, $d \in \mathbb{Z}$ is a common divisor of a and b if it divides both a and b.

For any $a, b \in \mathbb{Z}$, there exists a greatest common divisor, $GCD(a, b)$. It's the integer d that is the largest element of $D_a \cap D_b$.

Does d exist for any pair a, b?
Is d unique for any pair a, b?

Common divisors

If $a, b \in \mathbb{Z}$, and their sets of divisors are respectively D_a and D_b, then their common divisors are the elements of:

$$D_a \cap D_b$$

In other words, $d \in \mathbb{Z}$ is a common divisor of a and b if it divides both a and b.

For any $a, b \in \mathbb{Z}$, there exists a greatest common divisor, $GCD(a, b)$. It's the integer d that is the largest element of $D_a \cap D_b$.

Does d exist for any pair a, b?
Is d unique for any pair a, b?

Both of these things are true, so $d = GCD(a, b)$ is well-defined.

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Proof: We need to show that $GCD(b, r)$ divides a, b and also that it's the largest integer that does. It clearly divides b and r. Then, since a is an integer combination of b and r, it divides a.

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Proof: We need to show that $GCD(b, r)$ divides a, b and also that it's the largest integer that does. It clearly divides b and r. Then, since a is an integer combination of b and r, it divides a.

Now we know that $GDC(b, r)$ is a common divisor of a, b, we need to show it's the greatest one. So suppose for contradiction that there exists d such that $d|a$, $d|b$ and $d > GCD(b, r)$. So then $d \not| r$.

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Proof: We need to show that $GCD(b, r)$ divides a, b and also that it's the largest integer that does. It clearly divides b and r. Then, since a is an integer combination of b and r, it divides a.

Now we know that $GDC(b, r)$ is a common divisor of a, b, we need to show it's the greatest one. So suppose for contradiction that there exists d such that $d|a$, $d|b$ and $d > GCD(b, r)$. So then $d \not| r$.

But we have $a = q \cdot b + r$, so $a - q \cdot b = r$. d clearly divides the LHS, but not the RHS so they can't be equal! CONTRADICTION □

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Example: We want to find the $GCD(159, 15)$. We have $159 = 10 \cdot 15 + 9$.

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Example: We want to find the $GCD(159, 15)$. We have:

$$159 = 10 \cdot 15 + 9.$$

So according to the theorem,

$$GCD(159, 15) = GCD(15, 9) = 3.$$

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Example: We want to find the $GCD(159, 15)$. We have:

$$159 = 10 \cdot 15 + 9.$$

So according to the theorem,

$$GCD(159, 15) = GCD(15, 9) = 3.$$

If we weren't sure it's 3 yet, we can do one more step, because $15 = 9 + 6$:

$$GCD(159, 15) = GCD(15, 9) = GCD(9, 6)$$

Finding the Greatest Common Divisor (GCD)

Theorem

Let a, b, q, r be integers, a, b not both 0, such that $a = q \cdot b + r$. Then $GCD(a, b) = GCD(b, r)$.

Example: We want to find the $GCD(159, 15)$. We have:

$$159 = 10 \cdot 15 + 9.$$

So according to the theorem,

$$GCD(159, 15) = GCD(15, 9) = 3.$$

If we weren't sure it's 3 yet, we can do more steps, because $15 = 9 + 6$:

$$GCD(159, 15) = GCD(15, 9) = GCD(9, 6) = GCD(6, 3) = 3$$

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers a, b, $|a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers a, b, $|a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

$GCD(-4410, -5005) = GCD(4410, 5005)$

$5005 = 1 \cdot 4410 + 595$

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers a, b, $|a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

$GCD(-4410, -5005) = GCD(4410, 5005)$

$5005 = 1 \cdot 4410 + 595$

So $GCD(-4410, -5005) = GCD(4410, 595)$.

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers $a, b,\ |a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

$GCD(-4410, -5005) = GCD(4410, 5005)$

$5005 = 1 \cdot 4410 + 595$

$4410 = 7 \cdot 595 + 245$

So $GCD(-4410, -5005) = GCD(595, 245)$.

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers a, b, $|a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

$GCD(-4410, -5005) = GCD(4410, 5005)$

$5005 = 1 \cdot 4410 + 595$

$4410 = 7 \cdot 595 + 245$

$595 = 2 \cdot 245 + 105$

So $GCD(-4410, -5005) = GCD(245, 105)$.

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers $a, b,\ |a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

$GCD(-4410, -5005) = GCD(4410, 5005)$

$5005 = 1 \cdot 4410 + 595$

$4410 = 7 \cdot 595 + 245$

$595 = 2 \cdot 245 + 105$

$245 = 2 \cdot 105 + 35$

So $GCD(-4410, -5005) = GCD(105, 35)$.

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers a, b, $|a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

$GCD(-4410, -5005) = GCD(4410, 5005)$

$5005 = 1 \cdot 4410 + 595$

$4410 = 7 \cdot 595 + 245$

$595 = 2 \cdot 245 + 105$

$245 = 2 \cdot 105 + 35$

$105 = 3 \cdot 35$

So $GCD(-4410, -5005) = GCD(105, 35) =$.

Euclidean Algorithm

This is the Euclidean Algorithm. We can efficiently find the GCD of two integers $a, b,\ |a| > |b|$ by finding the integers q, r such that $a = q \cdot b + r$, and repeating the process until $r_i = 0$:

Example: find the $GCD(-4410, -5005)$.

$GCD(-4410, -5005) = GCD(4410, 5005)$

$5005 = 1 \cdot 4410 + 595$

$4410 = 7 \cdot 595 + 245$

$595 = 2 \cdot 245 + 105$

$245 = 2 \cdot 105 + 35$

$105 = 3 \cdot 35$

So $GCD(-4410, -5005) = GCD(105, 35) = 35.$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.

Go backwards with the Euclidean algorithm:

$5005 = 1 \cdot 4410 + 595$

$4410 = 7 \cdot 595 + 245$

$595 = 2 \cdot 245 + 105$

$245 = 2 \cdot 105 + 35$

$105 = 3 \cdot 35$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.

Go backwards with the Euclidean algorithm:

$5005 = 1 \cdot 4410 + 595$ $\qquad$ $595 = 5005 - 4410$

$4410 = 7 \cdot 595 + 245$

$595 = 2 \cdot 245 + 105$

$245 = 2 \cdot 105 + 35$

$105 = 3 \cdot 35$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.

Go backwards with the Euclidean algorithm:

$5005 = 1 \cdot 4410 + 595$ $\quad$ $595 = 5005 - 4410$

$4410 = 7 \cdot 595 + 245$ $\quad$ $245 = 4410 - 7 \cdot 595$

$595 = 2 \cdot 245 + 105$

$245 = 2 \cdot 105 + 35$

$105 = 3 \cdot 35$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.

Go backwards with the Euclidean algorithm:

$5005 = 1 \cdot 4410 + 595$ $\qquad$ $595 = 5005 - 4410$

$4410 = 7 \cdot 595 + 245$ $\qquad$ $245 = 4410 - 7 \cdot 595$

$$= 4410 - 7 \cdot (5005 - 4410)$$

$595 = 2 \cdot 245 + 105$ $\qquad$ $105 = 595 - 2 \cdot 245$

$245 = 2 \cdot 105 + 35$

$105 = 3 \cdot 35$

Good Characterization Theorem

$GCD(a, b)$ is an integer combination of a, b.

Go backwards with the Euclidean algorithm:

$$5005 = 1 \cdot 4410 + 595 \qquad 595 = 5005 - 4410$$

$$4410 = 7 \cdot 595 + 245 \qquad 245 = 4410 - 7 \cdot 595$$

$$= 4410 - 7 \cdot (5005 - 4410)$$

$$595 = 2 \cdot 245 + 105 \qquad 105 = 595 - 2 \cdot 245$$

$$245 = 2 \cdot 105 + 35 \qquad 35 = 245 - 2 \cdot 105$$

$$105 = 3 \cdot 35$$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.
Go backwards with the Euclidean algorithm:

$$5005 = 1 \cdot 4410 + 595 \qquad 595 = 5005 - 4410$$

$$4410 = 7 \cdot 595 + 245 \qquad 245 = 4410 - 7 \cdot 595$$

$$= 4410 - 7 \cdot (5005 - 4410)$$

$$595 = 2 \cdot 245 + 105 \qquad 105 = 595 - 2 \cdot 245$$

$$= 5005 - 4410 - 2 \cdot (4410 - 7 \cdot 595)$$

$$245 = 2 \cdot 105 + 35 \qquad 35 = 245 - 2 \cdot 105$$

$$105 = 3 \cdot 35$$

$$35 = 245 - 2 \cdot 105 =$$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.
Go backwards with the Euclidean algorithm:

$$5005 = 1 \cdot 4410 + 595 \qquad 595 = 5005 - 4410$$

$$4410 = 7 \cdot 595 + 245 \qquad 245 = 4410 - 7 \cdot 595$$
$$= 4410 - 7 \cdot (5005 - 4410)$$

$$595 = 2 \cdot 245 + 105 \qquad 105 = 595 - 2 \cdot 245$$
$$= 5005 - 4410 - 2 \cdot (4410 - 7 \cdot 595)$$

$$245 = 2 \cdot 105 + 35 \qquad 35 = 245 - 2 \cdot 105$$

$$105 = 3 \cdot 35$$

$$35 = 245 - 2 \cdot 105 = 4410 - 7 \cdot 595$$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.
Go backwards with the Euclidean algorithm:

$5005 = 1 \cdot 4410 + 595$ $\qquad$ $595 = 5005 - 4410$

$4410 = 7 \cdot 595 + 245$ $\qquad$ $245 = 4410 - 7 \cdot 595$
$$= 4410 - 7 \cdot (5005 - 4410)$$

$595 = 2 \cdot 245 + 105$ $\qquad$ $105 = 595 - 2 \cdot 245$
$$= 5005 - 3 \cdot 4410 + 14 \cdot 595$$

$245 = 2 \cdot 105 + 35$ $\qquad$ $35 = 245 - 2 \cdot 105$

$105 = 3 \cdot 35$

$$35 = 245 - 2 \cdot 105 = 4410 - 7 \cdot 595 - 2 \cdot (5005 - 3 \cdot 4410 + 14 \cdot 595)$$

the Extended Euclidean Algorithm

$GCD(a, b)$ is an integer combination of a, b.
Go backwards with the Euclidean algorithm:

$$5005 = 1 \cdot 4410 + 595 \qquad 595 = 5005 - 4410$$

$$4410 = 7 \cdot 595 + 245 \qquad 245 = 4410 - 7 \cdot 595$$

$$= 4410 - 7 \cdot (5005 - 4410)$$

$$595 = 2 \cdot 245 + 105 \qquad 105 = 595 - 2 \cdot 245$$

$$= 5005 - 3 \cdot 4410 + 14 \cdot 595$$

$$245 = 2 \cdot 105 + 35 \qquad 35 = 245 - 2 \cdot 105$$

$$105 = 3 \cdot 35$$

$$35 = 245 - 2 \cdot 105 = 4410 - 7 \cdot 595 - 2 \cdot (5005 - 3 \cdot 4410 + 14 \cdot 595)$$
$$= 8 \cdot 4410 - 7 \cdot 5005 - 2 \cdot (15 \cdot 5005 - 17 \cdot 4410)) = 42 \cdot 4410 - 37 \cdot 5005$$

Good Characterization Theorem

We just expressed $GCD(5005, 4410) = GCD(-5005, -4410)$ as a linear combination of $5005, 4410$ (and thus also a linear combination of $-5005, -4410$):

$$35 = 42 \cdot 4410 + (-37) \cdot 5005 = (-42) \cdot (-4410) + 37 \cdot (-5005)$$

using the Extended Euclidean Algorithm.

Theorem (Good Characterization Theorem)

Let a, b be integers not both 0. Then for an integer $d > 0$, we have:

$$d|a \text{ and } d|b \text{ and } d \text{ is an integer combiantion of } a, b$$

$$\Leftrightarrow d = GCD(a, b)$$

Good Characterization Theorem

Theorem (Good Characterization Theorem)

Let a, b be integers not both 0. Then for an integer $d > 0$, we have:

$$d|a \text{ and } d|b \text{ and } d \text{ is an integer combiantion of } a, b$$

$$\Leftrightarrow d = GCD(a, b)$$

By the Extended Euclidean Algorithm, we saw that we can express $GCD(a, b)$ as an integer combination of a, b. To convince ourselves that the Good Characterization Theorem is true, we need to show that no other positive common divisor of a, b can be expressed as an integer combination of a, b.

Good Characterization Theorem

Theorem (Good Characterization Theorem)

Let a, b be integers not both 0. Then for an integer $d > 0$, we have:

$$d|a \text{ and } d|b \text{ and } d \text{ is an integer combiantion of } a, b$$

$$\Leftrightarrow d = GCD(a, b)$$

By the Extended Euclidean Algorithm, we saw that we can express $GCD(a, b)$ as an integer combination of a, b. To convince ourselves that the Good Characterization Theorem is true, we need to show that no other positive common divisor of a, b can be expressed as an integer combination of a, b.

But any integer combination of a, b has to be divisible by $GCD(a, b)$!

Good Characterization Theorem

Theorem (Good Characterization Theorem)

Let a, b be integers not both 0. Then for an integer $d > 0$, we have:

$$d|a \text{ and } d|b \text{ and } d \text{ is an integer combiantion of } a, b$$

$$\Leftrightarrow d = GCD(a, b)$$

By the Extended Euclidean Algorithm, we saw that we can express $GCD(a, b)$ as an integer combination of a, b. To convince ourselves that the Good Characterization Theorem is true, we need to show that no other positive common divisor of a, b can be expressed as an integer combination of a, b.
But any integer combination of a, b has to be divisible by $GCD(a, b)$! Exercise: write out the formal proof.

Coprime integers

Definition

Two integers a, b are called coprime (or relatively prime) if $GCD(a, b) = 1$.

Coprime integers

Definition

Two integers a, b are called coprime (or relatively prime) if $GCD(a, b) = 1$.

- Are 13 and 60 coprime?
- Are 17 and 34 coprime?
- Can you find two even numbers that are coprime?
- If a, b are coprime, is 17 an integer combination of a and b?

Coprime integers

Definition

Two integers a, b are called coprime (or relatively prime) if $GCD(a, b) = 1$.

- Are 13 and 60 coprime? YES
- Are 17 and 34 coprime? NO, $GCD(17, 34) = 17$
- Can you find two even numbers that are coprime? NO
- If a, b are coprime, is 17 an integer combination of a and b?

Coprime integers

Definition

Two integers a, b are called coprime (or relatively prime) if $GCD(a, b) = 1$.

- Are 13 and 60 coprime? YES
- Are 17 and 34 coprime? NO, $GCD(17, 34) = 17$
- Can you find two even numbers that are coprime? NO
- If a, b are coprime, is 17 an integer combination of a and b?

Suppose a, b are coprime. Then by Good Characterization Theorem, 1 is an integer combination of a, b. So there exist some integers $q_1,\ q_2$ such that $1 = q_1 \cdot a + q_2 \cdot b$. Then:

$$17 = (17q_1) \cdot a + (17q_2) \cdot b.$$

Coprime integers

Definition

Two integers a, b are called coprime (or relatively prime) if $GCD(a, b) = 1$.

In other words, a, b are coprime iff 1 is an integer combination od a and b.
Equivalently, a, b are coprime iff any ($\forall$) integer c is an integer combination od a and b.

Coprime integers

Definition

Two integers a, b are called coprime (or relatively prime) if $GCD(a, b) = 1$.

In other words, a, b are coprime iff 1 is an integer combination od a and b.

Equivalently, a, b are coprime iff any ($\forall$) integer c is an integer combination od a and b.

Theorem

Let a, b, c be integers such that $c|ab$ and a, c are coprime, and $c \not| a$. Then $c|b$.

Example: if ab is even, and a is odd then b is even. $(c = 2)$

Theorem

Let a, b be integers not both 0. Then if $d = GCD(a, b)$, we have:

$$GCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Example: We know that $GCD(5005, 4410) = 35$. Then $\frac{5005}{35} = 143$ and $\frac{4410}{35} = 126$ are coprime.

Verify by the Euclidean Algorithm:

$143 = 126 + 17$

$126 = 7 \cdot 17 + 7$

$17 = 2 \cdot 7 + 3$

$7 = 2 \cdot 3 + 1$ ✓

Theorem

Let m, n, a be integers. Then if $m|a$, $n|a$, and $d = GCD(m, n)$, we have:

$$\frac{m \cdot n}{d} | a.$$

Example: Let $m = 4$, $n = 12$, $a = 24$. Then the premises are fulfilled, i.e. $4|24$ and $12|24$. Notice that $m \cdot n \not| a$. We have $d = GCD(4, 12) = 4$. Then:

$$\frac{m \cdot n}{d} = \frac{4 \cdot 12}{4} = 12,$$

and 12 indeed divides 24.

Corollary

In the setup above, if m, n are coprime then $m \cdot n|a$.

Linear Diophantine Equations

Definition

A linear equation with integer coefficients for which we are looking only for integer solutions is called a Linear Diophantine Equation (LDE.)

Examples:

- Find all integer solutions x, y of the equation $2x + 14y = 9$
- Find all integer solutions x, y of the equation $17x + 3y = 14$
- Find all integer solutions x of the equation $10x = 2015$

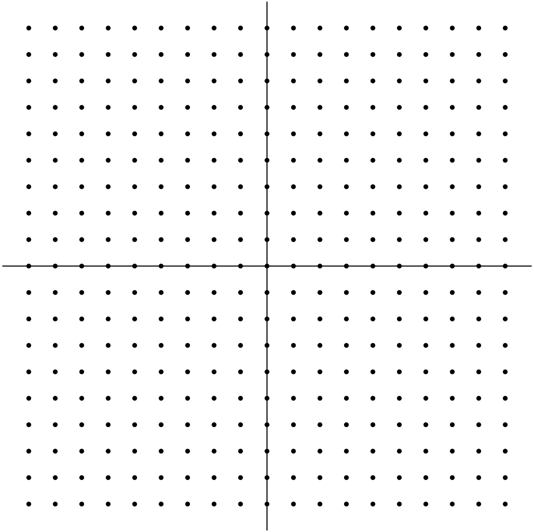
Linear Diophantione Equations

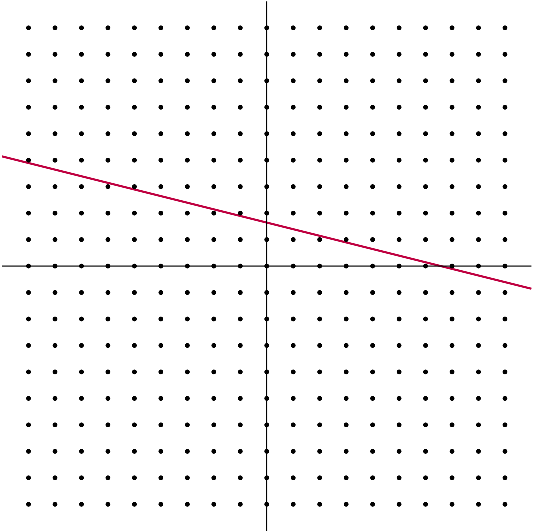
Definition

A linear equation with integer coefficients for which we are looking only for integer solutions is called a Linear Diophantine Equation (LDE.)

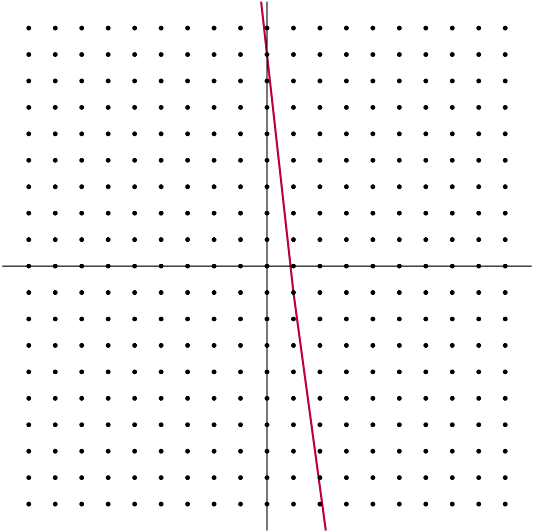
Examples:

- Find all integer solutions x, y of the equation $2x + 14y = 9$
  There are none. An integer combination of 2 and 14 will always be even.
- Find all integer solutions x, y of the equation $17x + 3y = 14$
  $x = 1,\ y = -1$ $\qquad$ $x = 4,\ y = -18$ $\qquad$ maybe more?
- Find all integer solutions x of the equation $10x = 2015$
  There are none. An equation of the form $ax = b,\ a, b \in \mathbb{Z}$ has integer solutions iff $a|b$.

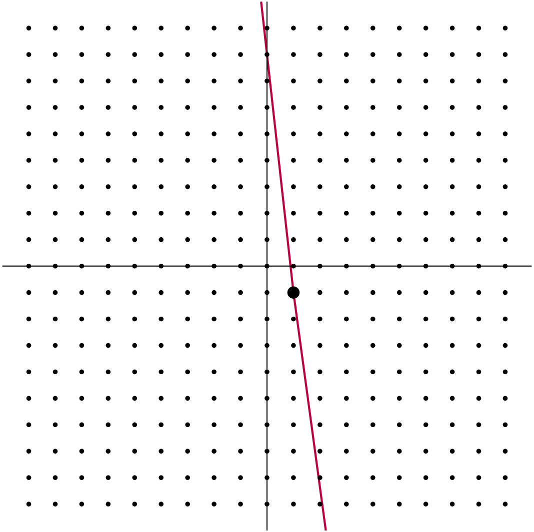




$$2x + 14y = 9$$



$$17x + 3y = 14$$



$$17x + 3y = 14$$

Complete solution of the LDE

Definition

For LDEs of the form $ax + by = c$, we call the set of its integer solutions

$$S = \{(x_i, y_i) \in \mathbb{Z} \times \mathbb{Z} : ax_i + by_i = c\}$$

the complete solution of the LDE.

- Infinitely many solutions exist if $GCD(a, b)|c$. Otherwise no solutions exist.
- If x_0, y_0 is a solution, then so is:

$$x_n = x_0 + \frac{b}{GCD(a,b)}n,\ \ y_n = y_0 - \frac{a}{GCD(a,b)}n \quad \text{for any } n \in \mathbb{Z}$$

Solving LDEs Summary

To solve a Linear Diophantine Equation given in the form

$$a \cdot x + b \cdot y = c,$$

you need to:

- Check that solutions exist (i.e. that $GCD(a, b)|c$)
- Express the $GCD(a, b)$ as a linear combination of a, b.
- Multiply this expression by $\frac{c}{GCD(a,b)}$ to get one solution.
- If x_0, y_0 is a solution, then so is:

$$x_n = x_0 + \frac{b}{GCD(a, b)}n, \; y_n = y_0 - \frac{a}{GCD(a, b)}n \quad \text{for any } n \in \mathbb{Z}$$

Your solution is an expression for the complete set.

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \; x, y \in \mathbb{Z}.$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \;\; x, y \in \mathbb{Z}.$$

First we need to find $GCD(97, 35)$ and make sure that it divides 13.

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \ \ x, y \in \mathbb{Z}.$$

First we need to find $GCD(97, 35)$ and make sure that it divides 13.

$97 = 2 \cdot 35 + 27$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \ \ x, y \in \mathbb{Z}.$$

First we need to find $GCD(97, 35)$ and make sure that it divides 13.

$97 = 2 \cdot 35 + 27$
$35 = 27 + 8$
$27 = 3 \cdot 8 + 3$
$8 = 2 \cdot 3 + 2$
$3 = 2 + 1$

$$GCD(97, 35) = 1$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \;\; x, y \in \mathbb{Z}.$$

First we need to find $GCD(97, 35)$ and make sure that it divides 13.

$97 = 2 \cdot 35 + 27$
$35 = 27 + 8$
$27 = 3 \cdot 8 + 3$
$8 = 2 \cdot 3 + 2$
$3 = 2 + 1$

$$GCD(97, 35) = 1$$

$$1 | 13 \checkmark$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \; x, y \in \mathbb{Z}.$$

First we need to find $GCD(97, 35)$ and make sure that it divides 13.

$$\begin{aligned}
97 &= 2 \cdot 35 + 27 & 27 &= 97 - 2 \cdot 35 \\
35 &= 27 + 8 & 8 &= 35 - 27 = 35 - (97 - 2 \cdot 35) = 3 \cdot 35 - 97 \\
27 &= 3 \cdot 8 + 3 & 3 &= 27 - 3 \cdot 8 = 4 \cdot 97 - 11 \cdot 35 \\
8 &= 2 \cdot 3 + 2 & 2 &= 8 - 2 \cdot 3 = 25 \cdot 35 - 9 \cdot 97 \\
3 &= 2 + 1 & 1 &= 3 - 2 = 13 \cdot 97 - 36 \cdot 35
\end{aligned}$$

$GCD(97, 35) = 1$

$$97 \cdot (13 \cdot 13) - 35 \cdot (36 \cdot 13) = 13$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13,\ \ x, y \in \mathbb{Z}.$$

First we need to find $GCD(97, 35)$ and make sure that it divides 13.

$97 = 2 \cdot 35 + 27$	$27 = 97 - 2 \cdot 35$
$35 = 27 + 8$	$8 = 35 - 27 = 35 - (97 - 2 \cdot 35) = 3 \cdot 35 - 97$
$27 = 3 \cdot 8 + 3$	$3 = 27 - 3 \cdot 8 = 4 \cdot 97 - 11 \cdot 35$
$8 = 2 \cdot 3 + 2$	$2 = 8 - 2 \cdot 3 = 25 \cdot 35 - 9 \cdot 97$
$3 = 2 + 1$	$1 = 3 - 2 = 13 \cdot 97 - 36 \cdot 35$
$GCD(97, 35) = 1$	

$$97 \cdot 169 - 35 \cdot 468 = 13$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \; x, y \in \mathbb{Z}.$$

So we found that one solution of this equation is:

$$x_0 = 169, \; y_0 = -468.$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \ \ x, y \in \mathbb{Z}.$$

So we found that one solution of this equation is:

$$x_0 = 169, \ \ y_0 = -468.$$

Then the complete set of solutions is

$$\{(x_n = x_0 + \frac{b}{GCD(a,b)}n, \ \ y_n = y_0 - \frac{a}{GCD(a,b)}n) \mid n \in \mathbb{Z}\}$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \ \ x, y \in \mathbb{Z}.$$

So we found that one solution of this equation is:

$$x_0 = 169, \ \ y_0 = -468.$$

Then the complete set of solutions is

$$\{(x_n = x_0 + 35 \cdot n, \ \ y_n = y_0 - 97 \cdot n) \mid n \in \mathbb{Z}\}$$

Example a)

Give the complete set of solutions of

$$97x + 35y = 13, \; x, y \in \mathbb{Z}.$$

So we found that one solution of this equation is:

$$x_0 = 169, \; y_0 = -468.$$

Then the complete set of solutions is

$$\{(x_n = 169 + 35 \cdot n, \; y_n = -468 - 97 \cdot n) \mid n \in \mathbb{Z}\}$$

Focus on the notation for a bit. Why is there a bracket around (x_n, y_n)?

Example a)

Give the complete set of solutions of

$$97x + 35y = 13,\ \ x, y \in \mathbb{Z}.$$

So we found that one solution of this equation is:

$$x_0 = 169,\ \ y_0 = -468.$$

Then the complete set of solutions is

$$\{(x_n = 169 + 35 \cdot n,\ \ y_n = -468 - 97 \cdot n) \mid n \in \mathbb{Z}\}$$

Focus on the notation for a bit. Why is there a bracket around (x_n, y_n)? It's a PAIR. Formally, we should write (x_0, y_0) too. In the set notation there is no room for informality!

Example b)

Give the complete set of solutions of

$$98x + 35y = 13, \;\; x, y \in \mathbb{Z}.$$

Example b)

Give the complete set of solutions of

$$98x + 35y = 13, \ \ x, y \in \mathbb{Z}.$$

First we need to find $GCD(98, 35)$ and make sure that it divides 13.

$98 = 2 \cdot 35 + 28$
$35 = 28 + 7$
$28 = 4 \cdot 7$

Example b)

Give the complete set of solutions of

$$98x + 35y = 13, \; x, y \in \mathbb{Z}.$$

First we need to find $GCD(98, 35)$ and make sure that it divides 13.

$98 = 2 \cdot 35 + 28$
$35 = 28 + 7$
$28 = 4 \cdot 7$

So $GCD(98, 35) = 7$. But $7 \not| 13$, so this equation has no solutions!

Example c)

Give the complete set of solutions of

$$258x + 147y = 369, \; x, y \in \mathbb{Z}.$$

Example c)

Give the complete set of solutions of

$$258x + 147y = 369, \ x, y \in \mathbb{Z}.$$

First we need to find $GCD(258, 147)$ and make sure that it divides 369.

Example c)

Give the complete set of solutions of

$$258x + 147y = 369, \; x, y \in \mathbb{Z}.$$

First we need to find $GCD(258, 147)$ and make sure that it divides 369.

$258 = 147 + 111$
$147 = 111 + 36$
$111 = 3 \cdot 36 + 3$
$36 = 12 \cdot 3$

So $GCD(258, 147) = 3$.

Example c)

Give the complete set of solutions of

$$258x + 147y = 369, \; x, y \in \mathbb{Z}.$$

First we need to find $GCD(258, 147)$ and make sure that it divides 369.

$258 = 147 + 111$
$147 = 111 + 36$
$111 = 3 \cdot 36 + 3$
$36 = 12 \cdot 3$

So $GCD(258, 147) = 3$.

$$3|369 \checkmark$$

Example c)

Give the complete set of solutions of

$$258x + 147y = 369, \;\; x, y \in \mathbb{Z}.$$

Now we need to express $GCD(258, 147)$ as a linear combination of 258 and 147.

$258 = 147 + 111$ 111=258-147

$147 = 111 + 36$ $36 = 147 - 111 = 2 \cdot 147 - 258$

$111 = 3 \cdot 36 + 3$ $3 = 111 - 3 \cdot 36 = 4 \cdot 258 - 7 \cdot 147$

$36 = 12 \cdot 3$

So $GCD(258, 147) = 3$.

$$3 | 369 \checkmark$$

Example c)

Give the complete set of solutions of

$$258x + 147y = 369,\ \ x, y \in \mathbb{Z}.$$

Now we need to express $GCD(258, 147)$ as a linear combination of 258 and 147.

$258 = 147 + 111$ | 111=258-147
$147 = 111 + 36$ | $36 = 147 - 111 = 2 \cdot 147 - 258$
$111 = 3 \cdot 36 + 3$ | $3 = 111 - 3 \cdot 36 = 4 \cdot 258 - 7 \cdot 147$
$36 = 12 \cdot 3$

$$\frac{369}{3} = 123$$

So:

$$258 \cdot (4 \cdot 123) + 147 \cdot (-7 \cdot 123) = 369$$

is a solution.

Example c)

Give the complete set of solutions of

$$258x + 147y = 369,\ \ x, y \in \mathbb{Z}.$$

Now we need to express $GCD(258, 147)$ as a linear combination of 258 and 147.

$258 = 147 + 111$ $\qquad$ 111=258-147

$147 = 111 + 36$ $\qquad$ $36 = 147 - 111 = 2 \cdot 147 - 258$

$111 = 3 \cdot 36 + 3$ $\qquad$ $3 = 111 - 3 \cdot 36 = 4 \cdot 258 - 7 \cdot 147$

$36 = 12 \cdot 3$

$$\frac{369}{3} = 123$$

So:

$$258 \cdot 492 + 147 \cdot (-861) = 369$$

is a solution.

Example c)

Give the complete set of solutions of

$$258x + 147y = 369,\ \ x, y \in \mathbb{Z}.$$

Now we know that

$$x_0 = 492,\ \ y_0 = -861$$

is a solution. Then so are all:

$$\{(x_n = \qquad\qquad\qquad\qquad ,\ \ y_n = \qquad\qquad\qquad\qquad \mid n \in \mathbb{Z}\}$$

Example c)

Give the complete set of solutions of

$$258x + 147y = 369,\ \ x, y \in \mathbb{Z}.$$

Now we know that

$$x_0 = 492,\ \ y_0 = -861$$

is a solution. Then so are all:

$$\{(x_n = 492 + \frac{147}{3}n,\ \ y_n = -861 - \frac{492}{3}n) \mid n \in \mathbb{Z}\}$$