Number Theory Chapter 1

Robert C. Vaughan

January 12, 2025

- We are motivated at this stage by wanting to understand the basic operations of addition and multiplication. The basic concept concerning multiplication is that of divisibility.

Divisibility

- We start with some definitions. We need some concept of divisibility and factorization.

Divisibility

- We start with some definitions. We need some concept of divisibility and factorization.
- Given two integers a and b we say that a divides b, if there is a third integer c such that

$$ac = b$$

and we write

$$a|b.$$

Divisibility

- We start with some definitions. We need some concept of divisibility and factorization.
- Given two integers a and b we say that a divides b, if there is a third integer c such that

$$ac = b$$

and we write

$$a|b.$$

- **Example.** If $a|b$ and $b|c$, then $a|c$.

Divisibility

- We start with some definitions. We need some concept of divisibility and factorization.
- Given two integers a and b we say that a divides b, if there is a third integer c such that

$$ac = b$$

and we write

$$a|b.$$

- **Example.** If $a|b$ and $b|c$, then $a|c$.
- **Proof.** There are d and e so that $b = ad$ and $c = be$. Hence $a(de) = (ad)e = be = c$ and de is an integer.

Divisibility

- There are some facts which are useful.

Divisibility

- There are some facts which are useful.
- For any a we have $0a = 0$.

Divisibility

- There are some facts which are useful.
- For any a we have $0a = 0$.
- If $ab = 1$, then $a = \pm 1$ and $b = \pm 1$ (with the same sign in each case).

Divisibility

- There are some facts which are useful.
- For any a we have $0a = 0$.
- If $ab = 1$, then $a = \pm 1$ and $b = \pm 1$ (with the same sign in each case).
- If $a \neq 0$ and $ac = ad$, then $c = d$.

Divisibility

Definition 1

A member of $\mathbb{N}$ greater than 1 which is only divisible by 1 and itself is called a prime number.

- We will use the letter p routinely to denote a prime number.

Divisibility

Definition 1

A member of $\mathbb{N}$ greater than 1 which is only divisible by 1 and itself is called a prime number.

- We will use the letter p routinely to denote a prime number.
- **Example.** 127 is a prime number.

Divisibility

Definition 1

A member of $\mathbb{N}$ greater than 1 which is only divisible by 1 and itself is called a prime number.

- We will use the letter p routinely to denote a prime number.
- **Example.** 127 is a prime number.
- **Proof.** How to prove this? Well obviously one only needs to check for divisors d with $1 < d < 127$.

Divisibility

Definition 1

A member of $\mathbb{N}$ greater than 1 which is only divisible by 1 and itself is called a prime number.

- We will use the letter p routinely to denote a prime number.
- **Example.** 127 is a prime number.
- **Proof.** How to prove this? Well obviously one only needs to check for divisors d with $1 < d < 127$.
- Moreover if $d|127$, then there is an $e = 127/d|127$ and one of d, e is $\leq \sqrt{127}$ so we only need to check out to 11.

Divisibility

Definition 1

A member of $\mathbb{N}$ greater than 1 which is only divisible by 1 and itself is called a prime number.

- We will use the letter p routinely to denote a prime number.
- **Example.** 127 is a prime number.
- **Proof.** How to prove this? Well obviously one only needs to check for divisors d with $1 < d < 127$.
- Moreover if $d|127$, then there is an $e = 127/d|127$ and one of d, e is $\leq \sqrt{127}$ so we only need to check out to 11.
- Oh, and really we only need to check $2, 3, 5, 7, 11$.

Divisibility

Definition 1

A member of $\mathbb{N}$ greater than 1 which is only divisible by 1 and itself is called a prime number.

- We will use the letter p routinely to denote a prime number.
- **Example.** 127 is a prime number.
- **Proof.** How to prove this? Well obviously one only needs to check for divisors d with $1 < d < 127$.
- Moreover if $d|127$, then there is an $e = 127/d|127$ and one of d, e is $\leq \sqrt{127}$ so we only need to check out to 11.
- Oh, and really we only need to check $2, 3, 5, 7, 11$.
- Also 2 and 5 are clearly not divisors and 3 is easily checked, so only 7 and 11 need any checking, and 7 leaves the remainder 1, not 0, and 11 the remainder 6.

Divisibility

- By the way, factorization and primality testing methods have important practical impact on some security systems.

Divisibility

- By the way, factorization and primality testing methods have important practical impact on some security systems.
- Factorization can be hard.

Divisibility

- By the way, factorization and primality testing methods have important practical impact on some security systems.
- Factorization can be hard.
- Here is an example. Is

$$5954579759875958495749857985958598$$
$$4759457948579595794859456799501$$

prime or composite?

Divisibility

- By the way, factorization and primality testing methods have important practical impact on some security systems.
- Factorization can be hard.
- Here is an example. Is

$$5954579759875958495749857985958598$$
$$4759457948579595794859456799501$$

prime or composite?

- Can you find a way to check this which is certain? Being wrong could be expensive - an employer might be very upset if you get it wrong! The method needs to be provably correct.

Divisibility

- By the way, factorization and primality testing methods have important practical impact on some security systems.
- Factorization can be hard.
- Here is an example. Is

$$595457975987595849574985798595859 8\\ 4759457948579595794859456799501$$

prime or composite?
- Can you find a way to check this which is certain? Being wrong could be expensive - an employer might be very upset if you get it wrong! The method needs to be provably correct.
- How about a number with 1000 digits?

Divisibility

- Since we are dealing with simple proofs for facts about $\mathbb{N}$ there is one proof method which is very important.

Divisibility

- Since we are dealing with simple proofs for facts about $\mathbb{N}$ there is one proof method which is very important.
- This is the principle of induction.

Divisibility

- Since we are dealing with simple proofs for facts about $\mathbb{N}$ there is one proof method which is very important.
- This is the principle of induction.
- It is actually embedded into the definition of $\mathbb{N}$.

Axioms for the Natural Numbers

- **The Peano axioms for $\mathbb{N}$.**

Axioms for the Natural Numbers

- **The Peano axioms for $\mathbb{N}$.**
- (i) 1 is a natural number.

Axioms for the Natural Numbers

- **The Peano axioms for $\mathbb{N}$.**
- (i) 1 is a natural number.
- (ii) If n is a natural number, then so is $n+1$, the successor of n.

Axioms for the Natural Numbers

- **The Peano axioms for $\mathbb{N}$.**
- (i) 1 is a natural number.
- (ii) If n is a natural number, then so is $n+1$, the successor of n.
- (iii) 1 is not the successor of any natural number.

Axioms for the Natural Numbers

- **The Peano axioms for $\mathbb{N}$.**
- (i) 1 is a natural number.
- (ii) If n is a natural number, then so is $n+1$, the successor of n.
- (iii) 1 is not the successor of any natural number.
- (iv) If $m+1=n+1$, then $m=n$.

Axioms for the Natural Numbers

- **The Peano axioms for $\mathbb{N}$.**
- (i) 1 is a natural number.
- (ii) If n is a natural number, then so is $n+1$, the successor of n.
- (iii) 1 is not the successor of any natural number.
- (iv) If $m+1=n+1$, then $m=n$.
- (v) **The Principle of Induction.** If a statement is true of 1 and if the truth of that statement for a number implies its truth for the successor of that number, then the statement is true for every natural number.

Axioms for the Natural Numbers

- **The Peano axioms for $\mathbb{N}$.**
- (i) 1 is a natural number.
- (ii) If n is a natural number, then so is $n+1$, the successor of n.
- (iii) 1 is not the successor of any natural number.
- (iv) If $m+1=n+1$, then $m=n$.
- (v) **The Principle of Induction.** If a statement is true of 1 and if the truth of that statement for a number implies its truth for the successor of that number, then the statement is true for every natural number.
- A statement which is provably equivalent is the **Well-ordering Principle** which says that any non-empty set of integers which is bounded below has a minimal element.

Primes and Factorization

- **Theorem.** Every member of $\mathbb{N}$ is a product of prime numbers.

Primes and Factorization

- **Theorem.** Every member of $\mathbb{N}$ is a product of prime numbers.
- **Proof.** 1 is an "empty product" of primes, so the case $n = 1$ holds.

Primes and Factorization

- **Theorem.** Every member of $\mathbb{N}$ is a product of prime numbers.
- **Proof.** 1 is an "empty product" of primes, so the case $n = 1$ holds.
- Suppose that we have proved the result for every m with $m \leq n$.

Primes and Factorization

- **Theorem.** Every member of $\mathbb{N}$ is a product of prime numbers.
- **Proof.** 1 is an "empty product" of primes, so the case $n = 1$ holds.
- Suppose that we have proved the result for every m with $m \leq n$.
- If $n + 1$ is prime we are done.

Primes and Factorization

- **Theorem.** Every member of $\mathbb{N}$ is a product of prime numbers.
- **Proof.** 1 is an "empty product" of primes, so the case $n = 1$ holds.
- Suppose that we have proved the result for every m with $m \le n$.
- If $n + 1$ is prime we are done.
- Suppose $n + 1$ is not prime. Then there is an a with $a | n + 1$ and $1 < a < n + 1$.

Primes and Factorization

- **Theorem.** Every member of $\mathbb{N}$ is a product of prime numbers.
- **Proof.** 1 is an "empty product" of primes, so the case $n = 1$ holds.
- Suppose that we have proved the result for every m with $m \leq n$.
- If $n + 1$ is prime we are done.
- Suppose $n + 1$ is not prime. Then there is an a with $a | n + 1$ and $1 < a < n + 1$.
- Then also $1 < \frac{n+1}{a} < n + 1$.

Primes and Factorization

- **Theorem.** Every member of $\mathbb{N}$ is a product of prime numbers.
- **Proof.** 1 is an "empty product" of primes, so the case $n = 1$ holds.
- Suppose that we have proved the result for every m with $m \le n$.
- If $n + 1$ is prime we are done.
- Suppose $n + 1$ is not prime. Then there is an a with $a|n + 1$ and $1 < a < n + 1$.
- Then also $1 < \frac{n+1}{a} < n + 1$.
- But then on the inductive hypothesis both a and $\frac{n+1}{a}$ are products of primes.

Primes and Factorization

- We can use this to prove the following.
  Theorem.[*Euclid*] There exist infinitely many primes.

Primes and Factorization

- We can use this to prove the following.
  Theorem.[*Euclid*] There exist infinitely many primes.
- **Proof.** We argue by contradiction.

Primes and Factorization

- We can use this to prove the following.
  Theorem.[*Euclid*] There exist infinitely many primes.
- **Proof.** We argue by contradiction.
- Suppose there are only a finite number of primes, say $p_1, p_2, \ldots, p_n$ and let

$$m = p_1 p_2 \ldots p_n + 1.$$

Primes and Factorization

- We can use this to prove the following.
  Theorem.[*Euclid*] There exist infinitely many primes.
- **Proof.** We argue by contradiction.
- Suppose there are only a finite number of primes, say $p_1, p_2, \ldots, p_n$ and let

$$m = p_1 p_2 \ldots p_n + 1.$$

- Since 2 is a prime we have $m > 1$.

Primes and Factorization

- We can use this to prove the following.
  Theorem.[*Euclid*] There exist infinitely many primes.
- **Proof.** We argue by contradiction.
- Suppose there are only a finite number of primes, say $p_1, p_2, \ldots, p_n$ and let

$$m = p_1 p_2 \ldots p_n + 1.$$

- Since 2 is a prime we have $m > 1$.
- By the previous theorem it is a product of primes, and in particular there is a prime p dividing m.

Primes and Factorization

- We can use this to prove the following.
  Theorem.[*Euclid*] There exist infinitely many primes.
- **Proof.** We argue by contradiction.
- Suppose there are only a finite number of primes, say $p_1, p_2, \ldots, p_n$ and let

$$m = p_1 p_2 \ldots p_n + 1.$$

- Since 2 is a prime we have $m > 1$.
- By the previous theorem it is a product of primes, and in particular there is a prime p dividing m.
- But p is one of the primes $p_1, p_2, \ldots, p_n$ so $p | m - p_1 p_2 \ldots p_n = 1$.

Primes and Factorization

- We can use this to prove the following.
  Theorem.[*Euclid*] There exist infinitely many primes.
- **Proof.** We argue by contradiction.
- Suppose there are only a finite number of primes, say $p_1, p_2, \ldots, p_n$ and let

$$m = p_1 p_2 \ldots p_n + 1.$$

- Since 2 is a prime we have $m > 1$.
- By the previous theorem it is a product of primes, and in particular there is a prime p dividing m.
- But p is one of the primes $p_1, p_2, \ldots, p_n$ so $p | m - p_1 p_2 \ldots p_n = 1$.
- But 1 is not divisible by any prime. So our assumption was false.

Dirichlet Box Principle

- Here is an idea which we will use multiple times during some of our simple proofs.

Dirichlet Box Principle

- Here is an idea which we will use multiple times during some of our simple proofs.
- **Example. Dirichlet's box principle**

Dirichlet Box Principle

- Here is an idea which we will use multiple times during some of our simple proofs.
- **Example. Dirichlet's box principle**
- *Suppose that we have n boxes and a collection of $n+1$ objects and we put the objects into boxes at random. Then one box will contain at least two objects.*

Dirichlet Box Principle

- Here is an idea which we will use multiple times during some of our simple proofs.
- **Example. Dirichlet's box principle**
- *Suppose that we have n boxes and a collection of $n + 1$ objects and we put the objects into boxes at random. Then one box will contain at least two objects.*
- **Proof.** The case $n = 1$ is obvious (I hope).

Dirichlet Box Principle

- Here is an idea which we will use multiple times during some of our simple proofs.
- **Example. Dirichlet's box principle**
- *Suppose that we have n boxes and a collection of $n+1$ objects and we put the objects into boxes at random. Then one box will contain at least two objects.*
- **Proof.** The case $n=1$ is obvious (I hope).
- Suppose the n-th case is already proven and now we have $n+1$ boxes and $n+2$ objects.

Dirichlet Box Principle

- Here is an idea which we will use multiple times during some of our simple proofs.
- **Example. Dirichlet's box principle**
- *Suppose that we have n boxes and a collection of $n+1$ objects and we put the objects into boxes at random. Then one box will contain at least two objects.*
- **Proof.** The case $n = 1$ is obvious (I hope).
- Suppose the n-th case is already proven and now we have $n+1$ boxes and $n+2$ objects.
- We argue by contradiction. Put the objects into the boxes at random and suppose that no box would have two objects in it.

Dirichlet Box Principle

- Here is an idea which we will use multiple times during some of our simple proofs.
- **Example. Dirichlet's box principle**
- *Suppose that we have* n *boxes and a collection of* $n+1$ *objects and we put the objects into boxes at random. Then one box will contain at least two objects.*
- **Proof.** The case $n=1$ is obvious (I hope).
- Suppose the n-th case is already proven and now we have $n+1$ boxes and $n+2$ objects.
- We argue by contradiction. Put the objects into the boxes at random and suppose that no box would have two objects in it.
- However even so at least one box would have one object in it. Remove that box. Now we have placed $n+1$ objects in the n remaining boxes and we have a contradiction to the case already proven.

Another Induction Example

- **Example.** The Fibonacci sequence is given by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$.

Another Induction Example

- **Example.** The Fibonacci sequence is given by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$.
- Show that if m, $n \in \mathbb{N}$ satisfy $m | F_n$ and $m | F_{n+1}$, then $m = 1$.

Another Induction Example

- **Example.** The Fibonacci sequence is given by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$.
- Show that if m, $n \in \mathbb{N}$ satisfy $m|F_n$ and $m|F_{n+1}$, then $m = 1$.
- We can use induction to give a proof.

Another Induction Example

- **Example.** The Fibonacci sequence is given by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$.
- Show that if m, $n \in \mathbb{N}$ satisfy $m|F_n$ and $m|F_{n+1}$, then $m = 1$.
- We can use induction to give a proof.
- **Proof.** We know that if $m \in \mathbb{N}$ and $m|1$, then $m = 1$, so this establishes the base case $n = 1$.

Another Induction Example

- **Example.** The Fibonacci sequence is given by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$.
- Show that if m, $n \in \mathbb{N}$ satisfy $m|F_n$ and $m|F_{n+1}$, then $m = 1$.
- We can use induction to give a proof.
- **Proof.** We know that if $m \in \mathbb{N}$ and $m|1$, then $m = 1$, so this establishes the base case $n = 1$.
- Suppose that we know that the n-th case holds and that $m \in \mathbb{N}$, $m|F_{n+2}$ and $m|F_{n+1}$.

Another Induction Example

- **Example.** The Fibonacci sequence is given by $F_1 = F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n = 2, 3, \ldots)$.
- Show that if m, $n \in \mathbb{N}$ satisfy $m|F_n$ and $m|F_{n+1}$, then $m = 1$.
- We can use induction to give a proof.
- **Proof.** We know that if $m \in \mathbb{N}$ and $m|1$, then $m = 1$, so this establishes the base case $n = 1$.
- Suppose that we know that the n-th case holds and that $m \in \mathbb{N}$, $m|F_{n+2}$ and $m|F_{n+1}$.
- Then $F_n = F_{n+2} - F_{n+1}$ and so $m|F_n$.

Another Induction Example

- **Example.** The Fibonacci sequence is given by $F_1 = F_2 = 1,\ F_{n+1} = F_n + F_{n-1}\ (n = 2, 3, \ldots)$.
- Show that if $m,\ n \in \mathbb{N}$ satisfy $m|F_n$ and $m|F_{n+1}$, then $m = 1$.
- We can use induction to give a proof.
- **Proof.** We know that if $m \in \mathbb{N}$ and $m|1$, then $m = 1$, so this establishes the base case $n = 1$.
- Suppose that we know that the n-th case holds and that $m \in \mathbb{N}$, $m|F_{n+2}$ and $m|F_{n+1}$.
- Then $F_n = F_{n+2} - F_{n+1}$ and so $m|F_n$.
- Hence, by the inductive hypothesis $m = 1$.

Divisibility Example

- **Example.** Show that $n|(n-1)!$ for all composite $n > 4$.

Divisibility Example

- **Example.** Show that $n|(n-1)!$ for all composite $n > 4$.
- Here we can just use the divisibility properties.

Divisibility Example

- **Example.** Show that $n|(n-1)!$ for all composite $n > 4$.
- Here we can just use the divisibility properties.
- **Proof.** Since n is composite we have $n = ab$ with $1 < a \le b < n$.

Divisibility Example

- **Example.** Show that $n|(n-1)!$ for all composite $n > 4$.
- Here we can just use the divisibility properties.
- **Proof.** Since n is composite we have $n = ab$ with $1 < a \leq b < n$.
- If $a \neq b$, then a and b occur as separate factors in $(n-1)! = 1.2.3...(n-1)$ and we are done.

Divisibility Example

- **Example.** Show that $n|(n-1)!$ for all composite $n > 4$.
- Here we can just use the divisibility properties.
- **Proof.** Since n is composite we have $n = ab$ with $1 < a \le b < n$.
- If $a \ne b$, then a and b occur as separate factors in $(n-1)! = 1.2.3...(n-1)$ and we are done.
- Thus we may suppose that $n = a^2$.

Divisibility Example

- **Example.** Show that $n|(n-1)!$ for all composite $n > 4$.
- Here we can just use the divisibility properties.
- **Proof.** Since n is composite we have $n = ab$ with $1 < a \le b < n$.
- If $a \ne b$, then a and b occur as separate factors in $(n-1)! = 1.2.3...(n-1)$ and we are done.
- Thus we may suppose that $n = a^2$.
- Since $n > 4$ we have $a > 2$. Thus $1 < a < 2a < a^2 = n$, so a and $2a$ are separate factors of $(n-1)!$.

The Division Algorithm

- We now come to something very important

The Division Algorithm

- We now come to something very important
- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

The Division Algorithm

- We now come to something very important
- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- The number q is called the quotient and r the remainder. By the way, it is exactly this which one uses when one performs long division.

The Division Algorithm

- We now come to something very important
- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique $q, r \in \mathbb{Z}$ such that

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

- The number q is called the quotient and r the remainder. By the way, it is exactly this which one uses when one performs long division.
- **Example.** Try dividing 19 into 192837465 by the method you were taught at grade school.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- **Proof.** We have two tasks, to existence & uniqueness.

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- **Proof.** We have two tasks, to existence & uniqueness.
- *Existence.* Define $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- **Proof.** We have two tasks, to existence & uniqueness.
- *Existence.* Define $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, then $a - d(-1) \in \mathcal{D}$ and $a - d(-1) = a + d > 0$, and if $a < 0$, then $a - d(a-1) = (d-1)(-a) + d > 0$.

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- **Proof.** We have two tasks, to existence & uniqueness.
- *Existence.* Define $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, then $a - d(-1) \in \mathcal{D}$ and $a - d(-1) = a + d > 0$, and if $a < 0$, then $a - d(a - 1) = (d - 1)(-a) + d > 0$.
- Hence $\mathcal{D}$ contains positive integers.

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- **Proof.** We have two tasks, to existence & uniqueness.
- *Existence.* Define $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, then $a - d(-1) \in \mathcal{D}$ and $a - d(-1) = a + d > 0$, and if $a < 0$, then $a - d(a-1) = (d-1)(-a) + d > 0$.
- Hence $\mathcal{D}$ contains positive integers.
- Let $\mathcal{D}^* = \mathcal{D} \cap \mathbb{N}$.

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- **Proof.** We have two tasks, to existence & uniqueness.
- *Existence.* Define $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, then $a - d(-1) \in \mathcal{D}$ and $a - d(-1) = a + d > 0$, and if $a < 0$, then $a - d(a-1) = (d-1)(-a) + d > 0$.
- Hence $\mathcal{D}$ contains positive integers.
- Let $\mathcal{D}^* = \mathcal{D} \cap \mathbb{N}$.
- Then $\mathcal{D}^*$ is bounded below and non-empty, so by the well-ordering principle it has a minimum.

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- **Proof.** We have two tasks, to existence & uniqueness.
- *Existence.* Define $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, then $a - d(-1) \in \mathcal{D}$ and $a - d(-1) = a + d > 0$, and if $a < 0$, then $a - d(a-1) = (d-1)(-a) + d > 0$.
- Hence $\mathcal{D}$ contains positive integers.
- Let $\mathcal{D}^* = \mathcal{D} \cap \mathbb{N}$.
- Then $\mathcal{D}^*$ is bounded below and non-empty, so by the well-ordering principle it has a minimum.
- Let r denote this minimum, and let q be the corresponding value of x. Then $a = dq + r, \quad 0 \le r$.

- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that
$$a = dq + r, \quad 0 \le r < d.$$
- **Proof.** We have two tasks, to existence & uniqueness.
- *Existence.* Define $\mathcal{D} = \{a - dx : x \in \mathbb{Z}\}$.
- If $a \ge 0$, then $a - d(-1) \in \mathcal{D}$ and $a - d(-1) = a + d > 0$, and if $a < 0$, then $a - d(a - 1) = (d - 1)(-a) + d > 0$.
- Hence $\mathcal{D}$ contains positive integers.
- Let $\mathcal{D}^* = \mathcal{D} \cap \mathbb{N}$.
- Then $\mathcal{D}^*$ is bounded below and non-empty, so by the well-ordering principle it has a minimum.
- Let r denote this minimum, and let q be the corresponding value of x. Then $a = dq + r, \quad 0 \le r$.
- If $r \ge d$, then $a = d(q + 1) + (r - d)$ is another solution, but $r - d < r$ contradicting the minimality of r.
- Hence $r < d$ as required.

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- *Uniqueness.* Observe that if we have a second solution

$$a = dq' + r', \quad 0 \le r' < d, \quad q' \ne q,$$

then

$$0 = a - a = (dq' + r') - (dq + r) = d(q' - q) + (r' - r).$$

The Division Algorithm

- **Theorem.** *The division algorithm.* Suppose that $a \in \mathbb{Z}$ and $d \in \mathbb{N}$. Then there are unique q, $r \in \mathbb{Z}$ such that

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

- *Uniqueness.* Observe that if we have a second solution

$$a = dq' + r', \quad 0 \le r' < d, \quad q' \ne q,$$

then

$$0 = a - a = (dq' + r') - (dq + r) = d(q' - q) + (r' - r).$$

- Then we would have

$$d \le d|q' - q| = |r' - r| < d$$

which is impossible.

- We will make frequent use of the division algorithm as well as the next theorem.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a, b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a, b)$ has positive elements. Let (a, b) denote its least positive element. Then (a, b) has the properties
(i) $(a, b)|a$,
(ii) $(a, b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a, b)$.

- **Definition.** *We call (a, b) the greatest common divisor of a and b, often abbreviated to gcd or GCD. The symbol (a, b) has many uses in mathematics, so to be clear one sometimes writes*

$$gcd(a, b) \text{ or } GCD(a, b).$$

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ *has positive elements. Let* (a,b) *denote its least positive element. Then* (a,b) *has the properties*
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c *satisfies* $c|a$ *and* $c|b$, *then* $c|(a,b)$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b)=\{ax+by : x\in\mathbb{Z}, y\in\mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

- **Proof.** Existence.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a, b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a, b)$ has positive elements. Let (a, b) denote its least positive element. Then (a, b) has the properties
(i) $(a, b)|a$,
(ii) $(a, b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a, b)$.

- **Proof.** Existence.
- If a is positive, then so is $a.1 + b.0$. Likewise if b is positive. If a is negative, then $a(-1) + b.0$ is positive, and again likewise if b is negative. The only remaining case is $a = b = 0$ which is expressly excluded. Thus $\mathcal{D}(a, b)$ does indeed have positive elements. Thus (a, b) exists.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

- *Properties.* Suppose (i) is false. By the division algorithm we have $a = (a,b)q + r$ with $0 \le r < (a,b)$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a, b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a, b)$ has positive elements. Let (a, b) denote its least positive element. Then (a, b) has the properties
(i) $(a, b)|a$,
(ii) $(a, b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a, b)$.

- *Properties.* Suppose (i) is false. By the division algorithm we have $a = (a, b)q + r$ with $0 \le r < (a, b)$.
- But the falsity of (i) means that $0 < r$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.
- *Properties.* Suppose (i) is false. By the division algorithm we have $a = (a,b)q + r$ with $0 \le r < (a,b)$.
- But the falsity of (i) means that $0 < r$.
- Thus $r = a - (a,b)q = a - (ax + by)q$ for some integers x and y.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

- *Properties.* Suppose (i) is false. By the division algorithm we have $a = (a,b)q + r$ with $0 \le r < (a,b)$.
- But the falsity of (i) means that $0 < r$.
- Thus $r = a - (a,b)q = a - (ax + by)q$ for some integers x and y.
- Hence $r = a(1 - xq) + b(-yq)$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.
- *Properties.* Suppose (i) is false. By the division algorithm we have $a = (a,b)q + r$ with $0 \le r < (a,b)$.
- But the falsity of (i) means that $0 < r$.
- Thus $r = a - (a,b)q = a - (ax + by)q$ for some integers x and y.
- Hence $r = a(1 - xq) + b(-yq)$.
- Since $0 < r < (a,b)$ this contradicts the minimality of (a,b).

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

  Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
  (i) $(a,b)|a$,
  (ii) $(a,b)|b$,
  (iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.
- *Properties.* Suppose (i) is false. By the division algorithm we have $a = (a,b)q + r$ with $0 \le r < (a,b)$.
- But the falsity of (i) means that $0 < r$.
- Thus $r = a - (a,b)q = a - (ax + by)q$ for some integers x and y.
- Hence $r = a(1 - xq) + b(-yq)$.
- Since $0 < r < (a,b)$ this contradicts the minimality of (a,b).
- Likewise for (ii).

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ *has positive elements. Let* (a,b) *denote its least positive element. Then* (a,b) *has the properties*
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c *satisfies* $c|a$ *and* $c|b$*, then* $c|(a,b)$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ *has positive elements. Let* (a,b) *denote its least positive element. Then* (a,b) *has the properties*
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c *satisfies* $c|a$ *and* $c|b$*, then* $c|(a,b)$*.*

- *Properties.* (iii) if the integer c satisfies $c|a$ and $c|b$, then $a = cu$ and $b = cv$ for some integers u and v.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b)=\{ax+by : x\in\mathbb{Z}, y\in\mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

- *Properties.* (iii) if the integer c satisfies $c|a$ and $c|b$, then $a=cu$ and $b=cv$ for some integers u and v.
- and for some integers x and y we have $(a,b)=ax+by$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

- *Properties.* (iii) if the integer c satisfies $c|a$ and $c|b$, then $a = cu$ and $b = cv$ for some integers u and v.
- and for some integers x and y we have $(a,b) = ax + by$.
- Thus

$$(a,b) = ax + by = cux + cvy = c(ux + vy)$$

so (iii) holds.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
- To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, then $d|\frac{a}{(a,b)}$ and $d|\frac{b}{(a,b)}$, and hence $d(a,b)|a$ and $d(a,b)|b$.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
- To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, then $d|\frac{a}{(a,b)}$ and $d|\frac{b}{(a,b)}$, and hence $d(a,b)|a$ and $d(a,b)|b$.
- But then $d(a,b)|(a,b)$ and so $d|1$, whence $d = 1$.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
- To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, then $d|\frac{a}{(a,b)}$ and $d|\frac{b}{(a,b)}$, and hence $d(a,b)|a$ and $d(a,b)|b$.
- But then $d(a,b)|(a,b)$ and so $d|1$, whence $d = 1$.
- **Example.** Suppose that a and b are not both 0. Then for any integer x we have $(a + bx, b) = (a, b)$.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
- To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, then $d|\frac{a}{(a,b)}$ and $d|\frac{b}{(a,b)}$, and hence $d(a,b)|a$ and $d(a,b)|b$.
- But then $d(a,b)|(a,b)$ and so $d|1$, whence $d = 1$.
- **Example.** Suppose that a and b are not both 0. Then for any integer x we have $(a + bx, b) = (a, b)$.
- Here is a proof. First of all $(a,b)|a$ and $(a,b)|b$, so $(a,b)|a + bx$.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
- To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, then $d|\frac{a}{(a,b)}$ and $d|\frac{b}{(a,b)}$, and hence $d(a,b)|a$ and $d(a,b)|b$.
- But then $d(a,b)|(a,b)$ and so $d|1$, whence $d = 1$.
- **Example.** Suppose that a and b are not both 0. Then for any integer x we have $(a+bx, b) = (a,b)$.
- Here is a proof. First of all $(a,b)|a$ and $(a,b)|b$, so $(a,b)|a+bx$.
- Hence $(a,b)|(a+bx, b)$.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
- To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, then $d | \frac{a}{(a,b)}$ and $d | \frac{b}{(a,b)}$, and hence $d(a,b)|a$ and $d(a,b)|b$.
- But then $d(a,b)|(a,b)$ and so $d|1$, whence $d = 1$.
- **Example.** Suppose that a and b are not both 0. Then for any integer x we have $(a + bx, b) = (a, b)$.
- Here is a proof. First of all $(a,b)|a$ and $(a,b)|b$, so $(a,b)|a + bx$.
- Hence $(a,b)|(a + bx, b)$.
- On the other hand $(a + bx, b)|a + bx$ and $(a + bx, b)|b$ so that $(a + bx)|a + bx - bx = a$.

The Greatest Common Divisor

- The GCD has some interesting properties. Here are two.
- **Example.** We have $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
- To see this observe that if $d = \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$, then $d|\frac{a}{(a,b)}$ and $d|\frac{b}{(a,b)}$, and hence $d(a,b)|a$ and $d(a,b)|b$.
- But then $d(a,b)|(a,b)$ and so $d|1$, whence $d = 1$.
- **Example.** Suppose that a and b are not both 0. Then for any integer x we have $(a+bx, b) = (a, b)$.
- Here is a proof. First of all $(a,b)|a$ and $(a,b)|b$, so $(a,b)|a+bx$.
- Hence $(a,b)|(a+bx, b)$.
- On the other hand $(a+bx,b)|a+bx$ and $(a+bx,b)|b$ so that $(a+bx)|a+bx-bx = a$.
- Hence $(a+bx,b)|(a,b)|(a+bx,b)$ and so $(a,b) = (a+bx,b)$.

The Greatest Common Divisor

- Here is another.

The Greatest Common Divisor

- Here is another.
- **Example.** *Suppose that* $(a, b) = 1$ *and* $ax = by$.

The Greatest Common Divisor

- Here is another.
- **Example.** *Suppose that* $(a, b) = 1$ *and* $ax = by$*.*
- *Then there is a* z *such that* $x = bz$*,* $y = az$*.*

The Greatest Common Divisor

- Here is another.
- **Example.** *Suppose that* $(a, b) = 1$ *and* $ax = by$*.*
- *Then there is a* z *such that* $x = bz$*,* $y = az$*.*
- It suffices to show that $b|x$, for then the conclusion follows on taking $z = x/b$.

The Greatest Common Divisor

- Here is another.
- **Example.** *Suppose that* $(a, b) = 1$ *and* $ax = by$.
- *Then there is a* z *such that* $x = bz$, $y = az$.
- It suffices to show that $b|x$, for then the conclusion follows on taking $z = x/b$.
- To see this observe that there are u and v so that $au + bv = (a, b) = 1$. Hence $x = aux + bvx = byu + bvx = b(yu + vx)$ and so $b|x$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both* 0*, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ *has positive elements. Let* (a,b) *denote its least positive element. Then* (a,b) *has the properties*
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ *and* $c|b$*, then* $c|(a,b)$.

- From the above we immediately have the following

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a, b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a, b)$ has positive elements. Let (a, b) denote its least positive element. Then (a, b) has the properties
(i) $(a, b)|a$,
(ii) $(a, b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a, b)$.

- From the above we immediately have the following
- **Corollary.** Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

- From the above we immediately have the following
- **Corollary.** Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

- Later we will look at a way of finding suitable x and y in examples.

The Greatest Common Divisor

- **Theorem.** *Given two integers a and b, not both 0, define*

$$\mathcal{D}(a,b) = \{ax + by : x \in \mathbb{Z}, y \in \mathbb{Z}\}.$$

Then $\mathcal{D}(a,b)$ has positive elements. Let (a,b) denote its least positive element. Then (a,b) has the properties
(i) $(a,b)|a$,
(ii) $(a,b)|b$,
(iii) if c satisfies $c|a$ and $c|b$, then $c|(a,b)$.

- From the above we immediately have the following
- **Corollary.** Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

- Later we will look at a way of finding suitable x and y in examples.
- As it stands the theorem gives no simple constructive way of finding them. It is a pure existence proof.

The Greatest Common Divisor

- **Corollary.** Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

The Greatest Common Divisor

- **Corollary.** Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

- As a first application of the corollary we establish

The Greatest Common Divisor

- **Corollary.** Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

- As a first application of the corollary we establish
- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.

The Greatest Common Divisor

- **Corollary.** Suppose that a and b are integers not both 0. Then there are integers x and y such that

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

- As a first application of the corollary we establish
- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- You might think this is obvious, but .....

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k + 1$.

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k+1$.
- If you multiply two together, e.g. $(4k_1+1)(4k_2+1) = 16k_1k_2 + 4k_2 + 4k_1 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$ you get another of the same kind.

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k+1$.
- If you multiply two together, e.g. $(4k_1+1)(4k_2+1) = 16k_1k_2 + 4k_2 + 4k_1 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$ you get another of the same kind.
- So $\mathcal{A}$ has "closure" under multiplication.

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k+1$.
- If you multiply two together, e.g. $(4k_1+1)(4k_2+1) = 16k_1k_2+4k_2+4k_1+1 = 4(4k_1k_2+k_1+k_2)+1$ you get another of the same kind.
- So $\mathcal{A}$ has "closure" under multiplication.
- We can define a "prime" p in this system if it is only divisible by 1 and itself in the system.

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k+1$.
- If you multiply two together, e.g. $(4k_1+1)(4k_2+1) = 16k_1k_2 + 4k_2 + 4k_1 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$ you get another of the same kind.
- So $\mathcal{A}$ has "closure" under multiplication.
- We can define a "prime" p in this system if it is only divisible by 1 and itself in the system.
- Here is a list of "primes" in $\mathcal{A}$.

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49 \ldots$$

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k+1$.
- If you multiply two together, e.g. $(4k_1+1)(4k_2+1) = 16k_1k_2+4k_2+4k_1+1 = 4(4k_1k_2+k_1+k_2)+1$ you get another of the same kind.
- So $\mathcal{A}$ has "closure" under multiplication.
- We can define a "prime" p in this system if it is only divisible by 1 and itself in the system.
- Here is a list of "primes" in $\mathcal{A}$.

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49 \ldots$$

- Thus 9, 21 and 49 are primes in $\mathcal{A}$ because 3 and 7 are not in $\mathcal{A}$.

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k + 1$.
- If you multiply two together, e.g. $(4k_1 + 1)(4k_2 + 1) = 16k_1k_2 + 4k_2 + 4k_1 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$ you get another of the same kind.
- So $\mathcal{A}$ has “closure” under multiplication.
- We can define a “prime” p in this system if it is only divisible by 1 and itself in the system.
- Here is a list of “primes” in $\mathcal{A}$.

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49 \ldots$$

- Thus 9, 21 and 49 are primes in $\mathcal{A}$ because 3 and 7 are not in $\mathcal{A}$.
- Now look at 441.

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k+1$.
- If you multiply two together, e.g. $(4k_1+1)(4k_2+1) = 16k_1k_2+4k_2+4k_1+1 = 4(4k_1k_2+k_1+k_2)+1$ you get another of the same kind.
- So $\mathcal{A}$ has "closure" under multiplication.
- We can define a "prime" p in this system if it is only divisible by 1 and itself in the system.
- Here is a list of "primes" in $\mathcal{A}$.

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49 \ldots$$

- Thus 9, 21 and 49 are primes in $\mathcal{A}$ because 3 and 7 are not in $\mathcal{A}$.
- Now look at 441.
- We have

$$441 = 9 \times 49 = 21^2.$$

So, in $\mathcal{A}$ factorisation is not unique!.

An Example

- Consider the set $\mathcal{A}$ of integers of the form $4k + 1$.
- If you multiply two together, e.g. $(4k_1 + 1)(4k_2 + 1) = 16k_1k_2 + 4k_2 + 4k_1 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$ you get another of the same kind.
- So $\mathcal{A}$ has "closure" under multiplication.
- We can define a "prime" p in this system if it is only divisible by 1 and itself in the system.
- Here is a list of "primes" in $\mathcal{A}$.

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49 \ldots$$

- Thus 9, 21 and 49 are primes in $\mathcal{A}$ because 3 and 7 are not in $\mathcal{A}$.
- Now look at 441.
- We have

$$441 = 9 \times 49 = 21^2.$$

So, in $\mathcal{A}$ factorisation is not unique!.
- Moreover $9|21^2$ but $9 \nmid 21$.

An Example

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?

An Example

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?
- Well $\mathbb{Z}$ has an additive structure and $\mathcal{A}$ does not.

An Example

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?
- Well $\mathbb{Z}$ has an additive structure and $\mathcal{A}$ does not.
- Add two members of $\mathbb{Z}$ and you get another one.

An Example

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?
- Well $\mathbb{Z}$ has an additive structure and $\mathcal{A}$ does not.
- Add two members of $\mathbb{Z}$ and you get another one.
- Add two members of $\mathcal{A}$ and you get a number which leaves the remainder 2 on division by 4, so is not in $\mathcal{A}$.

An Example

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?
- Well $\mathbb{Z}$ has an additive structure and $\mathcal{A}$ does not.
- Add two members of $\mathbb{Z}$ and you get another one.
- Add two members of $\mathcal{A}$ and you get a number which leaves the remainder 2 on division by 4, so is not in $\mathcal{A}$.
- Amazingly we have to use the additive structure to get something fundamental about the multiplicative structure.

An Example

- What is the difference between $\mathbb{Z}$ and $\mathcal{A}$?
- Well $\mathbb{Z}$ has an additive structure and $\mathcal{A}$ does not.
- Add two members of $\mathbb{Z}$ and you get another one.
- Add two members of $\mathcal{A}$ and you get a number which leaves the remainder 2 on division by 4, so is not in $\mathcal{A}$.
- Amazingly we have to use the additive structure to get something fundamental about the multiplicative structure.
- This is of huge significance and underpins some of the most fundamental questions in mathematics.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- **Proof.** If a or b are 0, then the result is obvious.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- **Proof.** If a or b are 0, then the result is obvious.
- Thus we may suppose that $ab \neq 0$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- **Proof.** If a or b are 0, then the result is obvious.
- Thus we may suppose that $ab \neq 0$.
- Suppose that $p \nmid a$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- **Proof.** If a or b are 0, then the result is obvious.
- Thus we may suppose that $ab \neq 0$.
- Suppose that $p \nmid a$.
- We know from the previous theorem that there are x and y so that $(a, p) = ax + py$ and that $(a, p)|p$ and $(a, p)|a$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- **Proof.** If a or b are 0, then the result is obvious.
- Thus we may suppose that $ab \neq 0$.
- Suppose that $p \nmid a$.
- We know from the previous theorem that there are x and y so that $(a,p) = ax + py$ and that $(a,p)|p$ and $(a,p)|a$.
- Since p is prime we must have $(a,p) = 1$ or p.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- **Proof.** If a or b are 0, then the result is obvious.
- Thus we may suppose that $ab \neq 0$.
- Suppose that $p \nmid a$.
- We know from the previous theorem that there are x and y so that $(a, p) = ax + py$ and that $(a, p)|p$ and $(a, p)|a$.
- Since p is prime we must have $(a, p) = 1$ or p.
- But we are supposing that $p \nmid a$ so $(a, p) \neq p$, i.e. $(a, p) = 1$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- **Proof.** If a or b are 0, then the result is obvious.
- Thus we may suppose that $ab \neq 0$.
- Suppose that $p \nmid a$.
- We know from the previous theorem that there are x and y so that $(a, p) = ax + py$ and that $(a, p)|p$ and $(a, p)|a$.
- Since p is prime we must have $(a, p) = 1$ or p.
- But we are supposing that $p \nmid a$ so $(a, p) \neq p$, i.e. $(a, p) = 1$.
- Hence $1 = ax + py$. But then

$$b = abx + pby$$

and since $p|ab$ we have $p|b$ as required.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.
- **Theorem.** Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and $p|p_1p_2\ldots p_r$. Then $p = p_j$ for some j.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.
- **Theorem.** Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and $p|p_1p_2\ldots p_r$. Then $p = p_j$ for some j.
- **Proof.** We prove this by induction on r.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.
- **Theorem.** Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and $p|p_1 p_2 \ldots p_r$. Then $p = p_j$ for some j.
- **Proof.** We prove this by induction on r.
- The case $r = 1$ is immediate from the definition of prime.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.
- **Theorem.** Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and $p|p_1p_2\ldots p_r$. Then $p = p_j$ for some j.
- **Proof.** We prove this by induction on r.
- The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p|p_1p_2\ldots p_{r+1}$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.
- **Theorem.** Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and $p|p_1p_2\ldots p_r$. Then $p = p_j$ for some j.
- **Proof.** We prove this by induction on r.
- The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p|p_1p_2\ldots p_{r+1}$.
- Then by the previous theorem we have $p|p_{r+1}$ or $p|p_1p_2\ldots p_r$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.
- **Theorem.** Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and $p|p_1p_2\ldots p_r$. Then $p = p_j$ for some j.
- **Proof.** We prove this by induction on r.
- The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p|p_1p_2\ldots p_{r+1}$.
- Then by the previous theorem we have $p|p_{r+1}$ or $p|p_1p_2\ldots p_r$.
- In the first case we must have $p = p_{r+1}$.

Euclid's Theorem

- **Theorem.** *Euclid.* Suppose that p is a prime number, and a and b are integers such that $p|ab$. Then either $p|a$ or $p|b$.
- We can use this to establish the following.
- **Theorem.** Suppose that $p, p_1, p_2, \ldots, p_r$ are prime numbers and $p|p_1 p_2 \ldots p_r$. Then $p = p_j$ for some j.
- **Proof.** We prove this by induction on r.
- The case $r = 1$ is immediate from the definition of prime.
- Suppose we have established the r-th case and that we have $p|p_1 p_2 \ldots p_{r+1}$.
- Then by the previous theorem we have $p|p_{r+1}$ or $p|p_1 p_2 \ldots p_r$.
- In the first case we must have $p = p_{r+1}$.
- In the second by the inductive hypothesis we must have $p = p_j$ for some j with $1 \le j \le r$.

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique apart from the order of the factors.

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique apart from the order of the factors.
- More precisely if a is a non-zero integer and $a \neq \pm 1$, then

$$a = (\pm 1) p_1 p_2 \ldots p_r$$

for some $r \geq 1$ and prime numbers $p_1, \ldots, p_r$, and r and the choice of sign is unique and the primes p_j are unique apart from their ordering.

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique.

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique.
- **Proof.** We may certainly suppose that $a > 0$, and so $a \geq 2$. We saw in the very first theorem that a will be a product of primes, say $a = p_1 p_2 \ldots p_r$ with $r \geq 1$. We have to prove uniqueness, and we will induct on r.

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique.
- **Proof.** We may certainly suppose that $a > 0$, and so $a \geq 2$. We saw in the very first theorem that a will be a product of primes, say $a = p_1 p_2 \ldots p_r$ with $r \geq 1$. We have to prove uniqueness, and we will induct on r.
- Suppose $r = 1$ and a is another product of primes $a = p'_1 \ldots p'_s$ where $s \geq 1$.

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique.
- **Proof.** We may certainly suppose that $a > 0$, and so $a \geq 2$. We saw in the very first theorem that a will be a product of primes, say $a = p_1 p_2 \dots p_r$ with $r \geq 1$. We have to prove uniqueness, and we will induct on r.
- Suppose $r = 1$ and a is another product of primes $a = p'_1 \dots p'_s$ where $s \geq 1$.
- Then $p'_1 | p_1$ and so $p'_1 = p_1$ and $p'_2 \dots p'_s = 1$, whence $s = 1$ also, and so establishes the base case $r = 1$.

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique.
- **Proof.** We may certainly suppose that $a > 0$, and so $a \ge 2$. We saw in the very first theorem that a will be a product of primes, say $a = p_1 p_2 \dots p_r$ with $r \ge 1$. We have to prove uniqueness, and we will induct on r.
- Suppose $r = 1$ and a is another product of primes $a = p_1' \dots p_s'$ where $s \ge 1$.
- Then $p_1' | p_1$ and so $p_1' = p_1$ and $p_2' \dots p_s' = 1$, whence $s = 1$ also, and so establishes the base case $r = 1$.
- Now suppose that the result holds for some $r \ge 1$ and we have a product of $r + 1$ primes, and and as before

$$a = p_1 p_2 \dots p_{r+1} = p_1' \dots p_s'.$$

The Fundamental Theorem of Arithmetic

- **Theorem.** *The Fundamental Theorem of Arithmetic.* Factorization into prime numbers is unique.
- **Proof.** We may certainly suppose that $a > 0$, and so $a \ge 2$. We saw in the very first theorem that a will be a product of primes, say $a = p_1 p_2 \dots p_r$ with $r \ge 1$. We have to prove uniqueness, and we will induct on r.
- Suppose $r = 1$ and a is another product of primes $a = p'_1 \dots p'_s$ where $s \ge 1$.
- Then $p'_1 | p_1$ and so $p'_1 = p_1$ and $p'_2 \dots p'_s = 1$, whence $s = 1$ also, and so establishes the base case $r = 1$.
- Now suppose that the result holds for some $r \ge 1$ and we have a product of $r + 1$ primes, and and as before

$$a = p_1 p_2 \dots p_{r+1} = p'_1 \dots p'_s.$$

- Then by the previous theorem $p'_1 = p_j$ for some j and then $p'_2 \dots p'_s = p_1 p_2 \dots p_{r+1}/p_j$ and we can apply the inductive hypothesis to obtain the desired conclusion.

GCD and LCM

- There are various other properties of GCDs.

GCD and LCM

- There are various other properties of GCDs.
- Suppose $a, b \in \mathbb{N}$. Then we can write

$$a = p_1^{r_1} \dots p_k^{r_k}, \quad b = p_1^{s_1} \dots p_k^{s_k}$$

where the $p_1, \dots p_k$ are the different primes in the factorization of a and b and we allow the possibility that the exponents r_j and s_j may be zero.

GCD and LCM

- There are various other properties of GCDs.
- Suppose $a, b \in \mathbb{N}$. Then we can write

$$a = p_1^{r_1} \dots p_k^{r_k}, \quad b = p_1^{s_1} \dots p_k^{s_k}$$

where the $p_1, \dots p_k$ are the different primes in the factorization of a and b and we allow the possibility that the exponents r_j and s_j may be zero.
- Then it can be checked easily that

$$(a, b) = p_1^{\min(r_1, s_1)} \dots p_k^{\min(r_k, s_k)}.$$

GCD and LCM

- There are various other properties of GCDs.
- Suppose $a, b \in \mathbb{N}$. Then we can write

$$a = p_1^{r_1} \dots p_k^{r_k}, \quad b = p_1^{s_1} \dots p_k^{s_k}$$

where the $p_1, \dots p_k$ are the different primes in the factorization of a and b and we allow the possibility that the exponents r_j and s_j may be zero.

- Then it can be checked easily that

$$(a, b) = p_1^{\min(r_1,s_1)} \dots p_k^{\min(r_k,s_k)}.$$

- **Definition.** We can also introduce here the *least common multiple* LCM $[a, b] = \frac{ab}{(a,b)}$ and this could also be defined by

$$[a, b] = p_1^{\max(r_1,s_1)} \dots p_k^{\max(r_k,s_k)}.$$

GCD and LCM

- There are various other properties of GCDs.
- Suppose $a, b \in \mathbb{N}$. Then we can write

$$a = p_1^{r_1} \dots p_k^{r_k}, \quad b = p_1^{s_1} \dots p_k^{s_k}$$

where the $p_1, \dots p_k$ are the different primes in the factorization of a and b and we allow the possibility that the exponents r_j and s_j may be zero.

- Then it can be checked easily that

$$(a, b) = p_1^{\min(r_1, s_1)} \dots p_k^{\min(r_k, s_k)}.$$

- **Definition.** We can also introduce here the *least common multiple* LCM $[a, b] = \frac{ab}{(a,b)}$ and this could also be defined by

$$[a, b] = p_1^{\max(r_1, s_1)} \dots p_k^{\max(r_k, s_k)}.$$

- It has the property of being the smallest positive number divisible by both a and b.

GCD and LCM

- **Example.** Show that if a and b are positive integers and $n > 1$, then $a^n - b^n \nmid a^n + b^n$.

GCD and LCM

- **Example.** Show that if a and b are positive integers and $n > 1$, then $a^n - b^n \nmid a^n + b^n$.
- **Proof.** We can suppose that $(a, b) = 1$, because if $d = (a, b)$ and $a^n - b^n | a^n + b^n$, then $(a/d)^n - (b/d)^n | (a/d)^n + (b/d)^n$.

GCD and LCM

- **Example.** Show that if a and b are positive integers and $n > 1$, then $a^n - b^n \nmid a^n + b^n$.
- **Proof.** We can suppose that $(a, b) = 1$, because if $d = (a, b)$ and $a^n - b^n | a^n + b^n$, then $(a/d)^n - (b/d)^n | (a/d)^n + (b/d)^n$.
- Suppose on the contrary that $a^n - b^n | a^n + b^n$.

GCD and LCM

- **Example.** Show that if a and b are positive integers and $n > 1$, then $a^n - b^n \nmid a^n + b^n$.
- **Proof.** We can suppose that $(a, b) = 1$, because if $d = (a, b)$ and $a^n - b^n | a^n + b^n$, then $(a/d)^n - (b/d)^n | (a/d)^n + (b/d)^n$.
- Suppose on the contrary that $a^n - b^n | a^n + b^n$.
- Then $a^n - b^n | a^n + b^n \pm (a^n - b^n)$, so $a^n - b^n | 2a^n$ and $a^n - b^n | 2b^n$.

GCD and LCM

- **Example.** Show that if a and b are positive integers and $n > 1$, then $a^n - b^n \nmid a^n + b^n$.
- **Proof.** We can suppose that $(a, b) = 1$, because if $d = (a, b)$ and $a^n - b^n | a^n + b^n$, then $(a/d)^n - (b/d)^n | (a/d)^n + (b/d)^n$.
- Suppose on the contrary that $a^n - b^n | a^n + b^n$.
- Then $a^n - b^n | a^n + b^n \pm (a^n - b^n)$, so $a^n - b^n | 2a^n$ and $a^n - b^n | 2b^n$.
- Hence $a^n - b^n | 2(a^n, b^n) = 2(a, b)^n = 2$.

GCD and LCM

- **Example.** Show that if a and b are positive integers and $n>1$, then $a^n-b^n\nmid a^n+b^n$.
- **Proof.** We can suppose that $(a,b)=1$, because if $d=(a,b)$ and $a^n-b^n|a^n+b^n$, then $(a/d)^n-(b/d)^n|(a/d)^n+(b/d)^n$.
- Suppose on the contrary that $a^n-b^n|a^n+b^n$.
- Then $a^n-b^n|a^n+b^n\pm(a^n-b^n)$, so $a^n-b^n|2a^n$ and $a^n-b^n|2b^n$.
- Hence $a^n-b^n|2(a^n,b^n)=2(a,b)^n=2$.
- We can suppose that $a>b$, whence $a^n-b^n\geq(b+1)^n-b^n\geq nb^{n-1}+\cdots+1\geq 3$ by the binomial theorem, which is impossible since $a^n-b^n|2$.