Definitions, Lemmas and so on

Definition – like a dictionary definition

Theorem – important conclusion

Lemma – less important conclusion

Corollary – a result which follows more or less obviously from a previous theorem or lemma

Proof – a sequence of logical steps, which can be followed to pass from an assumption or definition to a conclusion (i.e. a Theorem, Lemma or ....)

Example – illustrative calculation or very minor result

Build up gradually to surprising or well–hidden conclusions.

Sets

Set - a collection of objects together with some method of (in principle) identifying which objects belong to the collection and which do not.

If S is a set and x is an object which belongs to S then we say that x is an **element** of S or a **member** of S.

$x \in S$ reads "x is an element of S"

$y \notin S$ reads "y is not an element of S"

$\{1, 2, 3, 4, 5\} =$ the set with elements $1, 2, 3, 4, 5$

$\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of positive whole numbers

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the set of all whole numbers

Subsets

A set S is a **subset** of a set T if every element of S is also an element of T.

For example $\{a, b\}$ is a subset of the set $\{a, b, c\}$.

$\subset$ reads "is a subset of":

$$\{1, 2, 3, \ldots\} \subset \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

$\not\subset$ reads "is a not a subset of":

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \not\subset \{1, 2, 3, \ldots\}.$$

Every set is a subset of itself: $S \subset S$, for all sets S.

Similarly

$$\{78, 69, 45, 32\} \supset \{78, 45\}$$

$$\{78, 69, 45, 32\} \supset \{78, 32, 69, 45\}$$

and

$$\{78, 69, 45, 32\} \not\supset \{78, 32, 69, 45\}$$

$$\{78, 69, 45, 32\} \not\supset \{78, 31, 64, 49\}.$$

The empty set

The set with no elements is called the **empty set** denoted $\emptyset$.

The empty set $\emptyset$ is a subset of S, for all sets S.

There are no elements in $\emptyset$ so no element of $\emptyset$ fails to belong to S.

Beware: The set $\{\emptyset\}$ has one element, namely $\emptyset$, so is not the empty set.

Some sets of numbers

We have standard names for some sets of numbers.

(1) The positive whole numbers are called the natural numbers and the set $\{1, 2, 3, \ldots\}$ of natural numbers is denoted $\mathbb{N}$.

(2) The elements of $\{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$, the set of all whole numbers, positive, negative and zero are called the integers and the set of integers is denoted $\mathbb{Z}$.

(3) A number which can be expressed as a fraction p/q, where p and q are integers and $q \neq 0$ is called a rational number and the set of all rational numbers is denoted $\mathbb{Q}$.

(4) A number which has a decimal expansion is called a real number and the set of all real numbers is denoted $\mathbb{R}$.

Note that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. However $\mathbb{Z} \not\subset \mathbb{N}$, $\mathbb{Q} \not\subset \mathbb{Z}$ and $\mathbb{R} \not\subset \mathbb{Q}$.

Specification of new sets from old

":" reads "with the property that" or "such that".

For example:

$$\{n \in \mathbb{N} : n \text{ is even } \} = \{2, 4, 6, 8, \ldots\}$$

$$\{n \in \mathbb{N} : n > 9\} = \{10, 11, 12, \ldots\}$$

$$\{n \in \mathbb{N} : n \geq 11 \text{ and } n < 16\} = \{11, 12, 13, 14, 15\}.$$

Sometimes "$|$" is used instead of ":" as in

$$\{n \in \mathbb{N} \,|\, n \text{ is a multiple of } 10\} = \{10, 20, 30, \ldots\}.$$

Unions and intersections

The **union** of two sets S and T, denoted $S \cup T$ is the set consisting of all those elements which either belong to S or belong to T. For example

$$\{A, B, C\} \cup \{X, Y, Z\} = \{A, B, C, X, Y, Z\}$$

and

$$\{A, B, C, Y, Z\} \cup \{A, X, Y, Z\} = \{A, B, C, X, Y, Z\}.$$

The **intersection** of two sets S and T, denoted $S \cap T$ is the set consisting of only those elements which belong to both S and T. For example

$$\{A, B, C, L, M\} \cap \{L, M, X, Y, Z\} = \{L, M\}$$

and

$$\{A, B, C\} \cap \{X, Y, Z\} = \emptyset.$$

Complement and difference

If S is a subset of a set E then the **complement** of S **in** E, denoted S', is the set consisting of those elements of E which do not belong to S. That is

$$S' = \{x \in E : x \notin S\}.$$

For example if $E = \{a, b, c, d, e, f\}$ and $S = \{a, b, c\}$ then $S' = \{d, e, f\}$.

The **difference** of two sets S and T (in that order), denoted $S \backslash T$, is the set of elements of S which do not belong to T.

For example if $S = \{A, B, C, D, E, F\}$ and $T = \{D, E, F, G, H, I\}$ then $S \backslash T = \{A, B, C\}$.

Objectives

After covering this section of the course you should be able to:

(i) understand the use of terms such as Definition, Lemma, Theorem,...

(ii) read and use the symbols $\in$, $\{\ldots\}$, $\subset$, $\not\subset$, $\supset$, $\not\supset$ and $\emptyset$;

(iii) know which sets of numbers $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ refer to;

(iv) understand notation of the form $\{n \in \mathbb{Z} : n > 10\}$;

(v) know what unions, intersections, complements and differences of sets are and understand the meaning of $X \cup Y$, $X \cap Y$, $X \backslash Y$ and X', where X and Y are sets.

A puzzle

A professor decides to reward the class by handing out toffees. There are 24 toffees in a packet and the professor buys several packets. On the way to the lecture the prof eats 6 toffees. There are 30 students in the lecture and each receives the same number of toffees. There are then no toffees left. What's the least number of packets the prof could have bought and how many toffees would each student then get?

Solution

We can solve this problem algebraically.

Suppose that

the number of packets of toffees bought $= x$
the number of toffees each student gets $= y$

We can easily work out:

Total number of toffees bought: $= 24x$
Number of toffees handed out to class $= 24x - 6$

Since each student gets y toffees and there are 30 students

$$24x - 6 = 30y.$$

$$24x - 6 = 30y$$

Solve to find whole numbers x and y which are both positive.

$$24x - 6 = 30y$$

Solve to find whole numbers x and y which are both positive.

First divide through by 6 and the equation becomes

$$4x - 1 = 5y.$$

$$24x - 6 = 30y$$

Solve to find whole numbers x and y which are both positive.

First divide through by 6 and the equation becomes

$$4x - 1 = 5y.$$

Try values of x until we find one which works.

$$24x - 6 = 30y$$

Solve to find whole numbers x and y which are both positive.

First divide through by 6 and the equation becomes

$$4x - 1 = 5y.$$

Try values of x until we find one which works.

x	1	2	3	4
$4x-1$	3	7	11	15
y?	???	???	???	3

When x is 4 and y is 3 we have $4x - 1 = 5y$ so $24x - 6 = 30$ as well.

$$24x - 6 = 30y$$

Solve to find whole numbers x and y which are both positive.

First divide through by 6 and the equation becomes

$$4x - 1 = 5y.$$

Try values of x until we find one which works.

x	1	2	3	4
$4x-1$	3	7	11	15
y?	???	???	???	3

When x is 4 and y is 3 we have $4x - 1 = 5y$ so $24x - 6 = 30$ as well.

No smaller value of x makes $4x - 1$ equal to a multiple of 5.

$$24x - 6 = 30y$$

Solve to find whole numbers x and y which are both positive.

First divide through by 6 and the equation becomes

$$4x - 1 = 5y.$$

Try values of x until we find one which works.

x	1	2	3	4
$4x-1$	3	7	11	15
y?	???	???	???	3

When x is 4 and y is 3 we have $4x - 1 = 5y$ so $24x - 6 = 30$ as well.

No smaller value of x makes $4x - 1$ equal to a multiple of 5.

We now know that the prof could have got away with buying just $x = 4$ packets of toffees. Each of the students would then have received 3 toffees.

The Euclidean Algorithm

What is the biggest positive number that divides both 24 and 30?

Make two lists.

The Euclidean Algorithm

What is the biggest positive number that divides both 24 and 30?

Make two lists.

Positive divisors of 24 : $1, 2, 3, 4, 6, 8, 12, 24$

Positive divisors of 30 : $1, 2, 3, 5, 6, 10, 15, 30$

The Euclidean Algorithm

What is the biggest positive number that divides both 24 and 30?

Make two lists.

$$\text{Positive divisors of } 24 \quad : \quad 1, 2, 3, 4, 6, 8, 12, 24$$

$$\text{Positive divisors of } 30 \quad : \quad 1, 2, 3, 5, 6, 10, 15, 30$$

Pick the largest number which appears on both of the lists, which is 6.

Example 2.1. Find the biggest number which divides both 2028 and 2600.

Example 2.1. Find the biggest number which divides both 2028 and 2600.

Positive divisors of

$$2028 \quad : \quad 1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156, 169, 338, 507, 676, 1014, 2028$$

Example 2.1. Find the biggest number which divides both 2028 and 2600.

Positive divisors of

2028 : $1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156, 169, 338, 507, 676, 1014, 2028$

2600 : $1, 2, 4, 5, 8, 10, 13, 20, 25, 26, 40, 50, 52, 65, 100, 104, 130, 200, 260, 325, 520, 650, 1300, 2600$

Example 2.1. Find the biggest number which divides both 2028 and 2600.

Positive divisors of

2028 : $1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78, 156, 169, 338, 507, 676, 1014, 2028$

2600 : $1, 2, 4, 5, 8, 10, 13, 20, 25, 26, 40, 50, 52, 65, 100, 104, 130, 200, 260, 325, 520, 650, 1300, 2600$

The biggest number dividing both 2028 and 2600 is 52.

The algorithm

The biggest natural number which divides both natural numbers a and b is called the **greatest common divisor** of a and b.

The algorithm

The biggest natural number which divides both natural numbers a and b is called the **greatest common divisor** of a and b.

Given natural numbers a and b we wish to find their greatest common divisor.

The algorithm

The biggest natural number which divides both natural numbers a and b is called the **greatest common divisor** of a and b.

Given natural numbers a and b we wish to find their greatest common divisor.

The recipe works as follows.

EA1. Input the pair (b, a), with $0 < a < b$.

The algorithm

The biggest natural number which divides both natural numbers a and b is called the **greatest common divisor** of a and b.

Given natural numbers a and b we wish to find their greatest common divisor.

The recipe works as follows.

EA1. Input the pair (b, a), with $0 < a < b$.

EA2. Write $b = aq + r$, where q and r are integers with $0 \leq r < a$.

The algorithm

The biggest natural number which divides both natural numbers a and b is called the **greatest common divisor** of a and b.

Given natural numbers a and b we wish to find their greatest common divisor.

The recipe works as follows.

EA1. Input the pair (b, a), with $0 < a < b$.

EA2. Write $b = aq + r$, where q and r are integers with $0 \leq r < a$.

EA3. If $r = 0$ then **output** $\mathrm{gcd}(a, b) = a$ and **stop**.

The algorithm

The biggest natural number which divides both natural numbers a and b is called the **greatest common divisor** of a and b.

Given natural numbers a and b we wish to find their greatest common divisor.

The recipe works as follows.

EA1. Input the pair (b, a), with $0 < a < b$.

EA2. Write $b = aq + r$, where q and r are integers with $0 \leq r < a$.

EA3. If $r = 0$ then **output** $\gcd(a, b) = a$ and **stop**.

EA4. Replace the ordered pair (b, a) with (a, r). Repeat from (2).

Example 2.2. Find the greatest common divisor d of 12 and 63. Find $x, y \in \mathbb{Z}$ such that $12x + 63y = d$.

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

We write out the results of Step EA2 as the algorithm runs:

$$(2600{,}2028) \qquad 2600 = 2028 \cdot 1 + 572 \tag{2.1}$$

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

We write out the results of Step EA2 as the algorithm runs:

$$(2600{,}2028) \qquad 2600 = 2028 \cdot 1 + 572 \tag{2.1}$$

$$(2028{,}572) \qquad 2028 = 572 \cdot 3 + 312 \tag{2.2}$$

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

We write out the results of Step EA2 as the algorithm runs:

$$(2600{,}2028) \qquad 2600 = 2028 \cdot 1 + 572 \tag{2.1}$$

$$(2028{,}572) \qquad 2028 = 572 \cdot 3 + 312 \tag{2.2}$$

$$(572{,}312) \qquad 572 = 312 \cdot 1 + 260 \tag{2.3}$$

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

We write out the results of Step EA2 as the algorithm runs:

$$(2600{,}2028) \qquad 2600 = 2028 \cdot 1 + 572 \tag{2.1}$$

$$(2028{,}572) \qquad 2028 = 572 \cdot 3 + 312 \tag{2.2}$$

$$(572{,}312) \qquad 572 = 312 \cdot 1 + 260 \tag{2.3}$$

$$(312{,}260) \qquad 312 = 260 \cdot 1 + 52 \tag{2.4}$$

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

We write out the results of Step EA2 as the algorithm runs:

$$(2600{,}2028) \qquad 2600 = 2028 \cdot 1 + 572 \tag{2.1}$$

$$(2028{,}572) \qquad 2028 = 572 \cdot 3 + 312 \tag{2.2}$$

$$(572{,}312) \qquad 572 = 312 \cdot 1 + 260 \tag{2.3}$$

$$(312{,}260) \qquad 312 = 260 \cdot 1 + 52 \tag{2.4}$$

$$(260{,}52) \qquad 260 = 52 \cdot 5 + 0. \tag{2.5}$$

Example 2.3. Find the greatest common divisor d of 2600 and 2028. Find integers x and y such that $d = 2600x + 2028y$.

We write out the results of Step EA2 as the algorithm runs:

$$
\begin{aligned}
&(2600{,}2028) && 2600 = 2028 \cdot 1 + 572 && (2.1)\\
&(2028{,}572) && 2028 = 572 \cdot 3 + 312 && (2.2)\\
&(572{,}312) && 572 = 312 \cdot 1 + 260 && (2.3)\\
&(312{,}260) && 312 = 260 \cdot 1 + 52 && (2.4)\\
&(260{,}52) && 260 = 52 \cdot 5 + 0. && (2.5)
\end{aligned}
$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 2.1.

To find the integers x, y we work back from (2.4) to (2.1).

To find the integers x, y we work back from (2.4) to (2.1).

$$52 = 312 - 260 \cdot 1 \qquad \text{from (2.4)}$$

To find the integers x, y we work back from (2.4) to (2.1).

$$\begin{aligned} 52 &= 312 - 260 \cdot 1 && \text{from } (2.4) \\ &= 312 - (572 - 312 \cdot 1) = 312 \cdot 2 - 572 && \text{from } (2.3) \end{aligned}$$

To find the integers x, y we work back from (2.4) to (2.1).

$$
\begin{aligned}
52 &= 312 - 260 \cdot 1 && \text{from } (2.4) \\
&= 312 - (572 - 312 \cdot 1) = 312 \cdot 2 - 572 && \text{from } (2.3) \\
&= (2028 - 572 \cdot 3) \cdot 2 - 572 = 2028 \cdot 2 - 572 \cdot 7 && \text{from } (2.2)
\end{aligned}
$$

To find the integers x, y we work back from (2.4) to (2.1).

$$\begin{aligned} 52 &= 312 - 260 \cdot 1 && \text{from } (2.4) \\ &= 312 - (572 - 312 \cdot 1) = 312 \cdot 2 - 572 && \text{from } (2.3) \\ &= (2028 - 572 \cdot 3) \cdot 2 - 572 = 2028 \cdot 2 - 572 \cdot 7 && \text{from } (2.2) \\ &= 2028 \cdot 2 - (2600 - 2028 \cdot 1) \cdot 7 = 2028 \cdot 9 - 2600 \cdot 7 && \text{from } (2.1). \end{aligned}$$

To find the integers x, y we work back from (2.4) to (2.1).

$$\begin{aligned} 52 &= 312 - 260 \cdot 1 && \text{from (2.4)} \\ &= 312 - (572 - 312 \cdot 1) = 312 \cdot 2 - 572 && \text{from (2.3)} \\ &= (2028 - 572 \cdot 3) \cdot 2 - 572 = 2028 \cdot 2 - 572 \cdot 7 && \text{from (2.2)} \\ &= 2028 \cdot 2 - (2600 - 2028 \cdot 1) \cdot 7 = 2028 \cdot 9 - 2600 \cdot 7 && \text{from (2.1).} \end{aligned}$$

Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

$$(2028{,}626) \qquad 2028 = 626 \cdot 3 + 150 \tag{2.6}$$

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

$$(2028,626) \qquad 2028 = 626 \cdot 3 + 150 \tag{2.6}$$

$$(626,150) \qquad 626 = 150 \cdot 4 + 26 \tag{2.7}$$

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

$$(2028,626) \qquad 2028 = 626 \cdot 3 + 150 \tag{2.6}$$

$$(626,150) \qquad 626 = 150 \cdot 4 + 26 \tag{2.7}$$

$$(150,26) \qquad 150 = 26 \cdot 5 + 20 \tag{2.8}$$

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

$$(2028,626) \qquad 2028 = 626 \cdot 3 + 150 \tag{2.6}$$

$$(626,150) \qquad 626 = 150 \cdot 4 + 26 \tag{2.7}$$

$$(150,26) \qquad 150 = 26 \cdot 5 + 20 \tag{2.8}$$

$$(26,20) \qquad 26 = 20 \cdot 1 + 6 \tag{2.9}$$

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

$$(2028,626) \qquad 2028 = 626 \cdot 3 + 150 \tag{2.6}$$

$$(626,150) \qquad 626 = 150 \cdot 4 + 26 \tag{2.7}$$

$$(150,26) \qquad 150 = 26 \cdot 5 + 20 \tag{2.8}$$

$$(26,20) \qquad 26 = 20 \cdot 1 + 6 \tag{2.9}$$

$$(20,6) \qquad 20 = 6 \cdot 3 + 2 \tag{2.10}$$

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

$$
\begin{aligned}
(2028,626) \qquad 2028 &= 626 \cdot 3 + 150 && (2.6)\\
(626,150) \qquad 626 &= 150 \cdot 4 + 26 && (2.7)\\
(150,26) \qquad 150 &= 26 \cdot 5 + 20 && (2.8)\\
(26,20) \qquad 26 &= 20 \cdot 1 + 6 && (2.9)\\
(20,6) \qquad 20 &= 6 \cdot 3 + 2 && (2.10)\\
(6,2) \qquad 6 &= 2 \cdot 3 + 0. && (2.11)
\end{aligned}
$$

Example 2.4. Find the greatest common divisor d of 2028 and 626. Find $x, y \in \mathbb{Z}$ such that $2028x - 626y = d$.

$$(2028,626) \qquad 2028 = 626 \cdot 3 + 150 \tag{2.6}$$
$$(626,150) \qquad 626 = 150 \cdot 4 + 26 \tag{2.7}$$
$$(150,26) \qquad 150 = 26 \cdot 5 + 20 \tag{2.8}$$
$$(26,20) \qquad 26 = 20 \cdot 1 + 6 \tag{2.9}$$
$$(20,6) \qquad 20 = 6 \cdot 3 + 2 \tag{2.10}$$
$$(6,2) \qquad 6 = 2 \cdot 3 + 0. \tag{2.11}$$

This gives $\gcd(2028, 626) = 2$.

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

$$2 = 20 \cdot 1 - 6 \cdot 3 \qquad \text{from } (2.10)$$

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (2} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (2}
\end{aligned}
$$

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (2.10)} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (2.9)} \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (2.8)}
\end{aligned}
$$

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from } (2.10) \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from } (2.9) \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from } (2.8) \\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from } (2.7)
\end{aligned}
$$

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (2.10)} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (2.9)} \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (2.8)} \\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from (2.7)} \\
&= (2028 - 626 \cdot 3) \cdot 96 - 626 \cdot 23 = 2028 \cdot 96 - 626 \cdot 311 && \text{from (2.6).}
\end{aligned}
$$

To find the integers x, y we work back from (2.10) to (2.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (2.10)} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (2.9)} \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (2.8)} \\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from (2.7)} \\
&= (2028 - 626 \cdot 3) \cdot 96 - 626 \cdot 23 = 2028 \cdot 96 - 626 \cdot 311 && \text{from (2.6).}
\end{aligned}
$$

Thus $2 = 2028 \cdot 96 - 626 \cdot 311$ so we may take $x = 96$ and $y = 311$.

Divisibility in the integers

Definition 2.5. Let a and b be integers. If there exists an integer q such that $b = qa$ then we say that a **divides** b, or $a|b$,.

Divisibility in the integers

Definition 2.5. Let a and b be integers. If there exists an integer q such that $b = qa$ then we say that a **divides** b, or $a|b$,.

Other ways of saying $a|b$ are that a is a **factor** of b, a is a **divisor** of b or b is a **multiple** of a.

Divisibility in the integers

Definition 2.5. Let a and b be integers. If there exists an integer q such that $b = qa$ then we say that a **divides** b, or $a|b$,.

Other ways of saying $a|b$ are that a is a **factor** of b, a is a **divisor** of b or b is a **multiple** of a.

We write $a \nmid b$ to denote "a does not divide b".

Example 2.6. From the definition we can easily check that $6|18$ because $18 = 6 \cdot 3$.

Example 2.6. From the definition we can easily check that $6|18$ because $18 = 6 \cdot 3$.

In the same way we see that 6 divides $24, 12, 6, 0$ and -6.

Example 2.6. From the definition we can easily check that $6|18$ because $18 = 6{\cdot}3$.

In the same way we see that 6 divides $24, 12, 6, 0$ and -6.

Example 2.7. We shall prove that $6|(6n + 6)$, for all integers n.

Example 2.6. From the definition we can easily check that $6|18$ because $18 = 6 \cdot 3$.

In the same way we see that 6 divides $24, 12, 6, 0$ and -6.

Example 2.7. We shall prove that $6|(6n + 6)$, for all integers n.

Example 2.8. Prove that $4|[(2n + 1)^2 - 1]$, for all integers n.

Definition 2.9. The **modulus** or **absolute value** of a real number x is denoted $|x|$ and is given by the formula

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0. \end{cases}$$

Definition 2.9. The **modulus** or **absolute value** of a real number x is denoted $|x|$ and is given by the formula

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0. \end{cases}$$

For example

$$|-6| = 6 = |6|,$$
$$102 = |102| = |-102| \text{ and}$$
$$|0| = 0 = -0 = |-0|.$$

Theorem 2.10. [**The Division Algorithm**] *Let a and b be integers with $a \neq 0$. Then there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.*

Theorem 2.10. [**The Division Algorithm**] *Let a and b be integers with $a \neq 0$. Then there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.*

(1) The condition that $a \neq 0$ is necessary. If it's left out then the statement becomes untrue.

Theorem 2.10. *[**The Division Algorithm**] Let a and b be integers with $a \neq 0$. Then there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.*

(1) The condition that $a \neq 0$ is necessary. If it's left out then the statement becomes untrue.

(2) There are two parts to the conclusion of the Theorem. Firstly it says that such q and r do exist. Secondly it says that q and r are unique.

Theorem 2.10. [**The Division Algorithm**] *Let a and b be integers with $a \neq 0$. Then there exist unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.*

(1) The condition that $a \neq 0$ is necessary. If it's left out then the statement becomes untrue.

(2) There are two parts to the conclusion of the Theorem. Firstly it says that such q and r do exist. Secondly it says that q and r are unique.

(3) Does the Theorem work in other settings?

Example 2.11. Every integer n can be written as $n = 2q + r$, with $0 \leq r < 2$.

Example 2.11. Every integer n can be written as $n = 2q + r$, with $0 \leq r < 2$.

If $r = 0$ we say n is **even** and if $r = 1$ we say n is **odd**.

Example 2.11. Every integer n can be written as $n = 2q + r$, with $0 \leq r < 2$.

If $r = 0$ we say n is **even** and if $r = 1$ we say n is **odd**.

We've used the Division Algorithm (Theorem 2.10) to partition of integers into odd and even.

Example 2.11. Every integer n can be written as $n = 2q + r$, with $0 \leq r < 2$.

If $r = 0$ we say n is **even** and if $r = 1$ we say n is **odd**.

We've used the Division Algorithm (Theorem 2.10) to partition of integers into odd and even.

Example 2.12. Here we have partitioned the integers into three: those that leave remainder 0, those that leave remainder 1 and those that leave remainder 2, on applying the Division Algorithm with $a = 3$.

Example 2.13. Show that $3|n^3 - n$, for all integers n.

Example 2.13. Show that $3|n^3 - n$, for all integers n.

Example 2.14. Show that if n is an integer then n^3 has the form $4k$, $4k + 1$ or $4k + 3$, for some $k \in \mathbb{Z}$.

Why does the Euclidean Algorithm work?

Example 2.15. Consider the equation $112 = 20 \cdot 5 + 12$.

Why does the Euclidean Algorithm work?

Example 2.15. Consider the equation $112 = 20 \cdot 5 + 12$.

Why are the gcd's are both the same?

Why does the Euclidean Algorithm work?

Example 2.15. Consider the equation $112 = 20 \cdot 5 + 12$.

Why are the gcd's are both the same?

Lemma 2.16. *Let* s, t *and* u *be integers, which are not all zero, such that*

$$s = tq + u,$$

for some $q \in \mathbb{Z}$. *Then* $\gcd(s, t) = \gcd(t, u)$.

Why does the Euclidean Algorithm work?

Example 2.15. Consider the equation $112 = 20 \cdot 5 + 12$.

Why are the gcd's are both the same?

Lemma 2.16. *Let* s, t *and* u *be integers, which are not all zero, such that*

$$s = tq + u,$$

for some $q \in \mathbb{Z}$. *Then* $\gcd(s, t) = \gcd(t, u)$.

Strategy: show that any integer that divides both s and t must also divide u.

Why does the Euclidean Algorithm work?

Example 2.15. Consider the equation $112 = 20 \cdot 5 + 12$.

Why are the gcd's are both the same?

Lemma 2.16. *Let s, t and u be integers, which are not all zero, such that*

$$s = tq + u,$$

for some $q \in \mathbb{Z}$. Then $\gcd(s, t) = \gcd(t, u)$.

Strategy: show that any integer that divides both s and t must also divide u.

Then show that any integer that divides both t and u must also divide s.

Why does the Euclidean Algorithm work?

Example 2.15. Consider the equation $112 = 20 \cdot 5 + 12$.

Why are the gcd's are both the same?

Lemma 2.16. *Let* s, t *and* u *be integers, which are not all zero, such that*

$$s = tq + u,$$

for some $q \in \mathbb{Z}$. *Then* $\gcd(s, t) = \gcd(t, u)$.

Strategy: show that any integer that divides both s and t must also divide u.

Then show that any integer that divides both t and u must also divide s.

Then the set of common divisors of s and t is exactly the same as the set of common divisors of t and u and their greatest commond divisors are thus equal.

Example 2.17. We can write $337 = 11 \cdot 30 + 7$.

Example 2.17. We can write $337 = 11 \cdot 30 + 7$.

Therefore $\gcd(337, 11) = \gcd(11, 7) = 1$.

Example 2.17. We can write $337 = 11 \cdot 30 + 7$.

Therefore $\gcd(337, 11) = \gcd(11, 7) = 1$.

Lemma 2.18.

1. $a|a$*, for all integers* a*.*

Example 2.17. We can write $337 = 11 \cdot 30 + 7$.

Therefore $\gcd(337, 11) = \gcd(11, 7) = 1$.

Lemma 2.18.

1. $a|a$*, for all integers* a*.*

2. $a|0$*, for all integers* a*.*

Example 2.17. We can write $337 = 11 \cdot 30 + 7$.

Therefore $\gcd(337, 11) = \gcd(11, 7) = 1$.

Lemma 2.18.

1. *$a|a$, for all integers a.*

2. *$a|0$, for all integers a.*

3. *If a and b are integers, $a|b$ and $b > 0$ then $a \leq b$.*

Example 2.17. We can write $337 = 11 \cdot 30 + 7$.

Therefore $\gcd(337, 11) = \gcd(11, 7) = 1$.

Lemma 2.18.

1. $a|a$, *for all integers* a.

2. $a|0$, *for all integers* a.

3. *If* a *and* b *are integers,* $a|b$ *and* $b > 0$ *then* $a \leq b$.

4. *If* a *and* b *are positive integers and* $a|b$ *then* $\gcd(a, b) = a$.

Why the Euclidean Algorithm works

Example 2.19. Consider the Equations (2.6)–(2.11).

Why the Euclidean Algorithm works

Example 2.19. Consider the Equations (2.6)–(2.11).

Stringing all these facts together we have

$$\begin{aligned} 2 &= \gcd(6, 2) \\ &= \gcd(20, 6) \\ &= \gcd(26, 20) \\ &= \gcd(150, 26) \\ &= \gcd(626, 150) \\ &= \gcd(2028, 626), \end{aligned}$$

that is $\gcd(2028, 626) = 2$.

Example 2.20. Consider the Equations (2.1)–(2.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{ using Equation (2.1)}$$

Example 2.20. Consider the Equations (2.1)–(2.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{ using Equation (2.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{ using Equation (2.2)}$$

Example 2.20. Consider the Equations (2.1)–(2.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{ using Equation (2.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{ using Equation (2.2)}$$
$$\gcd(572, 312) = \gcd(312, 260), \text{ using Equation (2.3)}$$

Example 2.20. Consider the Equations (2.1)–(2.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{ using Equation (2.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{ using Equation (2.2)}$$
$$\gcd(572, 312) = \gcd(312, 260), \text{ using Equation (2.3)}$$
$$\gcd(312, 260) = \gcd(260, 52), \text{ using Equation (2.4)}.$$

Example 2.20. Consider the Equations (2.1)–(2.5).

$$\begin{aligned}
\gcd(2600, 2028) &= \gcd(2028, 572), \text{ using Equation (2.1)}\\
\gcd(2028, 572) &= \gcd(572, 312), \text{ using Equation (2.2)}\\
\gcd(572, 312) &= \gcd(312, 260), \text{ using Equation (2.3)}\\
\gcd(312, 260) &= \gcd(260, 52), \text{ using Equation (2.4)}.
\end{aligned}$$

From Equation (2.5) we see that $52|260$ so $\gcd(52, 260) = 52$.

Example 2.20. Consider the Equations (2.1)–(2.5).

$$\begin{aligned}\gcd(2600, 2028) &= \gcd(2028, 572), \text{ using Equation } (2.1)\\ \gcd(2028, 572) &= \gcd(572, 312), \text{ using Equation } (2.2)\\ \gcd(572, 312) &= \gcd(312, 260), \text{ using Equation } (2.3)\\ \gcd(312, 260) &= \gcd(260, 52), \text{ using Equation } (2.4).\end{aligned}$$

From Equation (2.5) we see that $52|260$ so $\gcd(52, 260) = 52$.

Therefore

$$52 = \gcd(260, 52) = \gcd(312, 260) =$$
$$\gcd(572, 312) = \gcd(2028, 572) = \gcd(2600, 2028),$$

Example 2.20. Consider the Equations (2.1)–(2.5).

$$\begin{aligned}\gcd(2600, 2028) &= \gcd(2028, 572), \text{ using Equation (2.1)}\\ \gcd(2028, 572) &= \gcd(572, 312), \text{ using Equation (2.2)}\\ \gcd(572, 312) &= \gcd(312, 260), \text{ using Equation (2.3)}\\ \gcd(312, 260) &= \gcd(260, 52), \text{ using Equation (2.4)}.\end{aligned}$$

From Equation (2.5) we see that $52|260$ so $\gcd(52, 260) = 52$.

Therefore

$$52 = \gcd(260, 52) = \gcd(312, 260) =$$
$$\gcd(572, 312) = \gcd(2028, 572) = \gcd(2600, 2028),$$

that is $\gcd(2600, 2028) = 52$.

And another thing

Given two integers a and b we can work back through the output of the Euclidean algorithm, as we did in Examples 2.2, 2.3 and 2.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

And another thing

Given two integers a and b we can work back through the output of the Euclidean algorithm, as we did in Examples 2.2, 2.3 and 2.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

Theorem 2.21. *Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. Then there exist integers u and v such that $d = au + bv$.*

And another thing

Given two integers a and b we can work back through the output of the Euclidean algorithm, as we did in Examples 2.2, 2.3 and 2.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

Theorem 2.21. *Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. Then there exist integers u and v such that $d = au + bv$.*

The input to the Euclidean algorithm is a pair of positive integers. What if $a < 0$?

And another thing

Given two integers a and b we can work back through the output of the Euclidean algorithm, as we did in Examples 2.2, 2.3 and 2.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

Theorem 2.21. *Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. Then there exist integers u and v such that $d = au + bv$.*

The input to the Euclidean algorithm is a pair of positive integers. What if $a < 0$?

$\gcd(a, b) = \gcd(-a, b) = \gcd(-a, -b) = \gcd(a, -b)$ and from this it follows that the Theorem holds in all cases.

An application

Example 2.22. Find integers x and y such that $2600x + 2082y = 104$.

An application

Example 2.22. Find integers x and y such that $2600x + 2082y = 104$.

In Example 2.3 we ran the Euclidean Algorithm and found $\gcd(2600, 2082) = 52$.

An application

Example 2.22. Find integers x and y such that $2600x + 2082y = 104$.

In Example 2.3 we ran the Euclidean Algorithm and found $\gcd(2600, 2082) = 52$.

Once we'd done so we were able to use the equations generated to find integers x and y such that

$$2600 \cdot (-7) + 2028 \cdot 9 = 52. \tag{2.12}$$

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

$$(123738{,}3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{2.13}$$

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

$$(123738{,}3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{2.13}$$

$$(3054{,}162) \qquad 3054 = 162 \cdot 18 + 138 \tag{2.14}$$

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

$$(123738,3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{2.13}$$

$$(3054,162) \qquad 3054 = 162 \cdot 18 + 138 \tag{2.14}$$

$$(162,138) \qquad 162 = 138 \cdot 1 + 24 \tag{2.15}$$

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

$$(123738{,}3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{2.13}$$

$$(3054{,}162) \qquad 3054 = 162 \cdot 18 + 138 \tag{2.14}$$

$$(162{,}138) \qquad 162 = 138 \cdot 1 + 24 \tag{2.15}$$

$$(138{,}24) \qquad 138 = 24 \cdot 5 + 18 \tag{2.16}$$

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

$$(123738{,}3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{2.13}$$

$$(3054{,}162) \qquad 3054 = 162 \cdot 18 + 138 \tag{2.14}$$

$$(162{,}138) \qquad 162 = 138 \cdot 1 + 24 \tag{2.15}$$

$$(138{,}24) \qquad 138 = 24 \cdot 5 + 18 \tag{2.16}$$

$$(24{,}18) \qquad 24 = 18 \cdot 1 + 6 \tag{2.17}$$

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

$$(123738{,}3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{2.13}$$
$$(3054{,}162) \qquad 3054 = 162 \cdot 18 + 138 \tag{2.14}$$
$$(162{,}138) \qquad 162 = 138 \cdot 1 + 24 \tag{2.15}$$
$$(138{,}24) \qquad 138 = 24 \cdot 5 + 18 \tag{2.16}$$
$$(24{,}18) \qquad 24 = 18 \cdot 1 + 6 \tag{2.17}$$
$$(18{,}6) \qquad 18 = 3 \cdot 6 + 0. \tag{2.18}$$

Example 2.23. Find integers x and y such that $-72 = 123738x - 3054y$.

First we run the Euclidean Algorithm to find $\gcd(12378, 3054)$.

$$(123738{,}3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{2.13}$$

$$(3054{,}162) \qquad 3054 = 162 \cdot 18 + 138 \tag{2.14}$$

$$(162{,}138) \qquad 162 = 138 \cdot 1 + 24 \tag{2.15}$$

$$(138{,}24) \qquad 138 = 24 \cdot 5 + 18 \tag{2.16}$$

$$(24{,}18) \qquad 24 = 18 \cdot 1 + 6 \tag{2.17}$$

$$(18{,}6) \qquad 18 = 3 \cdot 6 + 0. \tag{2.18}$$

This gives $\gcd(12378, 3054) = 6$.

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

$$6 = 24 - 18 \cdot 1 \qquad \text{from } (2.17)$$

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

$$\begin{aligned} 6 &= 24 - 18 \cdot 1 && \text{from (2.17)} \\ &= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (2.16)} \end{aligned}$$

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

$$
\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (2.17)}\\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (2.16)}\\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (2.15)}
\end{aligned}
$$

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (2.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (2.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (2.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 = 162 \cdot 132 - 3054 \cdot 7 && \text{from (2.14)}
\end{aligned}$$

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

$$\begin{aligned} 6 &= 24 - 18 \cdot 1 && \text{from (2.17)} \\ &= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (2.16)} \\ &= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (2.15)} \\ &= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 = 162 \cdot 132 - 3054 \cdot 7 && \text{from (2.14)} \\ &= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 = 12378 \cdot 132 - 3054 \cdot 535 && \text{from (2.13).} \end{aligned}$$

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (2.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (2.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (2.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 = 162 \cdot 132 - 3054 \cdot 7 && \text{from (2.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 = 12378 \cdot 132 - 3054 \cdot 535 && \text{from (2.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \tag{2.19}$$

Next we work back from (2.17) to (2.13) to find integers u, v such that

$$6 = 123738u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (2.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (2.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (2.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 = 162 \cdot 132 - 3054 \cdot 7 && \text{from (2.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 = 12378 \cdot 132 - 3054 \cdot 535 && \text{from (2.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \tag{2.19}$$

and we may take $u = 132$ and $v = -535$.

Existence of solutions

Existence of solutions

Lemma 2.24. *Let* a, b *and* c *be integers (*a, b *not both zero). The equation*

$$ax + by = c \tag{2.20}$$

has integer solutions x, y *if and only if* $\gcd(a, b) | c$.

Existence of solutions

Lemma 2.24. *Let a, b and c be integers (a, b not both zero). The equation*

$$ax + by = c \tag{2.20}$$

has integer solutions x, y if and only if $\gcd(a, b)|c$.

Example 2.25. Are there integers x and y such that $2600x + 2028y = 130$?

Existence of solutions

Lemma 2.24. *Let a, b and c be integers (a, b not both zero). The equation*

$$ax + by = c \tag{2.20}$$

has integer solutions x, y if and only if $\gcd(a, b)|c$.

Example 2.25. Are there integers x and y such that $2600x + 2028y = 130$?

Example 2.26. For which c does the equation $72x + 49y = c$ have a solution?

Existence of solutions

Lemma 2.24. *Let a, b and c be integers (a, b not both zero). The equation*

$$ax + by = c \tag{2.20}$$

has integer solutions x, y if and only if $\gcd(a, b) | c$.

Example 2.25. Are there integers x and y such that $2600x + 2028y = 130$?

Example 2.26. For which c does the equation $72x + 49y = c$ have a solution?

$\gcd(72, 49) = 1$

Existence of solutions

Lemma 2.24. *Let a, b and c be integers (a, b not both zero). The equation*

$$ax + by = c \tag{2.20}$$

has integer solutions x, y if and only if $\gcd(a, b)|c$.

Example 2.25. Are there integers x and y such that $2600x + 2028y = 130$?

Example 2.26. For which c does the equation $72x + 49y = c$ have a solution?

$\gcd(72, 49) = 1$

so the equation $72x + 49y = c$ has a solution for every choice of c.

Objectives

After covering this chapter of the course you should be able to:

(i) use terms such as Definition, Lemma, and proof with confidence;

(ii) read and understand simple proofs;

(iii) remember Definition 2.5 of a divides b, for integers a and b;

(iv) apply this definition to prove simple divisibility properties;

(v) state the Division Algorithm and be able to use it to demonstrate properties of integers;

(vi) remember the definition of greatest common divisor of two integers;

(vii) apply this definition to prove results;

(viii) apply the Euclidean algorithm and explain why it works;

(ix) find solutions to equations of the kind given above.

“There exists ...”

Example 2.4 asked for integers x and y such that $2028x - 626y = \gcd(2028, 626)$.

One such pair $x = 96$, $y = 311$, was found by applying the Euclidean Algorithm.

Once such a pair has been found we have proved the truth of the statement
“There exist integers x and y such that $2028x - 626y = \gcd(2028, 626)$.”

It is only necessary to find one pair x, y to prove that this statement is true.

There are lots of other pairs besides the one given, $x = 409$, $y = 1325$, for example, but this doesn’t matter.

The assertion can be seen to be true once we’ve found our first solution.

Notation: the symbol "$\exists$" is read "there exists".

Example 3.1. Prove that $\exists q \in \mathbb{Z}$ such that $7q = 28$.

Example 3.2. Prove that $\exists x \in \mathbb{R}$ such that $x \cdot 0 = 0$.

“For all...”

Examples 2.8, 2.13 and 2.14 we show that something holds for all integers.

In each case we do this by using a letter n to represent an arbitrary integer.

Again, it is easy to verify these results for particular values of n but this does not prove that the statements hold for all integers.

Counter–example and disproof

Is the following statement true or false?

$$3|n^2 + 2n, \text{ for all } n \in \mathbb{Z}.$$

Notation: the symbol "$\forall$" is read "for all".

Example 3.3. Show, by finding a counter–example that the statement

$$\text{``}n^2 \text{ is even, } \forall n \in \mathbb{Z}\text{''}$$

is false.

Example 3.4. Disprove the assertion that

"$\exists n \in \mathbb{Z}$ such that n^3 can be written as $4k+2$, with $k \in \mathbb{Z}$".

Example 3.5. Consider the statement

"$\exists x \in \mathbb{R}$ such that $x^2 = -10$.

Example 3.5. Consider the statement

"$\exists x \in \mathbb{R}$ such that $x^2 = -10$.

To prove it's false I must show it fails for all $x \in \mathbb{R}$ (infinitely many).

Example 3.5. Consider the statement

$$\text{“}\exists x \in \mathbb{R} \text{ such that } x^2 = -10.$$

To prove it's false I must show it fails for all $x \in \mathbb{R}$ (infinitely many).

I can use a basic property of real number arithmetic to do this. Namely, if $x \in \mathbb{R}$ then $x^2 \geq 0$.

Example 3.5. Consider the statement

"$\exists x \in \mathbb{R}$ such that $x^2 = -10$.

To prove it's false I must show it fails for all $x \in \mathbb{R}$ (infinitely many).

I can use a basic property of real number arithmetic to do this. Namely, if $x \in \mathbb{R}$ then $x^2 \geq 0$.

Thus, no matter what value b takes the statement is false.

Example 3.5. Consider the statement

$$\text{“}\exists x \in \mathbb{R} \text{ such that } x^2 = -10.$$

To prove it's false I must show it fails for all $x \in \mathbb{R}$ (infinitely many).

I can use a basic property of real number arithmetic to do this. Namely, if $x \in \mathbb{R}$ then $x^2 \geq 0$.

Thus, no matter what value b takes the statement is false.

Note that a counter–example is no use here as I must check all possible values of x.

"If ... then ..."

Example 3.6. Consider the assertion

$$\text{“if } x > 2 \text{ then } x^2 + x - 6 > 0\text{”.}$$

“if A then B” and “if B then A”

“If I am a frog then I can swim”

is a plausible enough statement.

Switching A and B we have:

“If I can swim then I am a frog”.

This can’t be true!

Example 3.7. If we switch the order of A and B in Example 3.6 we obtain the statement

"If $x^2 + x - 6 > 0$ then $x > 2$. "

The Converse

Switching A and B gives a new statement (unless A and B are the same).

The switched statement is called the **converse** of the original.

The Converse

Switching A and B gives a new statement (unless A and B are the same).

The switched statement is called the **converse** of the original.
Example 3.8. The converse of

"If $x^2 > 0$ then $x > 0$"

is

"If $x > 0$ then $x^2 > 0$".

The Converse

Switching A and B gives a new statement (unless A and B are the same).

The switched statement is called the **converse** of the original.
Example 3.8. The converse of

"If $x^2 > 0$ then $x > 0$"

is

"If $x > 0$ then $x^2 > 0$".

This time the original statement is false but its converse is true.

The Converse

Switching A and B gives a new statement (unless A and B are the same).

The switched statement is called the **converse** of the original.
Example 3.8. The converse of

“If $x^2 > 0$ then $x > 0$”

is

“If $x > 0$ then $x^2 > 0$”.

This time the original statement is false but its converse is true.

Even if the original statement is true its converse may not be, and vice–versa.

The Converse

Switching A and B gives a new statement (unless A and B are the same).

The switched statement is called the **converse** of the original.
Example 3.8. The converse of

"If $x^2 > 0$ then $x > 0$"

is

"If $x > 0$ then $x^2 > 0$".

This time the original statement is false but its converse is true.

Even if the original statement is true its converse may not be, and vice–versa.

In some circumstances it may turn out however that both statements are true.

"... if and only if ..."

Example 3.9. Let $a, b, c \in \mathbb{R}$ with $a > 0$.

"... if and only if ..."

Example 3.9. Let $a, b, c \in \mathbb{R}$ with $a > 0$.

Consider the statement

"If $b^2 - 4ac \geq 0$ then $ax^2 + bx + c = 0$ has a real solution."

"... if and only if ..."

Example 3.9. Let $a, b, c \in \mathbb{R}$ with $a > 0$.

Consider the statement

"If $b^2 - 4ac \geq 0$ then $ax^2 + bx + c = 0$ has a real solution."

We know that this is true.

Shorthand

What we have shown in the previous example is that

“[if $b^2 - 4ac \geq 0$ then $ax^2 + bx + c = 0$ has a real solution]
AND
[if $ax^2 + bx + c = 0$ has a real solution then $b^2 - 4ac \geq 0$]”

is a true statement.

Shorthand

What we have shown in the previous example is that

“[if $b^2 - 4ac \geq 0$ then $ax^2 + bx + c = 0$ has a real solution]
AND
[if $ax^2 + bx + c = 0$ has a real solution then $b^2 - 4ac \geq 0$]”

is a true statement.

Instead we may say

“$ax^2 + bx + c = 0$ has a real solution if and only if $b^2 - 4ac \geq 0$.”

Shorthand

What we have shown in the previous example is that

“[if $b^2 - 4ac \geq 0$ then $ax^2 + bx + c = 0$ has a real solution]
AND
[if $ax^2 + bx + c = 0$ has a real solution then $b^2 - 4ac \geq 0$]”

is a true statement.

Instead we may say

“$ax^2 + bx + c = 0$ has a real solution if and only if $b^2 - 4ac \geq 0$.”

Sometimes

“if and only if”

is shortened to

“iff”.

In general a statement of the form

“A if and only if B”

means

“[if A then B] AND [if B then A]”.

Lemma 3.10. *Assume that* a *and* b *are positive integers. Then* $a|b$ *if and only if* $\gcd(a, b) = a$.

Lemma 3.10. *Assume that a and b are positive integers. Then $a|b$ if and only if $\gcd(a,b) = a$.*

Proof. The statement of the Lemma uses shorthand and when written out in full becomes

Lemma 3.10. *Assume that a and b are positive integers. Then $a|b$ if and only if* $\gcd(a,b) = a$.

Proof. The statement of the Lemma uses shorthand and when written out in full becomes

"[if $a|b$ then $\gcd(b,a) = a$] AND [if $\gcd(b,a) = a$ then $a|b$]".

Lemma 3.10. *Assume that a and b are positive integers. Then $a|b$ if and only if $\gcd(a, b) = a$.*

Proof. The statement of the Lemma uses shorthand and when written out in full becomes

"[if $a|b$ then $\gcd(b, a) = a$] AND [if $\gcd(b, a) = a$ then $a|b$]".

The general rule in a proof of such a statement is prove each part separately. □

In general terms to show that

"A if and only if B"

is true we must establish the truth of both

"if A then B"

and

"if B then A".

Synonyms

All the entries on a given line of the following table mean the same thing.

if A then B	A $\Rightarrow$ B	B if A
if B then A	A $\Leftarrow$ B	A if B
A if and only if B	A $\Leftrightarrow$ B	A iff B

Contradiction

Most of the proofs we have seen so far are direct.

Contradiction

Most of the proofs we have seen so far are direct.

In Lemma 2.16 we prove that if s, t and u are integers and $s = tq + u$, for some $q \in \mathbb{Z}$, then $\gcd(s, t) = \gcd(t, u)$.

Contradiction

Most of the proofs we have seen so far are direct.

In Lemma 2.16 we prove that if s, t and u are integers and $s = tq + u$, for some $q \in \mathbb{Z}$, then $\gcd(s, t) = \gcd(t, u)$.

The proof starts with the assumption that $s = tq + u$ and makes deductions until the required result is reached.

Contradiction

Most of the proofs we have seen so far are direct.

In Lemma 2.16 we prove that if s, t and u are integers and $s = tq + u$, for some $q \in \mathbb{Z}$, then $\gcd(s,t) = \gcd(t,u)$.

The proof starts with the assumption that $s = tq + u$ and makes deductions until the required result is reached.

Here is an example of another kind of, indirect, argument.

Example 3.11. Show that $x^2 = -1$ has no real solution.

Step(1) **Assume the opposite of what is to be proved.**

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.**

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.**

As $r \in \mathbb{R}$ we have $0 \leq r^2$.

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.**

As $r \in \mathbb{R}$ we have $0 \leq r^2$.

Step(3) **Show that something we've derived is false.**

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.**

As $r \in \mathbb{R}$ we have $0 \leq r^2$.

Step(3) **Show that something we've derived is false.**

Combining the fact above with the assumption that $r^2 = -1$ we obtain $0 \leq -1$, which is clearly false.

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.**

As $r \in \mathbb{R}$ we have $0 \leq r^2$.

Step(3) **Show that something we've derived is false.**

Combining the fact above with the assumption that $r^2 = -1$ we obtain $0 \leq -1$, which is clearly false.

Step(4) **Conclude that the assumption is false and so prove the required result.**

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.**

As $r \in \mathbb{R}$ we have $0 \leq r^2$.

Step(3) **Show that something we've derived is false.**

Combining the fact above with the assumption that $r^2 = -1$ we obtain $0 \leq -1$, which is clearly false.

Step(4) **Conclude that the assumption is false and so prove the required result.**

The false statement in Step(3) was a direct consequence of the assumption that a solution $x = r$ to $x^2 = -1$ exists.

Step(1) **Assume the opposite of what is to be proved.**

Suppose that there is a real number r such that $r^2 = -1$ and see where this leads us.

Step(2) **Derive some consequences of the assumption.**

As $r \in \mathbb{R}$ we have $0 \leq r^2$.

Step(3) **Show that something we've derived is false.**

Combining the fact above with the assumption that $r^2 = -1$ we obtain $0 \leq -1$, which is clearly false.

Step(4) **Conclude that the assumption is false and so prove the required result.**

The false statement in Step(3) was a direct consequence of the assumption that a solution $x = r$ to $x^2 = -1$ exists.

We are forced to conclude that no solution exists.

Indirect argument

This is a technique of argument known as **contradiction**.

Indirect argument

This is a technique of argument known as **contradiction**.

We start by assuming that whatever we wish to prove is false.

Indirect argument

This is a technique of argument known as **contradiction**.

We start by assuming that whatever we wish to prove is false.

This assumption is then used to make deductions.

Indirect argument

This is a technique of argument known as **contradiction**.

We start by assuming that whatever we wish to prove is false.

This assumption is then used to make deductions.

We hope that these deductions lead to something which we know is false: that is to a contradiction.

Indirect argument

This is a technique of argument known as **contradiction**.

We start by assuming that whatever we wish to prove is false.

This assumption is then used to make deductions.

We hope that these deductions lead to something which we know is false: that is to a contradiction.

We conclude that our assumption is wrong so what we want to prove is true.

Examples: proof by contradiction

The proof that $q > 0$ in the proof of Lemma 2.18.3 is a proof by contradiction.

Examples: proof by contradiction

The proof that $q > 0$ in the proof of Lemma 2.18.3 is a proof by contradiction.

Theorem 3.12. *There are no natural numbers x and y such that $x^2 - 2y^2 = 0$.*

Examples: proof by contradiction

The proof that $q > 0$ in the proof of Lemma 2.18.3 is a proof by contradiction.
Theorem 3.12. *There are no natural numbers x and y such that $x^2 - 2y^2 = 0$.*

We can use this to prove something that may seem more familiar, namely that $\sqrt{2}$ is not a rational number.

Examples: proof by contradiction

The proof that $q > 0$ in the proof of Lemma 2.18.3 is a proof by contradiction.
Theorem 3.12. *There are no natural numbers* x *and* y *such that* $x^2 - 2y^2 = 0$*.*

We can use this to prove something that may seem more familiar, namely that $\sqrt{2}$ is not a rational number.

As this follows easily from the Theorem we call it a Corollary.

Examples: proof by contradiction

The proof that $q > 0$ in the proof of Lemma 2.18.3 is a proof by contradiction.
Theorem 3.12. *There are no natural numbers x and y such that $x^2 - 2y^2 = 0$.*

We can use this to prove something that may seem more familiar, namely that $\sqrt{2}$ is not a rational number.

As this follows easily from the Theorem we call it a Corollary.

Again we use proof by contradiction.

Examples: proof by contradiction

The proof that $q > 0$ in the proof of Lemma 2.18.3 is a proof by contradiction.
Theorem 3.12. *There are no natural numbers x and y such that $x^2 - 2y^2 = 0$.*

We can use this to prove something that may seem more familiar, namely that $\sqrt{2}$ is not a rational number.

As this follows easily from the Theorem we call it a Corollary.

Again we use proof by contradiction.

Corollary 3.13. *There is no rational number r such that $r^2 = 2$. That is $\sqrt{2} \notin \mathbb{Q}$.*

Proof of Corollary 3.13

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Proof of Corollary 3.13

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Step(2) As $r \in \mathbb{Q}$ we have $r = p/q$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.

Proof of Corollary 3.13

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Step(2) As $r \in \mathbb{Q}$ we have $r = p/q$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We have

$$\left(\frac{p}{q}\right)^2 = 2$$

Proof of Corollary 3.13

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Step(2) As $r \in \mathbb{Q}$ we have $r = p/q$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We have

$$\left(\frac{p}{q}\right)^2 = 2$$

$$\Rightarrow \qquad \frac{p^2}{q^2} = 2$$

Proof of Corollary 3.13

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Step(2) As $r \in \mathbb{Q}$ we have $r = p/q$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We have

$$\begin{aligned} & \left(\frac{p}{q}\right)^2 = 2 \\ \Rightarrow \quad & \frac{p^2}{q^2} = 2 \\ \Rightarrow \quad & p^2 = 2q^2, \ \text{as } q \neq 0, \end{aligned}$$

Proof of Corollary 3.13

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Step(2) As $r \in \mathbb{Q}$ we have $r = p/q$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We have

$$\begin{aligned} & \left(\frac{p}{q}\right)^2 = 2 \\ \Rightarrow \quad & \frac{p^2}{q^2} = 2 \\ \Rightarrow \quad & p^2 = 2q^2, \text{ as } q \neq 0, \\ \Rightarrow \quad & |p|^2 = 2|q|^2 \end{aligned}$$

Proof of Corollary 3.13

Step(1) Suppose that there is a rational number r such that $r^2 = 2$.

Step(2) As $r \in \mathbb{Q}$ we have $r = p/q$, where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We have

$$
\begin{aligned}
 & \left(\frac{p}{q}\right)^2 = 2 \\
\Rightarrow \quad & \frac{p^2}{q^2} = 2 \\
\Rightarrow \quad & p^2 = 2q^2, \text{ as } q \neq 0, \\
\Rightarrow \quad & |p|^2 = 2|q|^2 \\
\Rightarrow \quad & |p|^2 - 2|q|^2 = 0.
\end{aligned}
$$

The introduction of $|\cdot|$ is justified because $(-x)^2 = x^2 = |x|^2$, for all $x \in \mathbb{R}$.

Step(3) As $r^2 = 2$ it cannot be the case that $p = 0$, because then we'd have $2 = 0$.

Step(3) As $r^2 = 2$ it cannot be the case that $p = 0$, because then we'd have $2 = 0$.

Thus p and q are non–zero.

Step(3) As $r^2 = 2$ it cannot be the case that $p = 0$, because then we'd have $2 = 0$.

Thus p and q are non–zero.

Therefore $|p|$ and $|q|$ are natural numbers and we have deduced, in Step(2), a contradiction to Theorem 3.12.

Step(3) As $r^2 = 2$ it cannot be the case that $p = 0$, because then we'd have $2 = 0$.

Thus p and q are non–zero.

Therefore $|p|$ and $|q|$ are natural numbers and we have deduced, in Step(2), a contradiction to Theorem 3.12.

It follows that there is no such rational number r.

Step(3) As $r^2 = 2$ it cannot be the case that $p = 0$, because then we'd have $2 = 0$.

Thus p and q are non–zero.

Therefore $|p|$ and $|q|$ are natural numbers and we have deduced, in Step(2), a contradiction to Theorem 3.12.

It follows that there is no such rational number r.

Note that $\sqrt{2}$ by definition has square equal to 2: so we've shown it can't be in $\mathbb{Q}$.

Objectives

After covering this chapter of the course you should be able to:

(i) recognise and use the symbols $\exists$, $\forall$, $\Rightarrow$, $\Leftarrow$ and $\Leftrightarrow$;

(ii) apply appropriate arguments to show whether or not statements of the form

"$\exists$ ...",

"$\forall$ ..."

"if ... then ... "

and

"... if and only if ..."

are true;

(iii) explain what a Corollary is;

(iv) understand and use proof by contradiction.

Induction

Some properties of sets and numbers are so obvious that we treat them as natural laws which do not require proof.

Induction

Some properties of sets and numbers are so obvious that we treat them as natural laws which do not require proof.

We call such a property an axiom.

Induction

Some properties of sets and numbers are so obvious that we treat them as natural laws which do not require proof.

We call such a property an axiom.

For instance all the properties of numbers listed at the beginning of Section 2.2 are axioms for numbers.

Induction

Some properties of sets and numbers are so obvious that we treat them as natural laws which do not require proof.

We call such a property an axiom.

For instance all the properties of numbers listed at the beginning of Section 2.2 are axioms for numbers.

The method of proof by induction is based on the following property which is really an axiom for the natural numbers $\mathbb{N}$.

The Principle of proof by induction

Assume that $P(n)$ is a statement, for all $n \in \mathbb{N}$.

The Principle of proof by induction

Assume that $P(n)$ is a statement, for all $n \in \mathbb{N}$.

Assume further that it can be shown that

(1) $P(1)$ is true and

The Principle of proof by induction

Assume that $P(n)$ is a statement, for all $n \in \mathbb{N}$.

Assume further that it can be shown that

(1) $P(1)$ is true and

(2) if $P(k)$ is true then $P(k+1)$ is true, for $k \geq 1$.

The Principle of proof by induction

Assume that $P(n)$ is a statement, for all $n \in \mathbb{N}$.

Assume further that it can be shown that

(1) $P(1)$ is true and

(2) if $P(k)$ is true then $P(k+1)$ is true, for $k \geq 1$.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Example 4.1. Suppose that we wish to prove that

$$\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1}, \text{ for all } n \in \mathbb{N}.$$

Example 4.1. Suppose that we wish to prove that

$$\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1}, \text{ for all } n \in \mathbb{N}.$$

Here $P(n)$ is the statement

$$\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1},$$

Example 4.1. Suppose that we wish to prove that

$$\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1}, \text{ for all } n \in \mathbb{N}.$$

Here $P(n)$ is the statement

$$\sum_{j=1}^{n} \frac{1}{j(j+1)} = 1 - \frac{1}{n+1},$$

and we wish to prove $P(1), P(2), P(3), \ldots$.

Example 4.2 (Bernoulli's Inequality). Prove that

$$(1+x)^n \geq 1+nx, \text{ for all } n \in \mathbb{N} \text{ and for all } x \in \mathbb{R}, x > 0.$$

Example 4.3 (Summing a geometric progression). Prove that

$$\sum_{j=0}^{n-1} ar^j = \frac{a(r^n - 1)}{r - 1}, \text{ for all } a \in \mathbb{R} \text{ and } r \in \mathbb{R}, r \neq 1, \text{ and for all } n \in \mathbb{N}.$$

Example 4.4 (Special cases of summing gp's).

(1) $a = 1$, $r = x$ ($\neq 1$):

From Example 4.3

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}.$$

Example 4.4 (Special cases of summing gp's).

(1) $a = 1$, $r = x$ $(\neq 1)$:

From Example 4.3

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}.$$

Multiplying through by $x - 1$ gives

$$(1 + x + x^2 + \cdots + x^{n-1})(x - 1) = x^n - 1.$$

If we defined division for polynomials as we've done for integers, in Definition 2.5, we could say that this shows that

$$(x-1)|(x^n-1)$$

and that

$$(1+x+x^2+\cdots+x^{n-1})|(x^n-1).$$

If we defined division for polynomials as we've done for integers, in Definition 2.5, we could say that this shows that

$$(x-1)|(x^n-1)$$

and that

$$(1+x+x^2+\cdots+x^{n-1})|(x^n-1).$$

For example

$$(1+x)(x-1)=x^2-1,$$
$$(1+x+x^2)(x-1)=x^3-1,$$
$$(1+x+x^2+x^3)(x-1)=x^4-1.$$

(2) $a = 1$, $r = -x$ $(x \neq -1)$, $n = 2m + 1$, $m \in \mathbb{N}$:

The lefthand side of the equality of Example 4.3 becomes

$$\sum_{j=0}^{2m} ar^j = \sum_{j=0}^{2m} (-x)^j$$

(2) $a = 1$, $r = -x$ $(x \neq -1)$, $n = 2m + 1$, $m \in \mathbb{N}$:

The lefthand side of the equality of Example 4.3 becomes

$$\sum_{j=0}^{2m} ar^j = \sum_{j=0}^{2m} (-x)^j$$
$$= 1 - x + x^2 - \cdots + (-1)^{2m} x^{2m}$$

(2) $a = 1$, $r = -x$ $(x \neq -1)$, $n = 2m + 1$, $m \in \mathbb{N}$:

The lefthand side of the equality of Example 4.3 becomes

$$\begin{aligned} \sum_{j=0}^{2m} ar^j &= \sum_{j=0}^{2m} (-x)^j \\ &= 1 - x + x^2 - \cdots + (-1)^{2m} x^{2m} \\ &= 1 - x + x^2 - \cdots + x^{2m}. \end{aligned}$$

(2) $a = 1$, $r = -x$ $(x \neq -1)$, $n = 2m + 1$, $m \in \mathbb{N}$:

The lefthand side of the equality of Example 4.3 becomes

$$\sum_{j=0}^{2m} ar^j = \sum_{j=0}^{2m} (-x)^j$$
$$= 1 - x + x^2 - \cdots + (-1)^{2m} x^{2m}$$
$$= 1 - x + x^2 - \cdots + x^{2m}.$$

The righthand side is

$$\frac{a(r^n - 1)}{r - 1} = \frac{(-x)^{2m+1} - 1}{-x - 1}$$
$$= \frac{x^{2m+1} + 1}{x + 1}.$$

From Example 4.3

$$1 - x + x^2 - \cdots + x^{2m} = \frac{x^{2m+1} + 1}{x + 1}.$$

From Example 4.3

$$1 - x + x^2 - \cdots + x^{2m} = \frac{x^{2m+1} + 1}{x + 1}.$$

Multiplying by $x + 1$ gives

$$(1 - x + x^2 - \cdots + x^{2m})(x + 1) = x^{2m+1} + 1.$$

For example

$$(1 - x + x^2)(x + 1) = x^3 + 1,$$

For example

$$(1 - x + x^2)(x + 1) = x^3 + 1,$$
$$(1 - x + x^2 - x^3 + x^4)(x + 1) = x^5 + 1,$$

For example

$$
\begin{aligned}
(1-x+x^2)(x+1) &= x^3+1, \\
(1-x+x^2-x^3+x^4)(x+1) &= x^5+1, \\
(1-x+x^2-x^3+x^4-x^5+x^6)(x+1) &= x^7+1.
\end{aligned}
$$

For example

$$(1 - x + x^2)(x + 1) = x^3 + 1,$$
$$(1 - x + x^2 - x^3 + x^4)(x + 1) = x^5 + 1,$$
$$(1 - x + x^2 - x^3 + x^4 - x^5 + x^6)(x + 1) = x^7 + 1.$$

We can say

$$(x + 1) | (x^{2m+1} + 1) \text{ and}$$
$$(1 - x + x^2 - \cdots + x^{2m}) | (x^{2m+1} + 1).$$

Change of basis

It is sometimes useful to be able to start the induction at some point other than $n = 1$.

In this case we use the following fact which follows from the Axiom of Induction.

Let $s \in \mathbb{Z}$. Assume that $P(n)$ is a statement, for all $n \geq s$.

Assume further that it can be shown that

(1′) $P(s)$ is true and

(2′) if $P(k)$ is true then $P(k+1)$ is true, for $k \geq s$.

Then $P(n)$ is true for all $n \geq s$.

Example 4.5. Show that $2^n > n^3$, for all $n \geq 10$.

Note that $2^9 = 512 < 729 = 9^3$, so the result does not hold when $n = 9$.

Binomial coefficients

The **binomial coefficient** or **choice number** $\binom{n}{k}$ is given by the formula

$$\binom{n}{k} = \frac{n!}{(n-k)!k!},$$

for non-negative integers n and k, with $0 \leq k \leq n$.

Binomial coefficients

The **binomial coefficient** or **choice number** $\binom{n}{k}$ is given by the formula

$$\binom{n}{k} = \frac{n!}{(n-k)!k!},$$

for non-negative integers n and k, with $0 \leq k \leq n$.

We define $0! = 1$ so that $\binom{n}{0} = \binom{n}{n} = 1$, for all n.

As you can verify

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

As you can verify

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

We can use this fact to generate binomial coefficients. Start with $\binom{0}{0}$ and write out succesive rows starting with $1 = \binom{n}{0}$ and ending with $\binom{n}{n} = 1$.

As you can verify

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

We can use this fact to generate binomial coefficients. Start with $\binom{0}{0}$ and write out succesive rows starting with $1 = \binom{n}{0}$ and ending with $\binom{n}{n} = 1$.

Fill the rows making the kth entry on the nth row the sum of the $(k-1)$th and kth entries from the row above.

$$
\begin{array}{ccccccc}
 & & & \binom{0}{0} & & & \\
 & & \swarrow & & \searrow & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & \\
 & \swarrow & \searrow & & \swarrow & \searrow & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\
\swarrow & \searrow & \swarrow & & \searrow & \swarrow & \searrow \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3}
\end{array}
$$

Then the $(n+1)$st row will contain the binomial coefficients $\binom{n}{k}$, for $k = 0, \ldots, n$.

This array is known as **Pascal's triangle** and is more familiar as

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & \swarrow & & \searrow & & & & & \\
 & & & & 1 & & & & 1 & & & & \\
 & & & \swarrow & & \searrow & & \swarrow & & \searrow & & & \\
 & & 1 & & & & 2 & & & & 1 & & \\
 & \swarrow & & \searrow & & \swarrow & & \searrow & & \swarrow & & \searrow & \\
1 & & & & 3 & & & & 3 & & & & 1
\end{array}
$$

Diagonal sums

Write out Pascal's triangle with the left hand "1"s aligned in a column.

$$\begin{array}{cccccccc}
1 \\
1 & 1 \\
1 & 2 & 1 \\
1 & 3 & 3 & 1 \\
1 & 4 & 6 & 4 & 1 \\
1 & 5 & 10 & 10 & 5 & 1 \\
1 & 6 & 15 & 20 & 15 & 6 & 1 \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1
\end{array}$$

Diagonal sums

Write out Pascal's triangle with the left hand "1"s aligned in a column.

1							
1	1						
1	2	1					
1	3	3	1				
1	4	6	4	1			
1	5	10	10	5	1		
1	6	15	20	15	6	1	
1	7	21	35	35	21	7	1

Now add numbers on the diagonals running from lower left to upper right:

$$1$$
$$1$$
$$1+1=2$$
$$1+2=3$$
$$1+3+1=5$$
$$1+4+3=8$$
$$1+5+6+1=13$$
$$1+6+10+4=21.$$

$$
\begin{gathered}
1 \\
1 \\
1+1=2 \\
1+2=3 \\
1+3+1=5 \\
1+4+3=8 \\
1+5+6+1=13 \\
1+6+10+4=21.
\end{gathered}
$$

These are the first 8 of the **Fibonacci** numbers.

Fibonacci numbers

The Fibonacci numbers are generated by the rules

$$
\begin{aligned}
f_1 &= 1 \\
f_2 &= 1 \\
f_{n+1} &= f_n + f_{n-1}, \text{ for } n \geq 2.
\end{aligned}
$$

Fibonacci numbers

The Fibonacci numbers are generated by the rules

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_{n+1} &= f_n + f_{n-1}, \text{ for } n \geq 2. \end{aligned}$$

Thus the Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, \ldots$$

Do the diagonals of Pascal's triangle sum to the Fibonacci numbers after the first 8?

Do the diagonals of Pascal's triangle sum to the Fibonacci numbers after the first 8?

They do because each entry on a diagonal is the sum of one number from the diagonal one row above it and a second number from the diagonal two rows above it.

Do the diagonals of Pascal's triangle sum to the Fibonacci numbers after the first 8?

They do because each entry on a diagonal is the sum of one number from the diagonal one row above it and a second number from the diagonal two rows above it.

Thus each diagonal is the sum of the two diagonals above it.

Example 4.6. Consider the following.

$$f_2 = 1$$

Example 4.6. Consider the following.

$$f_2 = 1$$
$$f_3 = 2$$

Example 4.6. Consider the following.

$$f_2 = 1$$
$$f_3 = 2$$
$$f_4 = 3$$

Example 4.6. Consider the following.

$$\begin{aligned} f_2 &= 1 \\ f_3 &= 2 \\ f_4 &= 3 \\ f_2 + f_4 &= 4 \end{aligned}$$

Example 4.6. Consider the following.

$$f_2 = 1$$

$$f_3 = 2$$

$$f_4 = 3$$

$$f_2 + f_4 = 4$$

$$f_5 = 5$$

Example 4.6. Consider the following.

$$\begin{aligned} f_2 &= 1 \\ f_3 &= 2 \\ f_4 &= 3 \\ f_2 + f_4 &= 4 \\ f_5 &= 5 \\ f_2 + f_5 &= 6 \end{aligned}$$

Example 4.6. Consider the following.

$$\begin{aligned} f_2 &= 1 \\ f_3 &= 2 \\ f_4 &= 3 \\ f_2 + f_4 &= 4 \\ f_5 &= 5 \\ f_2 + f_5 &= 6 \\ f_3 + f_5 &= 7 \end{aligned}$$

Example 4.6. Consider the following.

$$
\begin{aligned}
f_2 &= 1 \\
f_3 &= 2 \\
f_4 &= 3 \\
f_2 + f_4 &= 4 \\
f_5 &= 5 \\
f_2 + f_5 &= 6 \\
f_3 + f_5 &= 7 \\
f_4 + f_5 &= 8
\end{aligned}
$$

Example 4.6. Consider the following.

$$\begin{aligned} f_2 &= 1 \\ f_3 &= 2 \\ f_4 &= 3 \\ f_2 + f_4 &= 4 \\ f_5 &= 5 \\ f_2 + f_5 &= 6 \\ f_3 + f_5 &= 7 \\ f_4 + f_5 &= 8 \\ f_2 + f_5 + f_9 = 1 + 5 + 34 &= 40 \end{aligned}$$

Example 4.6. Consider the following.

$$
\begin{aligned}
f_2 &= 1 \\
f_3 &= 2 \\
f_4 &= 3 \\
f_2 + f_4 &= 4 \\
f_5 &= 5 \\
f_2 + f_5 &= 6 \\
f_3 + f_5 &= 7 \\
f_4 + f_5 &= 8 \\
f_2 + f_5 + f_9 = 1 + 5 + 34 &= 40 \\
f_3 + f_7 + f_{10} = 2 + 13 + 55 &= 70.
\end{aligned}
$$

Example 4.6. Consider the following.

$$
\begin{aligned}
f_2 &= 1\\
f_3 &= 2\\
f_4 &= 3\\
f_2 + f_4 &= 4\\
f_5 &= 5\\
f_2 + f_5 &= 6\\
f_3 + f_5 &= 7\\
f_4 + f_5 &= 8\\
f_2 + f_5 + f_9 = 1 + 5 + 34 &= 40\\
f_3 + f_7 + f_{10} = 2 + 13 + 55 &= 70.
\end{aligned}
$$

Is every integer a sum of different Fibonacci numbers?

Example 4.7. If we take every third Fibonacci number we obtain a new sequence of numbers,

$$f_3, f_6, f_9, f_{12}, \ldots$$

Example 4.7. If we take every third Fibonacci number we obtain a new sequence of numbers,

$$f_3, f_6, f_9, f_{12}, \ldots$$

with values

$$2, 8, 34, 144, 610, 2584, 10946, 46368, 196418, \ldots$$

Example 4.7. If we take every third Fibonacci number we obtain a new sequence of numbers,

$$f_3, f_6, f_9, f_{12}, \ldots$$

with values

$$2, 8, 34, 144, 610, 2584, 10946, 46368, 196418, \ldots$$

We shall prove, by induction that f_{3n} is even, for all $n \geq 1$.

Example 4.8 (The binomial theorem). This example is not examinable

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k, \text{ for all } n \in \mathbb{N} \text{ and all } x, y \in \mathbb{R}.$$

Objectives

After covering this chapter of the course you should be able to:

(i) understand the principle of proof by induction;

(ii) carry out proof by induction, both starting with the integer 1 and starting with an integer other than 1;

(iii) remember the definition of binomial coefficients;

(iv) remember the definition of the Fibonacci numbers.

Greatest common divisors again

Whenever we ran the Euclidean Algorithm, on natural numbers a and b, we obtained not only $\gcd(a, b)$ but also integers u and v such that

$$\gcd(a, b) = au + bv.$$

Greatest common divisors again

Whenever we ran the Euclidean Algorithm, on natural numbers a and b, we obtained not only $\gcd(a,b)$ but also integers u and v such that

$$\gcd(a,b) = au + bv.$$

This gave us Theorem 2.21:

Let a and b be integers, not both zero, and let $d = \gcd(a,b)$. Then there exist integers u and v such that $d = au + bv$.

Greatest common divisors again

Whenever we ran the Euclidean Algorithm, on natural numbers a and b, we obtained not only $\gcd(a, b)$ but also integers u and v such that

$$\gcd(a, b) = au + bv.$$

This gave us Theorem 2.21:

Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. Then there exist integers u and v such that $d = au + bv$.

Second proof of Theorem 2.21

Suppose that we have positive integers a and b.

Second proof of Theorem 2.21

Suppose that we have positive integers a and b.

Consider the set

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}.$$

Second proof of Theorem 2.21

Suppose that we have positive integers a and b.

Consider the set

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}.$$

This is a set of positive integers.

Second proof of Theorem 2.21

Suppose that we have positive integers a and b.

Consider the set

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}.$$

This is a set of positive integers.

We shall prove the theorem by showing that it's smallest element is $\gcd(a, b)$.

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}$$

It is a fundamental property of numbers that every non-empty set of positive integers has a smallest element.

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}$$

It is a fundamental property of numbers that every non-empty set of positive integers has a smallest element.

It's easy to see S is non-empty as it contains, for example $a + b$.

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}$$

It is a fundamental property of numbers that every non-empty set of positive integers has a smallest element.

It's easy to see S is non-empty as it contains, for example $a + b$.

Therefore S has a smallest element, s say. Then

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}$$

It is a fundamental property of numbers that every non-empty set of positive integers has a smallest element.

It's easy to see S is non-empty as it contains, for example $a + b$.

Therefore S has a smallest element, s say. Then

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \qquad (5.1)$$

$$S = \{ak + bl \in \mathbb{Z} : ak + bl > 0 \text{ and } k, l \in \mathbb{Z}\}$$

It is a fundamental property of numbers that every non-empty set of positive integers has a smallest element.

It's easy to see S is non-empty as it contains, for example $a + b$.

Therefore S has a smallest element, s say. Then

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{5.1}$$

Now, using the Division Algorithm, we can write

$$a = sq + r, \text{ where } 0 \leq r < s.$$

Substituting for s using (5.1) this becomes

$$\begin{aligned} a &= (ak + bl)q + r \\ &= a(kq) + b(lq) + r, \end{aligned}$$

Substituting for s using (5.1) this becomes

$$\begin{aligned} a &= (ak + bl)q + r \\ &= a(kq) + b(lq) + r, \end{aligned}$$

so

$$r = a(1 - kq) + b(-lq), \text{ with } 0 \leq r < s.$$

Substituting for s using (5.1) this becomes

$$\begin{aligned} a &= (ak + bl)q + r \\ &= a(kq) + b(lq) + r, \end{aligned}$$

so

$$r = a(1 - kq) + b(-lq), \text{ with } 0 \leq r < s.$$

If $r \neq 0$ then we have $r \in S$ and $r < s$, a contradiction.

Substituting for s using (5.1) this becomes

$$\begin{aligned} a &= (ak + bl)q + r \\ &= a(kq) + b(lq) + r, \end{aligned}$$

so

$$r = a(1 - kq) + b(-lq), \text{ with } 0 \leq r < s.$$

If $r \neq 0$ then we have $r \in S$ and $r < s$, a contradiction.

Therefore $r = 0$ and $a = sq$. That is, $s|a$.

Substituting for s using (5.1) this becomes

$$\begin{aligned} a &= (ak + bl)q + r \\ &= a(kq) + b(lq) + r, \end{aligned}$$

so

$$r = a(1 - kq) + b(-lq), \text{ with } 0 \leq r < s.$$

If $r \neq 0$ then we have $r \in S$ and $r < s$, a contradiction.

Therefore $r = 0$ and $a = sq$. That is, $s|a$.

Similarly $s|b$.

Now suppose that $c|a$ and $c|b$.

Now suppose that $c|a$ and $c|b$.

Then $a = cu$ and $b = cv$, for some $u, v \in \mathbb{Z}$.

Now suppose that $c|a$ and $c|b$.

Then $a = cu$ and $b = cv$, for some $u, v \in \mathbb{Z}$.

Substitution in (5.1) gives

$$s = c(uk) + c(vl) = c(uk + vl).$$

Now suppose that $c|a$ and $c|b$.

Then $a = cu$ and $b = cv$, for some $u, v \in \mathbb{Z}$.

Substitution in (5.1) gives

$$s = c(uk) + c(vl) = c(uk + vl).$$

Therefore $c|s$ and from Lemma 2.18.3 we have $c \leq s$.

Now suppose that $c|a$ and $c|b$.

Then $a = cu$ and $b = cv$, for some $u, v \in \mathbb{Z}$.

Substitution in (5.1) gives

$$s = c(uk) + c(vl) = c(uk + vl).$$

Therefore $c|s$ and from Lemma 2.18.3 we have $c \leq s$.

This completes the proof that $s = \gcd(a, b)$ and we've already found k, l such that $s = ak + bl$, so Theorem 2.21 follows.

Coprime integers

Definition 5.1. If a and b are integers with $\gcd(a, b) = 1$ then we say that a and b are **coprime**.

Coprime integers

Definition 5.1. If a and b are integers with $\gcd(a, b) = 1$ then we say that a and b are **coprime**.

Example 5.2. 6 and 35 are coprime and

$$6 \cdot 6 - 1 \cdot 35 = 1.$$

Coprime integers

Definition 5.1. If a and b are integers with $\gcd(a,b) = 1$ then we say that a and b are **coprime**.

Example 5.2. 6 and 35 are coprime and

$$6 \cdot 6 - 1 \cdot 35 = 1.$$

What about

$$5 \cdot 5 - 12 \cdot 2 = 1?$$

Coprime integers

Definition 5.1. If a and b are integers with $\gcd(a, b) = 1$ then we say that a and b are **coprime**.

Example 5.2. 6 and 35 are coprime and

$$6 \cdot 6 - 1 \cdot 35 = 1.$$

What about

$$5 \cdot 5 - 12 \cdot 2 = 1?$$

We have u and v such that $15u + 12v = 1$.

Does this force $\gcd(15, 12) = 1$?

In this example the gcd is 1, but this could be a coincidence.

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Step(1) Prove that if a and b are coprime then there exist integers u and v such that $au + bv = 1$.

If a and b are coprime then it follows directly from Theorem 2.21 that such u and v exist.

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Step(1) Prove that if a and b are coprime then there exist integers u and v such that $au + bv = 1$.

If a and b are coprime then it follows directly from Theorem 2.21 that such u and v exist.

Step(2) Prove that if there exist integers u and v such that $au + bv = 1$ then $\gcd(a, b) = 1$.

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Step(1) Prove that if a and b are coprime then there exist integers u and v such that $au + bv = 1$.

If a and b are coprime then it follows directly from Theorem 2.21 that such u and v exist.

Step(2) Prove that if there exist integers u and v such that $au + bv = 1$ then $\gcd(a, b) = 1$.

Assume that there are integers u and v such that $au + bv = 1$.

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Step(1) Prove that if a and b are coprime then there exist integers u and v such that $au + bv = 1$.

If a and b are coprime then it follows directly from Theorem 2.21 that such u and v exist.

Step(2) Prove that if there exist integers u and v such that $au + bv = 1$ then $\gcd(a, b) = 1$.

Assume that there are integers u and v such that $au + bv = 1$.

Let $d = \gcd(a, b)$.

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Step(1) Prove that if a and b are coprime then there exist integers u and v such that $au + bv = 1$.

If a and b are coprime then it follows directly from Theorem 2.21 that such u and v exist.

Step(2) Prove that if there exist integers u and v such that $au + bv = 1$ then $\gcd(a, b) = 1$.

Assume that there are integers u and v such that $au + bv = 1$.

Let $d = \gcd(a, b)$.

Then $d|a$ and $d|b$ so $d|(au + bv)$:

Corollary 5.3. *Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.*

Proof. This is an if and only if proof so has two halves.

Step(1) Prove that if a and b are coprime then there exist integers u and v such that $au + bv = 1$.

If a and b are coprime then it follows directly from Theorem 2.21 that such u and v exist.

Step(2) Prove that if there exist integers u and v such that $au + bv = 1$ then $\gcd(a, b) = 1$.

Assume that there are integers u and v such that $au + bv = 1$.

Let $d = \gcd(a, b)$.

Then $d|a$ and $d|b$ so $d|(au + bv)$:

We have $d = 1$, so a and b are coprime, as required.

Euclid's Lemma

Lemma 5.4. *Let* a, b *and* c *be integers with* $\gcd(a, b) = 1$*. If* $a|bc$ *then* $a|c$*.*

Application to solving equations

Lemma 2.24: an equation of the form $ax + by = c$ has solution if and only if $c | \gcd(a, b)$.

Application to solving equations

Lemma 2.24: an equation of the form $ax + by = c$ has solution if and only if $c | \gcd(a, b)$.

Theorem 5.5. *Let* a, b, c *be integers and let* $d = \gcd(a, b)$*. The equation*

$$ax + by = c \tag{5.2}$$

has an integer solution if and only if $d|c$*. If* $d|c$ *then equation* (5.2) *has infinitely many solutions*

Application to solving equations

Lemma 2.24: an equation of the form $ax + by = c$ has solution if and only if $c | \gcd(a, b)$.

Theorem 5.5. *Let* a, b, c *be integers and let* $d = \gcd(a, b)$*. The equation*

$$ax + by = c \tag{5.2}$$

has an integer solution if and only if $d|c$*. If* $d|c$ *then equation* (5.2) *has infinitely many solutions*

and if $x = u_0$, $y = v_0$ *is one solution then* $x = u_1$, $y = v_1$ *is a solution if and only if*

$$u_1 = u_0 + (b/d)t \text{ and } v_1 = v_0 - (a/d)t, \text{ for some } t \in \mathbb{Z}.$$

Example 2.20 continued

Example 5.6.
$\gcd(2600, 2028) = 52$ and the equation $2600x + 2028y = 104$ has a solution $x = -14, y = 18$.

Example 2.20 continued

Example 5.6.
$\gcd(2600, 2028) = 52$ and the equation $2600x + 2028y = 104$ has a solution $x = -14, y = 18$.

As $2600/52 = 50$ and $2028/52 = 39$ the solutions to this equation are

$$x = -14 + 39t,\ y = 18 - 50t,\ \text{for } t \in \mathbb{Z}.$$

Example 2.20 continued

Example 5.6.
$\gcd(2600, 2028) = 52$ and the equation $2600x + 2028y = 104$ has a solution $x = -14, y = 18$.

As $2600/52 = 50$ and $2028/52 = 39$ the solutions to this equation are

$$x = -14 + 39t, \;\; y = 18 - 50t, \;\; \text{for } t \in \mathbb{Z}.$$

For each integer t we have a solution, some of which are shown below.

t	x	y
-2	-92	-118
-1	-53	68
0	-14	18
1	25	-32
2	64	-82

Prime Numbers

It follows from the definition of division that every integer n is divisible by ± 1 and by $\pm n$.

Amongst the positive integers a special case is the integer 1 which has only one positive divisor, namely 1.

All other positive integers n have at least 2 positive divisors, 1 and n, and may have more.

Definition 5.7. A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p. An integer which is not prime is called **composite**.

For example $2, 5, 7, 11, 13, 17$ and 19 are prime whilst the first few composite integers are:

4	which is divisible by	2
6	which is divisible by	2 and 3
8	which is divisible by	2 and 4
9	which is divisible by	3
10	which is divisible by	2 and 5.

The prime divisor property

A fundamental property of prime numbers is the following.

Theorem 5.8. *If* p *is a prime and* $p|ab$ *then* $p|a$ *or* $p|b$*.*

The prime divisor property

A fundamental property of prime numbers is the following.

Theorem 5.8. *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

If $p|a$ then we have nothing to prove.

The prime divisor property

A fundamental property of prime numbers is the following.

Theorem 5.8. *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

If $p|a$ then we have nothing to prove.

If $p \nmid a$ then the common divisors of a and p are ± 1 (since the only divisors of p are ± 1 and $\pm p$).

The prime divisor property

A fundamental property of prime numbers is the following.

Theorem 5.8. *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

If $p|a$ then we have nothing to prove.

If $p \nmid a$ then the common divisors of a and p are ± 1 (since the only divisors of p are ± 1 and $\pm p$).

Hence $\gcd(a, p) = 1$.

The prime divisor property

A fundamental property of prime numbers is the following.

Theorem 5.8. *If p is a prime and $p|ab$ then $p|a$ or $p|b$.*

If $p|a$ then we have nothing to prove.

If $p \nmid a$ then the common divisors of a and p are ± 1 (since the only divisors of p are ± 1 and $\pm p$).

Hence $\gcd(a, p) = 1$.

From Lemma 5.4 (Euclid's Lemma) it follows that $p|b$, as required. □

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

The same goes for 29: if $29|bc$ then $29|b$ or $29|c$.

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

The same goes for 29: if $29|bc$ then $29|b$ or $29|c$.

This does not hold for all integers.

For instance $6|24$ and $24 = 8 \cdot 3$, so $6|8 \cdot 3$ but $6 \nmid 8$ and $6 \nmid 3$.

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

The same goes for 29: if $29|bc$ then $29|b$ or $29|c$.

This does not hold for all integers.

For instance $6|24$ and $24 = 8 \cdot 3$, so $6|8 \cdot 3$ but $6 \nmid 8$ and $6 \nmid 3$.

Once we've discussed prime factorisation it will be easy to see why this property doesn't hold for any composite integers.

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

The same goes for 29: if $29|bc$ then $29|b$ or $29|c$.

This does not hold for all integers.

For instance $6|24$ and $24 = 8 \cdot 3$, so $6|8 \cdot 3$ but $6 \nmid 8$ and $6 \nmid 3$.

Once we've discussed prime factorisation it will be easy to see why this property doesn't hold for any composite integers.

The Theorem above can easily be extended to products of more than 2 integers.

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

The same goes for 29: if $29|bc$ then $29|b$ or $29|c$.

This does not hold for all integers.

For instance $6|24$ and $24 = 8 \cdot 3$, so $6|8 \cdot 3$ but $6 \nmid 8$ and $6 \nmid 3$.

Once we've discussed prime factorisation it will be easy to see why this property doesn't hold for any composite integers.

The Theorem above can easily be extended to products of more than 2 integers.

For example, if $3|abc$ then, from the Theorem either $3|ab$ or $3|c$.

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

The same goes for 29: if $29|bc$ then $29|b$ or $29|c$.

This does not hold for all integers.

For instance $6|24$ and $24 = 8 \cdot 3$, so $6|8 \cdot 3$ but $6 \nmid 8$ and $6 \nmid 3$.

Once we've discussed prime factorisation it will be easy to see why this property doesn't hold for any composite integers.

The Theorem above can easily be extended to products of more than 2 integers.

For example, if $3|abc$ then, from the Theorem either $3|ab$ or $3|c$.

If $3|ab$ then, from the Theorem again, $3|a$ or $3|b$.

Example 5.9. If $3|bc$ then either $3|b$ or $3|c$.

The same goes for 29: if $29|bc$ then $29|b$ or $29|c$.

This does not hold for all integers.

For instance $6|24$ and $24 = 8 \cdot 3$, so $6|8 \cdot 3$ but $6 \nmid 8$ and $6 \nmid 3$.

Once we've discussed prime factorisation it will be easy to see why this property doesn't hold for any composite integers.

The Theorem above can easily be extended to products of more than 2 integers.

For example, if $3|abc$ then, from the Theorem either $3|ab$ or $3|c$.

If $3|ab$ then, from the Theorem again, $3|a$ or $3|b$.

Therefore, if $3|abc$ then $3|a$ or $3|b$ or $3|c$.

Corollary 5.10. *If* p *is prime and* $p|a_1 \cdots a_n$ *then* $p|a_i$*, for some* i*.*

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Basis: $P(2)$ follows from Theorem 5.8.

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Basis: $P(2)$ follows from Theorem 5.8.

Inductive Hypothesis: If $n \geq 2$ and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Basis: $P(2)$ follows from Theorem 5.8.

Inductive Hypothesis: If $n \geq 2$ and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Inductive Step: Suppose that $p|a_1 \cdots a_{n+1}$. Let

$$a = a_1 \cdots a_n \text{ and } b = a_{n+1}.$$

Then $p|ab$ so, from Theorem 5.8, $p|a$ or $p|b$.

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Basis: $P(2)$ follows from Theorem 5.8.

Inductive Hypothesis: If $n \geq 2$ and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Inductive Step: Suppose that $p|a_1 \cdots a_{n+1}$. Let

$$a = a_1 \cdots a_n \text{ and } b = a_{n+1}.$$

Then $p|ab$ so, from Theorem 5.8, $p|a$ or $p|b$.

If $p|a$ the inductive hypothesis implies that $p|a_i$, for some i with $1 \leq i \leq n$.

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Basis: $P(2)$ follows from Theorem 5.8.

Inductive Hypothesis: If $n \geq 2$ and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Inductive Step: Suppose that $p|a_1 \cdots a_{n+1}$. Let

$$a = a_1 \cdots a_n \text{ and } b = a_{n+1}.$$

Then $p|ab$ so, from Theorem 5.8, $p|a$ or $p|b$.

If $p|a$ the inductive hypothesis implies that $p|a_i$, for some i with $1 \leq i \leq n$.

If $p|b$ then $p|a_{n+1}$.

Corollary 5.10. *If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.*

Proof. The proof is by induction on n, starting with $n = 2$.

Basis: $P(2)$ follows from Theorem 5.8.

Inductive Hypothesis: If $n \geq 2$ and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Inductive Step: Suppose that $p|a_1 \cdots a_{n+1}$. Let

$$a = a_1 \cdots a_n \text{ and } b = a_{n+1}.$$

Then $p|ab$ so, from Theorem 5.8, $p|a$ or $p|b$.

If $p|a$ the inductive hypothesis implies that $p|a_i$, for some i with $1 \leq i \leq n$.

If $p|b$ then $p|a_{n+1}$.

Hence $p|a_i$, for some i, as required.

Prime Factorisation

An expression of an integer n as a product of primes is called a **prime factorisation** of n.

Prime Factorisation

An expression of an integer n as a product of primes is called a **prime factorisation** of n.

For example 12 and 25 have prime factorisations $12 = 2 \cdot 2 \cdot 3$ and $25 = 5 \cdot 5$, respectively.

Prime Factorisation

An expression of an integer n as a product of primes is called a **prime factorisation** of n.

For example 12 and 25 have prime factorisations $12 = 2 \cdot 2 \cdot 3$ and $25 = 5 \cdot 5$, respectively.

We aim to show that every positive integer greater than one has a prime factorisation and that this prime factorisation is unique, up to the order in which the prime factors occur.

Prime Factorisation

An expression of an integer n as a product of primes is called a **prime factorisation** of n.

For example 12 and 25 have prime factorisations $12 = 2 \cdot 2 \cdot 3$ and $25 = 5 \cdot 5$, respectively.

We aim to show that every positive integer greater than one has a prime factorisation and that this prime factorisation is unique, up to the order in which the prime factors occur.

For instance

$$2 \cdot 5 \cdot 2 \cdot 7,$$
$$2 \cdot 7 \cdot 2 \cdot 5,$$
$$7 \cdot 2 \cdot 2 \cdot 5$$

are all prime factorisations of 140 but are regarded as the same because the number of 2's, 5's and 7's is the same in each.

Example 5.11. Write 7 and 21 as a products of primes:

Example 5.11. Write 7 and 21 as a products of primes:

$$7 \quad \text{and} \quad 3 \cdot 7$$

Example 5.11. Write 7 and 21 as a products of primes:

$$7 \quad \text{and} \quad 3 \cdot 7$$

We consider these as products of primes of length one and two respectively.

Example 5.11. Write 7 and 21 as a products of primes:

$$7 \quad \text{and} \quad 3 \cdot 7$$

We consider these as products of primes of length one and two respectively.

We cannot write 7 as a product of primes of length more than one.

Example 5.11. Write 7 and 21 as a products of primes:

$$7 \quad \text{and} \quad 3 \cdot 7$$

We consider these as products of primes of length one and two respectively.

We cannot write 7 as a product of primes of length more than one.

What about a larger prime like 6991 say? Can I write this as a product of primes: other than the length one product 6991?

The Fundamental Theorem of Arithmetic

Theorem 5.12. *Every integer $n > 1$ is a product of one or more primes. This product is unique apart from the order in which the primes occur.*

The Fundamental Theorem of Arithmetic

Theorem 5.12. *Every integer $n > 1$ is a product of one or more primes. This product is unique apart from the order in which the primes occur.*

Proof.

Step(1) Prove that every $n > 1$ has a prime factorisation.

Step(2) Prove that prime factorisations are unique.

Collected prime factorisation

It is often convenient to write the prime factorisation of an integer with all like primes collected together, in ascending order, and with exponential notation.

Collected prime factorisation

It is often convenient to write the prime factorisation of an integer with all like primes collected together, in ascending order, and with exponential notation.

For example we could write the prime factorisations of 140 and 2200 as

$$140 = 2^2 \cdot 5 \cdot 7 \text{ and}$$
$$2200 = 2^3 \cdot 5^2 \cdot 11.$$

Collected prime factorisation

It is often convenient to write the prime factorisation of an integer with all like primes collected together, in ascending order, and with exponential notation.

For example we could write the prime factorisations of 140 and 2200 as

$$\begin{aligned} 140 &= 2^2 \cdot 5 \cdot 7 \text{ and} \\ 2200 &= 2^3 \cdot 5^2 \cdot 11. \end{aligned}$$

We call this the **collected prime factorisation** of an integer n or say that we've written n in **standard form**.

Collected prime factorisation

It is often convenient to write the prime factorisation of an integer with all like primes collected together, in ascending order, and with exponential notation.

For example we could write the prime factorisations of 140 and 2200 as

$$\begin{aligned} 140 &= 2^2 \cdot 5 \cdot 7 \text{ and} \\ 2200 &= 2^3 \cdot 5^2 \cdot 11. \end{aligned}$$

We call this the **collected prime factorisation** of an integer n or say that we've written n in **standard form**.

From the Fundamental Theorem of Arithmetic it follows that collected prime factorisations are unique. We record this fact in the following corollary.

Corollary 5.13. *Let $n > 1$ be an integer. Then n may be written uniquely as*

$$n = p_1^{a_1} \cdots p_k^{a_k},$$

where $k \geq 1$, $p_1 < \cdots < p_k$, p_i is prime and $a_i \geq 1$.

Corollary 5.13. *Let $n > 1$ be an integer. Then n may be written uniquely as*

$$n = p_1^{a_1} \cdots p_k^{a_k},$$

where $k \geq 1$, $p_1 < \cdots < p_k$, p_i is prime and $a_i \geq 1$.

Example 5.14. It is easy to multiply together integers in standard form: we just add corresponding superscripts.

For example

$$3388 = 2^2 \cdot 7 \cdot 11^2$$

and

$$2200 = 2^3 \cdot 5^2 \cdot 11$$

so

$$3388 \cdot 2200 = 2^5 \cdot 5^2 \cdot 7 \cdot 11^3.$$

In general if integers a and b have standard forms

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \qquad \text{and} \qquad b = p_1^{\beta_1} \cdots p_n^{\beta_n}$$

then ab has standard form

$$ab = p_1^{\alpha_1+\beta_1} \cdots p_n^{\alpha_n+\beta_n}.$$

In general if integers a and b have standard forms

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \qquad \text{and} \qquad b = p_1^{\beta_1} \cdots p_n^{\beta_n}$$

then ab has standard form

$$ab = p_1^{\alpha_1+\beta_1} \cdots p_n^{\alpha_n+\beta_n}.$$

Here we've padded out the collected prime factorisations (with p_i^0 where necessary) to make them the same length: as in the following example.

$$2200 = 2^3 \cdot 5^2 \cdot 11 = 2^3 \cdot 5^2 \cdot 7^0 \cdot 11^1 \cdot 13^0$$

and

$$572572 = 2^2 \cdot 7 \cdot 11^2 \cdot 13^2 = 2^2 \cdot 5^0 \cdot 7^1 \cdot 11^2 \cdot 13^2$$

so

$$2200 \cdot 572572 = 2^5 \cdot 5^2 \cdot 7^1 \cdot 11^3 \cdot 13^2.$$

Example 5.15. Reversing the idea of the previous example, it's easy to find the divisors of an integer given in standard form.

For instance if $a|3388$ then

$$3388 = 2^2 \cdot 7 \cdot 11^2 = ab,$$

for some integer b.

Example 5.16. As 2200 has standard form

$$2^3 \cdot 5^2 \cdot 11$$

the positive divisor of 2200 are of the form

$$2^a 5^b 11^c,$$

where

$$0 \le a \le 3, \qquad 0 \le b \le 2 \qquad \text{and} \qquad 0 \le c \le 1.$$

First list all such triples (a, b, c):

$$\begin{array}{cccccc}
(0,0,0) & (0,0,1) & (0,1,0) & (0,1,1) & (0,2,0) & (0,2,1) \\
(1,0,0) & (1,0,1) & (1,1,0) & (1,1,1) & (1,2,0) & (1,2,1) \\
(2,0,0) & (2,0,1) & (2,1,0) & (2,1,1) & (2,2,0) & (2,2,1) \\
(3,0,0) & (3,0,1) & (3,1,0) & (3,1,1) & (3,2,0) & (3,2,1)
\end{array}$$

First list all such triples (a, b, c):

$$\begin{array}{cccccc}
(0,0,0) & (0,0,1) & (0,1,0) & (0,1,1) & (0,2,0) & (0,2,1) \\
(1,0,0) & (1,0,1) & (1,1,0) & (1,1,1) & (1,2,0) & (1,2,1) \\
(2,0,0) & (2,0,1) & (2,1,0) & (2,1,1) & (2,2,0) & (2,2,1) \\
(3,0,0) & (3,0,1) & (3,1,0) & (3,1,1) & (3,2,0) & (3,2,1)
\end{array}$$

The positive divisors of 2200 are therefore:

$$\begin{array}{cccccc}
1 & 11 & 5 & 5 \cdot 11 & 5^2 & 5^2 \cdot 11 \\
2 & 2 \cdot 11 & 2 \cdot 5 & 2 \cdot 5 \cdot 11 & 2 \cdot 5^2 & 2 \cdot 5^2 \cdot 11 \\
2^2 & 2^2 \cdot 11 & 2^2 \cdot 5 & 2^2 \cdot 5 \cdot 11 & 2^2 \cdot 5^2 & 2^2 \cdot 5^2 \cdot 11 \\
2^3 & 2^3 \cdot 11 & 2^3 \cdot 5 & 2^3 \cdot 5 \cdot 11 & 2^3 \cdot 5^2 & 2^3 \cdot 5^2 \cdot 11
\end{array}$$

Example 5.17. It's easy to find the greatest common divisor of numbers in standard form.

The standard form of 572572 is

$$2^2 \cdot 7 \cdot 11^2 \cdot 13^2$$

so any divisor of 572572 has the form

$$2^e 7^f 11^g 13^h,$$

with

$$0 \leq e \leq 2, \qquad 0 \leq f \leq 1, \qquad 0 \leq g \leq 2 \qquad \text{and} \qquad 0 \leq h \leq 2.$$

Example 5.17. It's easy to find the greatest common divisor of numbers in standard form.

The standard form of 572572 is

$$2^2 \cdot 7 \cdot 11^2 \cdot 13^2$$

so any divisor of 572572 has the form

$$2^e 7^f 11^g 13^h,$$

with

$$0 \le e \le 2, \qquad 0 \le f \le 1, \qquad 0 \le g \le 2 \qquad \text{and} \qquad 0 \le h \le 2.$$

Hence common divisors of 2200 and 572572 have the form $2^u 11^v$, with $0 \le u \le 2$ and $0 \le v \le 1$.

Example 5.17. It's easy to find the greatest common divisor of numbers in standard form.

The standard form of 572572 is

$$2^2 \cdot 7 \cdot 11^2 \cdot 13^2$$

so any divisor of 572572 has the form

$$2^e 7^f 11^g 13^h,$$

with

$$0 \le e \le 2, \qquad 0 \le f \le 1, \qquad 0 \le g \le 2 \qquad \text{and} \qquad 0 \le h \le 2.$$

Hence common divisors of 2200 and 572572 have the form $2^u 11^v$, with $0 \le u \le 2$ and $0 \le v \le 1$.

Therefore $\gcd(2200, 572572) = 2^2 \cdot 11 = 44$.

Example 5.18. Find $\gcd(11990979, 637637)$.

Fermat's Method of Factorisation

Multiplying: easy

Fermat's Method of Factorisation

Multiplying: easy

Factoring: difficult

Fermat's Method of Factorisation

Multiplying: easy

Factoring: difficult

See `www.rsasecurity.com/rsalabs/node.asp?id=2094#GetTheNumbers`

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$
$$16311^2 - 266004389 = 44332$$

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$
$$16311^2 - 266004389 = 44332$$
$$16312^2 - 266004389 = 76955$$

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$
$$16311^2 - 266004389 = 44332$$
$$16312^2 - 266004389 = 76955$$
$$16313^2 - 266004389 = 109580$$

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$
$$16311^2 - 266004389 = 44332$$
$$16312^2 - 266004389 = 76955$$
$$16313^2 - 266004389 = 109580$$
$$16314^2 - 266004389 = 142207$$

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$
$$16311^2 - 266004389 = 44332$$
$$16312^2 - 266004389 = 76955$$
$$16313^2 - 266004389 = 109580$$
$$16314^2 - 266004389 = 142207$$
$$16315^2 - 266004389 = 174836$$

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$
$$16311^2 - 266004389 = 44332$$
$$16312^2 - 266004389 = 76955$$
$$16313^2 - 266004389 = 109580$$
$$16314^2 - 266004389 = 142207$$
$$16315^2 - 266004389 = 174836$$
$$16316^2 - 266004389 = 207467$$

Example 5.19. Use Fermat's method of factorisation to find factors of 266004389.

We have $16309 < \sqrt{266004389} < 16310$. Therefore we start with $u = 16310$:

$$16310^2 - 266004389 = 11711$$
$$16311^2 - 266004389 = 44332$$
$$16312^2 - 266004389 = 76955$$
$$16313^2 - 266004389 = 109580$$
$$16314^2 - 266004389 = 142207$$
$$16315^2 - 266004389 = 174836$$
$$16316^2 - 266004389 = 207467$$
$$16317^2 - 266004389 = 240100 = 490^2.$$

Therefore $266004389 = 16317^2 - 490^2 = (16317 + 490)(16317 - 490)$.

Therefore $266004389 = 16317^2 - 490^2 = (16317 + 490)(16317 - 490)$.

$16317 + 490 = 16807$ and $16317 - 490 = 15827$ so

$$266004389 = 16807 \cdot 15827.$$

Therefore $266004389 = 16317^2 - 490^2 = (16317 + 490)(16317 - 490)$.

$16317 + 490 = 16807$ and $16317 - 490 = 15827$ so

$$266004389 = 16807 \cdot 15827.$$

Unfortunately, if n does not have 2 factors of similar size then this method of factoring can be very slow.

(It does however form the basis of some more powerful methods.)

Primality testing

Is n prime?

Primality testing

Is n prime?

Test it for divisibility by all prime numbers p such that $1 < p < n$.

Primality testing

Is n prime?

Test it for divisibility by all prime numbers p such that $1 < p < n$.

Better to use the following lemma.

Primality testing

Is n prime?

Test it for divisibility by all prime numbers p such that $1 < p < n$.

Better to use the following lemma.

Lemma 5.20. *An integer* $n > 1$ *is composite if and only if it has a prime divisor* p *such that* $p < \sqrt{n}$.

Example 5.21. To find all primes in the range 1 to 45:

Example 5.21. To find all primes in the range 1 to 45:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$$

is now a complete list of primes between 1 and 45.

Example 5.21. To find all primes in the range 1 to 45:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$$

is now a complete list of primes between 1 and 45.

This method of constructing lists of primes is known as the Sieve of Eratosthenes.

Example 5.21. To find all primes in the range 1 to 45:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$$

is now a complete list of primes between 1 and 45.

This method of constructing lists of primes is known as the Sieve of Eratosthenes.

In fact it is still too inefficient to use in practice to determine if a large number is prime.

A Theorem of Euclid

The following theorem appears in Book IX of the Elements, a mathematical textbook written by Euclid: a Greek mathematician who lived around 300 bc.

Theorem 5.22. *There are infinitely many primes.*

A Theorem of Euclid

The following theorem appears in Book IX of the Elements, a mathematical textbook written by Euclid: a Greek mathematician who lived around 300 bc.

Theorem 5.22. *There are infinitely many primes.*

The proof is by contradiction.

Objectives

After covering this chapter of the course you should be able to:

(i) recall Theorem 2.21 and understand its proof;

(ii) define a coprime pair of integers;

(iii) recall Corollary 5.3 and Euclid's Lemma and understand their proofs;

(iv) define prime and composite numbers;

(v) recall the prime divisor property, Theorem 5.8, and understand its proof;

(vi) recall the Fundamental Theorem of Arithmetic, Theorem 5.12, and understand its proof;

(vii) recognise and write down the prime factorisation and standard form or collected prime factorisation of an integer;

(viii) use prime factorisation to find divisors and greatest common divisors;

(ix) recall the statement of Theorem 5.22 and understand its proof.

Casting Out Nines

This is a method of testing integers for divisibility by 9.

Procedure 6.1. *Given a non–negative integer (written in base* 10*) repeat the following steps (in any order) until a number less than* 9 *is obtained.*

1. *Cross out any digits that sum to* 9 *or a multiple of* 9*.*

2. *Add the remaining digits.*

Casting Out Nines

This is a method of testing integers for divisibility by 9.

Procedure 6.1. *Given a non–negative integer (written in base* 10*) repeat the following steps (in any order) until a number less than* 9 *is obtained.*

1. Cross out any digits that sum to 9 *or a multiple of* 9*.*

2. Add the remaining digits.

The result is the remainder of division of n *by* 9*.*

Casting Out Nines

This is a method of testing integers for divisibility by 9.

Procedure 6.1. *Given a non–negative integer (written in base* 10*) repeat the following steps (in any order) until a number less than* 9 *is obtained.*

1. Cross out any digits that sum to 9 *or a multiple of* 9*.*

2. Add the remaining digits.

The result is the remainder of division of n *by* 9*.*

Example 6.2. Cast out Nines from 215763401.

Casting Out Nines

This is a method of testing integers for divisibility by 9.

Procedure 6.1. *Given a non–negative integer (written in base 10) repeat the following steps (in any order) until a number less than 9 is obtained.*

1. Cross out any digits that sum to 9 or a multiple of 9.

2. Add the remaining digits.

The result is the remainder of division of n by 9.

Example 6.2. Cast out Nines from 215763401.

Example 6.3. Cast out Nines from 51422211.

Arithmetic checking

The casting out nines procedure can be used to check the results of numerical calculations.

Arithmetic checking

The casting out nines procedure can be used to check the results of numerical calculations.

Example 6.4. Check the computation

$$215763401 \times 51422216 = 11095032211116616.$$

Arithmetic checking

The casting out nines procedure can be used to check the results of numerical calculations.

Example 6.4. Check the computation

$$215763401 \times 51422216 = 11095032211116616.$$

Example 6.5. Check

$$5^7 + 3 = 78128 = 304 \times 257$$

for arithmetic mistakes.

Divisiblity by 9

We can also use casting out nines to check for divisibility by 9. A number is divisible by 9 if and only if the result is 0.

Divisiblity by 9

We can also use casting out nines to check for divisibility by 9. A number is divisible by 9 if and only if the result is 0.

Example 6.6. Decide which of 215763401, 51422216 and 3254787 is divisible by 9.

The Telephone Number Trick

1. Write down your telephone number.

2. Write down your telephone number with digits reversed.

3. Subtract the smaller of these two numbers from the larger.

4. By casting out nines from the result decide whether or not it is divisible by 9.

The “Odd & Even” Number System

Red, white and blue arithmetic

Congruence

In the Red, White and Blue number system we collected together all integers which left remainder 1, after attempting division by 3, and called them blue.

Notice that if a and b are blue then $3|b-a$.

Conversely, given any two integers a and b such that $3|b-a$ we can write

$$b - a = 3k, \text{ for some } k \in \mathbb{Z}.$$

Using the division algorithm we can also write

$$b = 3q + r, \text{ for } r = 0, 1 \text{ or } 2.$$

Therefore

$$a = b - 3k = 3(q - k) + r.$$

That is a and b are both the same colour in the Red, White and Blue number system.

Our analysis shows that a and b are the same colour if and only if $3|b - a$. Generalising this from 3 to an arbitrary integer n leads us to the definition of congruence.

Definition 6.7. Let n be a positive integer and let $a, b \in \mathbb{Z}$. If $n|b-a$ then we say that a is **congruent** to b **modulo** n, and write

$$a \equiv b \pmod{n}.$$

For instance $17 \equiv 5 \pmod{12}$ and $216 \equiv 6 \pmod{7}$.

As in the case $n = 3$ above, $a \equiv b \pmod{n}$ if and only if a and b both leave the same remainder after attempting division by n.

In fact, if

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \qquad (6.1)$$

then

$$b - a = n(p - q),$$

so $n|b-a$: that is $a \equiv b \pmod{n}$.

On the other hand if we know that $a \equiv b \pmod{n}$ then $n|b-a$ so, using the argument above, with n instead of 3, we'll find that there is some r such that (6.1) holds.

Example 6.8. Congruence modulo 2 gives rise to the Odd and Even number system.

Example 6.9. Congruence modulo 3 gives rise to the Red, White and Blue number system.

Example 6.10. Suppose $n = 10$.

Then $0 \equiv 10 \pmod{10}$, $10 \equiv 101090 \pmod{10}$, $11 \equiv 121 \pmod{10}$ and $27 \equiv 253427 \pmod{10}$.

Every positive integer is congruent to its last digit (written to base 10).

In particular integers congruent to 0 all end in the digit 0.

These are exactly the integers divisible by 10.

Congruence is not the same as equality but it does share some of the properties of equality.

If we have any integers a, b and c and n is a positive integer then

1. $a \equiv a \pmod{n}$,
2. if $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$ and
3. if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

These are all properties of equality.

Let's check them for congruence.

The first one is easy since $n|0 = a - a$, for all integers a.

We'll check the last one here and leave the second as an exercise.

Modular arithmetic

Arithmetic with congruences is called modular arithmetic.

We've already seen a couple of examples: Odd & Even arithmetic and Red, White and Blue arithmetic.

The idea is to add and multiply integers in the usual way but to regard two numbers as the same if they are congruent.

There is a possible problem with this. Suppose we work modulo 10, that is $n = 10$.

Now take two integers which are congruent modulo 10, say 23 and 3. We are to regard these as the same.

This means that if we do something to one, say add 6, then we should get the same answer as if we add 6 to the other.

Here "the same answer" means the same answer modulo 10. Let's see:

$$23 + 6 = 29 \quad \text{and} \quad 3 + 6 = 9.$$

This is alright because $29 \equiv 9 \pmod{10}$ and so we regard 29 and 9 as the same.

Does this always work? The purpose of the next Lemma is to reassure us that it does.

Modular arithmetic is consistent

Lemma 6.11. *Let n be a positive integer. Suppose that a, b, u and v are integers such that*

$$a \equiv u \pmod{n}$$

and

$$b \equiv v \pmod{n}.$$

Then

(i) $-a \equiv -u \pmod{n}$*;*

(ii) $a + b \equiv u + v \pmod{n}$ *and*

(iii) $ab \equiv uv \pmod{n}$*.*

We prove parts (i) and (iii) here, leaving part (ii) as an exercise.

Lemma 6.12. *Every integer is congruent modulo* n *to one and only one of the integers in the list* $0, 1, \ldots, n-1$.

Lemma 6.12. *Every integer is congruent modulo n to one and only one of the integers in the list $0, 1, \ldots, n-1$.*

Proof. This follows from the division algorithm because if $a \in \mathbb{Z}$ then we can write $a = nq + r$, with $0 \leq r < n$.

Lemma 6.12. *Every integer is congruent modulo n to one and only one of the integers in the list $0, 1, \ldots, n-1$.*

Proof. This follows from the division algorithm because if $a \in \mathbb{Z}$ then we can write $a = nq + r$, with $0 \leq r < n$.

Then $n|a - r$ so $a \equiv r \pmod{n}$ and r is in the given list.

Lemma 6.12. *Every integer is congruent modulo n to one and only one of the integers in the list $0, 1, \ldots, n-1$.*

Proof. This follows from the division algorithm because if $a \in \mathbb{Z}$ then we can write $a = nq + r$, with $0 \le r < n$.

Then $n|a - r$ so $a \equiv r \pmod{n}$ and r is in the given list.

If $a \equiv r \pmod{n}$ and $a \equiv s \pmod{n}$ then, from the above, $r \equiv s$ with $0 \le r < n$ and $0 \le s < n$.

Lemma 6.12. *Every integer is congruent modulo n to one and only one of the integers in the list $0, 1, \ldots, n-1$.*

Proof. This follows from the division algorithm because if $a \in \mathbb{Z}$ then we can write $a = nq + r$, with $0 \leq r < n$.

Then $n|a - r$ so $a \equiv r \pmod{n}$ and r is in the given list.

If $a \equiv r \pmod{n}$ and $a \equiv s \pmod{n}$ then, from the above, $r \equiv s$ with $0 \leq r < n$ and $0 \leq s < n$.

Assuming that $r > s$ then $n|r-s$ and $n > r \geq r-s$, contradicting Lemma 2.18.3.

Lemma 6.12. *Every integer is congruent modulo n to one and only one of the integers in the list $0, 1, \ldots, n-1$.*

Proof. This follows from the division algorithm because if $a \in \mathbb{Z}$ then we can write $a = nq + r$, with $0 \leq r < n$.

Then $n|a - r$ so $a \equiv r \pmod{n}$ and r is in the given list.

If $a \equiv r \pmod{n}$ and $a \equiv s \pmod{n}$ then, from the above, $r \equiv s$ with $0 \leq r < n$ and $0 \leq s < n$.

Assuming that $r > s$ then $n|r-s$ and $n > r \geq r-s$, contradicting Lemma 2.18.3.

Thus a is congruent to only one integer in the list. $\square$

Example 6.13. In modular arithmetic we can always avoid computation with large numbers.

For example working modulo 10 we have

$$7459898790352045324 \equiv 4 \pmod{10}$$

and

$$9874558754423 \equiv 3 \pmod{10}.$$

Therefore

$$7459898790352045324 \cdot 9874558754423 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod{10}.$$

Similarly, working modulo 7 we have

$$4543362 \equiv 5 \pmod{7}.$$

Therefore

$$4543362^2 \equiv 5^2 \equiv 25 \equiv 4 \pmod{7}$$

and

$$4543362^3 = 4543362 \cdot 4543362^2 \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod{7}.$$

Divisibility by 9

When we write a number like 20195 to base 10 we are expressing the number

$$2 \times 10^4 + 0 \times 10^3 + 1 \times 10^2 + 9 \times 10^1 + 5$$

in shorthand (there's a 1 in the 100's column etc.).

Applying this argument in general we write

$$a_m a_{m-1} \cdots a_1 a_0$$

for the number

$$a_m \times 10^m + a_{m-1} \times 10^{m-1} + \cdots + a_1 \times 10 + a_0.$$

As $10^k \equiv 1 \pmod 9$, for $k = 1, \ldots, m$, we have

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9. \qquad (6.2)$$

Casting out nines again

Suppose we cast out nines (Procedure 6.1) from an integer m.

In Step 1 we cross out any digits which sum to a multiple of 9.

The sum of these digits is congruent to zero modulo 9 so, from (6.2), the result is an integer congruent to m modulo 9.

In Step 2 we add the digits and again, from (6.2), the result is an integer congruent to m modulo 9.

Thus the casting out nines procedure results at every stage in an integer congruent to m modulo 9.

The procedure ends with a number r such that $0 \leq r < 9$ and $r \equiv m \pmod 9$.

Therefore $9|m - r$, from which it follows that $m = 9q + r$, for some $q \in \mathbb{Z}$ and $0 \leq r < 9$.

That is, the output from Casting out Nines is the unique remainder guaranteed by the division algorithm, on attempting division by 9.

Divisibility by 9

The following lemma follows from (6.2).

Lemma 6.14. *An integer is divisible by* 9 *if and only if the sum of its digits is divisible by* 9.

Example 6.15. Are 31357989921 or 5179183229478 divisible by 9?

Divisibility by 4

Now $10^2 \equiv 0 \pmod 4$. Thus, for example,

$$1932526 = (19325 \times 100) + 26 \equiv 26 \pmod 4$$

and

$$93975656489084357745565568738675 =$$
$$(939756564890843577455655687386 \times 100) + 75 \equiv 75 \pmod 4.$$

More generally, if $a_m \cdots a_1 a_0$ is an integer written to base 10 then

$$a_m \cdots a_1 a_0 = (a_m \cdots a_2 \times 100) + a_1 a_0 \equiv a_1 a_0 \pmod{4}.$$

Therefore

$$a_m \cdots a_1 a_0 \equiv 0 \pmod{4} \quad \text{if and only if} \quad a_1 a_0 \equiv 0 \pmod{4}.$$

That is

$$4 | a_m \cdots a_1 a_0 \Leftrightarrow 4 | a_1 a_0.$$

Example 6.16. Does 4 divide 937475900345 or 80345003732?

Inverses in modular arithmetic

If we work in the rational numbers $\mathbb{Q}$ we can find a multiplicative inverse for any non-zero element.

For example the inverse of $11/201$ is $201/11$.

The same is true in $\mathbb{R}$ where the inverse of $x \neq 0$ is $1/x$.

In general if x is a number and y has the property that $xy = 1$ then we say that x has **inverse** y.

Most elements of $\mathbb{Z}$ don't have inverses in $\mathbb{Z}$. For example 2 has no inverse.

In fact ± 1 are the only elements of $\mathbb{Z}$ which have inverses. What about arithmetic modulo n.

Inverses modulo n

Example 6.17. Try to find the inverse of 2 modulo 6.

Example 6.18. Do either 3 or 7 have inverses modulo 10?

Example 6.19. Which numbers have inverses modulo 8?

Lemma 6.20. *An integer a has an inverse modulo n if and only if*

$$\gcd(a, n) = 1.$$

Lemma 6.20. *An integer a has an inverse modulo n if and only if*

$$\gcd(a, n) = 1.$$

What happens if we do arithmetic modulo a prime number p?

In this case, for every integer a either

Lemma 6.20. *An integer a has an inverse modulo n if and only if*

$$\gcd(a, n) = 1.$$

What happens if we do arithmetic modulo a prime number p?

In this case, for every integer a either

1. $p \nmid a$ in which case $\gcd(a, p) = 1$ or

Lemma 6.20. *An integer a has an inverse modulo n if and only if*

$$\gcd(a, n) = 1.$$

What happens if we do arithmetic modulo a prime number p?

In this case, for every integer a either

1. $p \nmid a$ in which case $\gcd(a, p) = 1$ or

2. $p|a$ in which case $a \equiv 0 \pmod{p}$.

Lemma 6.20. *An integer a has an inverse modulo n if and only if*

$$\gcd(a, n) = 1.$$

What happens if we do arithmetic modulo a prime number p?

In this case, for every integer a either

1. $p \nmid a$ in which case $\gcd(a, p) = 1$ or

2. $p | a$ in which case $a \equiv 0 \pmod{p}$.

Thus every integer which is not congruent to zero modulo p has an inverse.

In this way arithmetic modulo p resembles arithmetic in $\mathbb{Q}$ more closely that arithmetic in $\mathbb{Z}$.

Example 6.21. Write out the multiplication table for arithmetic modulo 5 with the integers $0, 1, 2, 3$ and 4. Hence find the inverse of every integer which is not congruent to zero modulo 5.

Solving Congruences

Example 6.22. Find all integers x such that

$$2x \equiv 4 \pmod{6}. \tag{6.3}$$

We call such equations **congruences** and this is an example of a **linear** congruence.

Solving Congruences

Example 6.22. Find all integers x such that

$$2x \equiv 4 \pmod{6}. \qquad (6.3)$$

We call such equations **congruences** and this is an example of a **linear** congruence.

If $x = a$ is a solution and $a \equiv b$ then $x = b$ is also a solution: so if there's one solution there are infinitely many.

Solving Congruences

Example 6.22. Find all integers x such that

$$2x \equiv 4 \pmod{6}. \tag{6.3}$$

We call such equations **congruences** and this is an example of a **linear** congruence.

If $x = a$ is a solution and $a \equiv b$ then $x = b$ is also a solution: so if there's one solution there are infinitely many.

Every integer is congruent to one of

$$0, 1, \ldots, n-1 \text{ modulo } n$$

so we seek solutions to congruences in this range.

Method 1

x	0	1	2	3	4	5
$2x \pmod 6$						

Method 1

x	0	1	2	3	4	5
$2x \pmod 6$						

From the table we see that the only solutions are $x = 2$ and $x = 5$.

Method 2

$$ax \equiv b \pmod{n} \tag{6.4}$$

Method 2

$$ax \equiv b \pmod{n} \tag{6.4}$$

x is a solution to (6.4) if and only if $n|(ax - b)$

Method 2

$$ax \equiv b \pmod{n} \tag{6.4}$$

x is a solution to (6.4) if and only if $n|(ax - b)$

if and only if $ax - b = ny$, for some integer y

Method 2

$$ax \equiv b \pmod{n} \tag{6.4}$$

x is a solution to (6.4) if and only if $n|(ax - b)$

if and only if $ax - b = ny$, for some integer y

if and only if $ax - ny = b$, for some $y \in \mathbb{Z}$.

Method 2

$$ax \equiv b \pmod{n} \tag{6.4}$$

x is a solution to (6.4) if and only if $n|(ax - b)$

if and only if $ax - b = ny$, for some integer y

if and only if $ax - ny = b$, for some $y \in \mathbb{Z}$.

From Theorem 5.5 this has a solution if and only if $\gcd(a, n)|b$.

Method 2

$$ax \equiv b \pmod{n} \tag{6.4}$$

x is a solution to (6.4) if and only if $n|(ax - b)$

if and only if $ax - b = ny$, for some integer y

if and only if $ax - ny = b$, for some $y \in \mathbb{Z}$.

From Theorem 5.5 this has a solution if and only if $\gcd(a, n)|b$.

If $\gcd(a, n)|b$ then we can use the Euclidean algorithm to find a particular solution to the equation.

Writing $\gcd(a, n) = d$, if $d|b$ and $x = u$, $y = v$ is a solution

Writing $\gcd(a, n) = d$, if $d|b$ and $x = u$, $y = v$ is a solution

then the list of solutions to this equation consists of all the pairs

$$x = u - (n/d)t,\ y = v - (a/d)t,\ \text{for } t \in \mathbb{Z}.$$

Writing $\gcd(a, n) = d$, if $d|b$ and $x = u$, $y = v$ is a solution

then the list of solutions to this equation consists of all the pairs

$$x = u - (n/d)t, \ y = v - (a/d)t, \ \text{for } t \in \mathbb{Z}.$$

Applying this to congruence (6.3) above,

Writing $\gcd(a, n) = d$, if $d|b$ and $x = u$, $y = v$ is a solution

then the list of solutions to this equation consists of all the pairs

$$x = u - (n/d)t, \ y = v - (a/d)t, \ \text{for } t \in \mathbb{Z}.$$

Applying this to congruence (6.3) above,

In the general case (of congruence (6.4)) the only remaining question is which of the solutions we have found are congruent?

Writing $\gcd(a, n) = d$, if $d|b$ and $x = u$, $y = v$ is a solution

then the list of solutions to this equation consists of all the pairs

$$x = u - (n/d)t, \;\; y = v - (a/d)t, \;\; \text{for } t \in \mathbb{Z}.$$

Applying this to congruence (6.3) above,

In the general case (of congruence (6.4)) the only remaining question is which of the solutions we have found are congruent?

If $d|b$ and $x = u$ is one solution to the congruence (6.4)

Writing $\gcd(a, n) = d$, if $d|b$ and $x = u$, $y = v$ is a solution

then the list of solutions to this equation consists of all the pairs

$$x = u - (n/d)t, \ y = v - (a/d)t, \ \text{for } t \in \mathbb{Z}.$$

Applying this to congruence (6.3) above,

In the general case (of congruence (6.4)) the only remaining question is which of the solutions we have found are congruent?

If $d|b$ and $x = u$ is one solution to the congruence (6.4)

then the list of solutions to (6.4) consists of the integers of the form $u - (n/d)t$, for $t \in \mathbb{Z}$.

Theorem 6.23. *Let* a, b *and* n *be integers with* $n > 0$ *and let* $d = \gcd(a, n)$*. Then the congruence* (6.4) *has a solution if and only if* $d|n$*. If* $d|n$ *then there are exactly* d *pairwise incongruent solutions to* (6.4)*.*

Theorem 6.23. *Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$. Then the congruence* (6.4) *has a solution if and only if $d|n$. If $d|n$ then there are exactly d pairwise incongruent solutions to* (6.4).

Example 6.24. Find all solutions to the congruence

$$2x \equiv 3 \pmod 6.$$

Theorem 6.23. *Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$. Then the congruence* (6.4) *has a solution if and only if $d|n$. If $d|n$ then there are exactly d pairwise incongruent solutions to* (6.4).

Example 6.24. Find all solutions to the congruence

$$2x \equiv 3 \pmod{6}.$$

Example 6.25. Find all solutions to the congruence $6x \equiv 9 \pmod{15}$.

Theorem 6.23. *Let* a, b *and* n *be integers with* $n > 0$ *and let* $d = \gcd(a, n)$*. Then the congruence* (6.4) *has a solution if and only if* $d|n$*. If* $d|n$ *then there are exactly* d *pairwise incongruent solutions to* (6.4)*.*

Example 6.24. Find all solutions to the congruence

$$2x \equiv 3 \pmod 6.$$

Example 6.25. Find all solutions to the congruence $6x \equiv 9 \pmod{15}$.

Example 6.26. Compare the solutions to the congruences

$$2x \equiv 4 \pmod 6 \text{ and } x \equiv 2 \pmod 6.$$

Random numbers: an application

In situations where we require random numbers we often wish to give a machine the task of generating these numbers.

Random numbers: an application

In situations where we require random numbers we often wish to give a machine the task of generating these numbers.

In many cases we'd also like the machine to be able to reproduce the sequence of random numbers that it outputs so that we can verify our results.

Random numbers: an application

In situations where we require random numbers we often wish to give a machine the task of generating these numbers.

In many cases we'd also like the machine to be able to reproduce the sequence of random numbers that it outputs so that we can verify our results.

Such sequences cannot be truly random and are called **pseudo-random**.

Random numbers: an application

In situations where we require random numbers we often wish to give a machine the task of generating these numbers.

In many cases we'd also like the machine to be able to reproduce the sequence of random numbers that it outputs so that we can verify our results.

Such sequences cannot be truly random and are called **pseudo-random**.

Pseudo-random numbers are often generated by computer but this means that we need to find good algorithms to produce them.

Random numbers: an application

In situations where we require random numbers we often wish to give a machine the task of generating these numbers.

In many cases we'd also like the machine to be able to reproduce the sequence of random numbers that it outputs so that we can verify our results.

Such sequences cannot be truly random and are called **pseudo-random**.

Pseudo-random numbers are often generated by computer but this means that we need to find good algorithms to produce them.

The art and science of random number generation is highly developed and very sophisticated. You can see this by looking at the web page Random number generators – The pLab Project Home Page at http://random.mat.sbg.ac.at/.

D.H. Lehmer's method (1949)

To generate a sequence of "random looking" integers

$$a_0, a_1, a_2, \ldots$$

use the following process.

D.H. Lehmer's method (1949)

To generate a sequence of "random looking" integers

$$a_0, a_1, a_2, \ldots$$

use the following process.

1. Fix a positive number n and two integers m and c, with $2 \leq m < n$ and $0 \leq c < n$.

D.H. Lehmer's method (1949)

To generate a sequence of "random looking" integers

$$a_0, a_1, a_2, \ldots$$

use the following process.

1. Fix a positive number n and two integers m and c, with $2 \leq m < n$ and $0 \leq c < n$.

2. Choose a start value a_0, such that $0 \leq a_0 \leq n$.

D.H. Lehmer's method (1949)

To generate a sequence of "random looking" integers

$$a_0, a_1, a_2, \ldots$$

use the following process.

1. Fix a positive number n and two integers m and c, with $2 \leq m < n$ and $0 \leq c < n$.

2. Choose a start value a_0, such that $0 \leq a_0 \leq n$.

3. Generate elements of the sequence successively using the formula

$$a_{k+1} = ma_k + c \pmod{n}, \quad \text{where} \quad 0 \leq a_{k+1} < n.$$

D.H. Lehmer's method (1949)

To generate a sequence of “random looking” integers

$$a_0, a_1, a_2, \ldots$$

use the following process.

1. Fix a positive number n and two integers m and c, with $2 \leq m < n$ and $0 \leq c < n$.

2. Choose a start value a_0, such that $0 \leq a_0 \leq n$.

3. Generate elements of the sequence successively using the formula

$$a_{k+1} = ma_k + c \pmod{n}, \quad \text{where} \quad 0 \leq a_{k+1} < n.$$

If a large value of n is chosen the sequence appears random, at least to start with.

Example 6.27. With $n = 800$, $m = 71$, $c = 57$, and $a_0 = 2$ the first ten elements of the sequence are

$$2, 199, 586, 63, 530, 87, 634, 271, 98, 615.$$

Example 6.27. With $n = 800$, $m = 71$, $c = 57$, and $a_0 = 2$ the first ten elements of the sequence are

$$2, 199, 586, 63, 530, 87, 634, 271, 98, 615.$$

Now altering a_0 to 551 the sequence produced is

$$551, 778, 95, 402, 599, 186, 463, 130, 487, 234.$$

Example 6.27. With $n = 800$, $m = 71$, $c = 57$, and $a_0 = 2$ the first ten elements of the sequence are

$$2, 199, 586, 63, 530, 87, 634, 271, 98, 615.$$

Now altering a_0 to 551 the sequence produced is

$$551, 778, 95, 402, 599, 186, 463, 130, 487, 234.$$

Keeping everything fixed except $n = 8000$ we obtain

$$551, 7178, 5695, 4402, 599, 2586, 7663, 130, 1287, 3434.$$

Example 6.27. With $n = 800$, $m = 71$, $c = 57$, and $a_0 = 2$ the first ten elements of the sequence are

$$2, 199, 586, 63, 530, 87, 634, 271, 98, 615.$$

Now altering a_0 to 551 the sequence produced is

$$551, 778, 95, 402, 599, 186, 463, 130, 487, 234.$$

Keeping everything fixed except $n = 8000$ we obtain

$$551, 7178, 5695, 4402, 599, 2586, 7663, 130, 1287, 3434.$$

With $n = 40$, $m = 22$, $c = 20$ and $a_0 = 13$ we obtain

$$13, 26, 32, 4, 28, 36, 12, 4, 28, 36, 12.$$

Of course such sequences are not random (by definition) and we have a formula for the terms.

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 6.28. *The* kth *term of the sequence generated by the process above is*

$$a_k = \left(m^k a_0 + \frac{c(m^k - 1)}{(m-1)} \right) \pmod{n},$$

with $0 \le a_k < n$.

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 6.28. *The kth term of the sequence generated by the process above is*

$$a_k = \left(m^k a_0 + \frac{c(m^k - 1)}{(m-1)} \right) \pmod{n},$$

with $0 \le a_k < n$.

Analysis of "how random" a pseudo-random sequence is involves applying statistical tests to the sequence.

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 6.28. *The kth term of the sequence generated by the process above is*

$$a_k = \left(m^k a_0 + \frac{c(m^k - 1)}{(m-1)} \right) \pmod{n},$$

with $0 \leq a_k < n$.

Analysis of "how random" a pseudo-random sequence is involves applying statistical tests to the sequence.

For instance the frequency of occurence of a particular integers in the sequence can be tested;

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 6.28. *The kth term of the sequence generated by the process above is*

$$a_k = \left(m^k a_0 + \frac{c(m^k - 1)}{(m-1)} \right) \pmod{n},$$

with $0 \leq a_k < n$.

Analysis of “how random” a pseudo-random sequence is involves applying statistical tests to the sequence.

For instance the frequency of occurence of a particular integers in the sequence can be tested;

as can the frequency of occurence of pairs of integers.

Objectives

After covering this chapter of the course you should be able to:

(i) recall the definition of congruence;

(ii) recall the statement of Lemma 6.11 and understand its proof;

(iii) do arithmetic modulo n;

(iv) understand how various divisibility tests work and be able to apply them;

(v) decide whether or not an integer has an inverse modulo n;

(vi) generate a sequence of random looking numbers.