Preamble

- Introduction to Pure Mathematics.
- Main theme – the notion of proof.
- Subsidiary theme – learning to write mathematics.

Preamble

- Introduction to Pure Mathematics.
- Main theme – the notion of proof.
- Subsidiary theme – learning to write mathematics.

Preamble

- Introduction to Pure Mathematics.
- Main theme – the notion of proof.
- Subsidiary theme – learning to write mathematics.

In mathematics we usually consider statements which are either true or false.

We do not consider a statement is known to be true until it has been explained clearly why it is.

We call such an explanation a proof.

The module is based on a principal branch of pure mathematics: algebra, via number systems.

Investigation of number systems involves making precise statements and deciding whether or not they are true.

Explanations and arguments must clearly set out and logically structured so that they can be understood by any reader with the appropriate background.

An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

In mathematics we usually consider statements which are either true or false.
We do not consider a statement is known to be true until it has been explained clearly why it is.
We call such an explanation a proof.
The module is based on a principal branch of pure mathematics: algebra, via number systems.
Investigation of number systems involves making precise statements and deciding whether or not they are true.
Explanations and arguments must clearly set out and logically structured so that they can be understood by any reader with the appropriate background.
An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

In mathematics we usually consider statements which are either true or false.
We do not consider a statement is known to be true until it has been explained clearly why it is.
We call such an explanation a proof.
The module is based on a principal branch of pure mathematics: algebra, via number systems.
Investigation of number systems involves making precise statements and deciding whether or not they are true.
Explanations and arguments must clearly set out and logically structured so that they can be understood by any reader with the appropriate background.
An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

In mathematics we usually consider statements which are either true or false.
We do not consider a statement is known to be true until it has been explained clearly why it is.
We call such an explanation a proof.
The module is based on a principal branch of pure mathematics: algebra, via number systems.
Investigation of number systems involves making precise statements and deciding whether or not they are true.
Explanations and arguments must clearly set out and logically structured so that they can be understood by any reader with the appropriate background.
An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

In mathematics we usually consider statements which are either true or false.
We do not consider a statement is known to be true until it has been explained clearly why it is.
We call such an explanation a proof.
The module is based on a principal branch of pure mathematics: algebra, via number systems.
Investigation of number systems involves making precise statements and deciding whether or not they are true.
Explanations and arguments must clearly set out and logically structured so that they can be understood by any reader with the appropriate background.
An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

In mathematics we usually consider statements which are either true or false.
We do not consider a statement is known to be true until it has been explained clearly why it is.
We call such an explanation a proof.
The module is based on a principal branch of pure mathematics: algebra, via number systems.
Investigation of number systems involves making precise statements and deciding whether or not they are true.
Explanations and arguments must clearly set out and logically structured so that they can be understood by any reader with the appropriate background.
An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

In mathematics we usually consider statements which are either true or false.
We do not consider a statement is known to be true until it has been explained clearly why it is.
We call such an explanation a proof.
The module is based on a principal branch of pure mathematics: algebra, via number systems.
Investigation of number systems involves making precise statements and deciding whether or not they are true.
Explanations and arguments must clearly set out and logically structured so that they can be understood by any reader with the appropriate background.
An important aspect of this module is to develop your ability to write clear legible mathematics: partly by reading the notes and other sources but mainly by attempting the exercises.

Set theory primer

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

A brief introduction to set theory is given in the Appendix to the notes in the booklet.

After reading this appendix you should be familiar with the standard notation for set theory and be able to answer the questions on CBA 1.

Set theory primer

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

A brief introduction to set theory is given in the Appendix to the notes in the booklet.

After reading this appendix you should be familiar with the standard notation for set theory and be able to answer the questions on CBA 1.

Set theory primer

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

A brief introduction to set theory is given in the Appendix to the notes in the booklet.

After reading this appendix you should be familiar with the standard notation for set theory and be able to answer the questions on CBA 1.

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 $\mathbb{R} \not\subset \mathbb{Q}$.

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 $\mathbb{R} \not\subset \mathbb{Q}$.

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 $\mathbb{R} \not\subset \mathbb{Q}$.

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 $\mathbb{R} \not\subset \mathbb{Q}$.

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 $\mathbb{R} \not\subset \mathbb{Q}$.

A puzzle

Move forward to a time after the collapse of the banking system when we have returned to bartering. In the university 1 loaf of bread can be exchanged for 11 apples and a chocolate cake can be exchanged for 15 apples. A professor has baked a batch of cakes and a student turns out to have a dozen loaves of bread and hundreds of apples. The professor wants just one apple, so would like to exchange some cakes for one apple and some loaves of bread. Can this be done, and if so how?

Solution

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64	65	66

Is there more than one solution?

We can describe the problem algebraically. Let a, b and c and stand for the value of an **a**pple, a **c**ake and a loaf of **b**read, respectively. Then $c = 15a$ and $b = 11a$.

To find other solutions ....

Have we found all solutions?

Solution

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64	65	66

Is there more than one solution?

We can describe the problem algebraically. Let a, b and c and stand for the value of an **a**pple, a **c**ake and a loaf of **b**read, respectively. Then $c = 15a$ and $b = 11a$.

To find other solutions ....

Have we found all solutions?

Solution

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64	65	66

Is there more than one solution?

We can describe the problem algebraically. Let a, b and c and stand for the value of an **a**pple, a **c**ake and a loaf of **b**read, respectively. Then $c = 15a$ and $b = 11a$.

To find other solutions ....

Have we found all solutions?

Solution

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64	65	66

Is there more than one solution?

We can describe the problem algebraically. Let a, b and c and stand for the value of an **a**pple, a **c**ake and a loaf of **b**read, respectively. Then $c = 15a$ and $b = 11a$.

To find other solutions ....

Have we found all solutions?

Solution

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64	65	66

Is there more than one solution?

We can describe the problem algebraically. Let a, b and c and stand for the value of an **a**pple, a **c**ake and a loaf of **b**read, respectively. Then $c = 15a$ and $b = 11a$.

To find other solutions ....

Have we found all solutions?

More barterning

Now suppose that at bottle of French wine is worth 30 apples and a bottle of English wine is worth 24 apples. A lecturer has a crate of french wine and some apples and the professor now wants 6 apples, but only has a crate of English wine. Can a fair transaction be made so that the prof ends up with 6 apples?

We can describe the problem algebraically again. Let f and e stand for the values of **F**rench and **E**nglish wine, respectively. Solve to find whole numbers x and y which are both positive.

Equations with integer solutions

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6).Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6).

e.g. Set $x = 1$ in the second problem and then take $y = 3/5$.

On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.6).

This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the bartering ones above.We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

Equations with integer solutions

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6).Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6).

e.g. Set $x = 1$ in the second problem and then take $y = 3/5$.

On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.6).

This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the bartering ones above.We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

Equations with integer solutions

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6).Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6).

e.g. Set $x = 1$ in the second problem and then take $y = 3/5$.

On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.6).

This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the bartering ones above.We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

Equations with integer solutions

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6).Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6).
e.g. Set $x = 1$ in the second problem and then take $y = 3/5$.
On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.6).
This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the bartering ones above.We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

Equations with integer solutions

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6).Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6).
e.g. Set $x = 1$ in the second problem and then take $y = 3/5$.
On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.6).
This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the bartering ones above.We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

Equations with integer solutions

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6).Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6).
e.g. Set $x = 1$ in the second problem and then take $y = 3/5$.
On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.6).
This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the bartering ones above.We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

Equations with integer solutions

The crucial feature of these problems is that we are only interested in solutions which are natural numbers (defined in Section A.6).Solutions would be very easy to find if we allowed ourselves to use rational numbers or real numbers (see Section A.6).
e.g. Set $x = 1$ in the second problem and then take $y = 3/5$.
On the other hand integer solutions are no easier to find than natural number solutions (integers are also defined in Section A.6).
This chapter looks into some of the properties of natural numbers and integers that, among other things, prove useful in solving problems such as the bartering ones above.We'll look at a a step by step recipe which would give us a number, like 6 in the second problem above, which can be used to simplify the problem and in fact determines whether or not there is a solution. We shall investigate, in some detail, how and why this works.

Greatest Common Divisors

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

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

Greatest Common Divisors

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

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

Greatest Common Divisors

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

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

Example 1.1

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.

Example 1.1

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.

Example 1.1

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.

Example 1.1

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 Euclidean 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 EA2.

The Euclidean 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 EA2.

The Euclidean 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 EA2.

The Euclidean 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 EA2.

The Euclidean 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 EA2.

The Euclidean 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 EA2.

Example 1.2

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

Example 1.3

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:

$$(2600, 2028) \tag{1.1}$$

$$2600 = 2028 \cdot 1 + 572 \tag{1.2}$$

(1.3)

(1.4)

(1.5)

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.3

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:

$$(2600, 2028) \tag{1.1}$$

$$2600 = 2028 \cdot 1 + 572 \tag{1.2}$$

(1.3)

(1.4)

(1.5)

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.3

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:

$$(2600, 2028) \qquad 2600 = 2028 \cdot 1 + 572 \tag{1.1}$$

$$(2028, 572) \qquad 2028 = 572 \cdot 3 + 312 \tag{1.2}$$

$$\tag{1.3}$$

$$\tag{1.4}$$

$$\tag{1.5}$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.3

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:

$$
\begin{aligned}
(2600, 2028) \qquad & 2600 = 2028 \cdot 1 + 572 && (1.1)\\
(2028, 572) \qquad & 2028 = 572 \cdot 3 + 312 && (1.2)\\
(572, 312) \qquad & 572 = 312 \cdot 1 + 260 && (1.3)\\
& && (1.4)\\
& && (1.5)
\end{aligned}
$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.3

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:

$$
\begin{aligned}
(2600, 2028) \qquad & 2600 = 2028 \cdot 1 + 572 && (1.1)\\
(2028, 572) \qquad & 2028 = 572 \cdot 3 + 312 && (1.2)\\
(572, 312) \qquad & 572 = 312 \cdot 1 + 260 && (1.3)\\
(312, 260) \qquad & 312 = 260 \cdot 1 + 52 && (1.4)\\
& && (1.5)
\end{aligned}
$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.3

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:

$$
\begin{aligned}
(2600,2028) \quad & 2600 = 2028 \cdot 1 + 572 && (1.1)\\
(2028,572) \quad & 2028 = 572 \cdot 3 + 312 && (1.2)\\
(572,312) \quad & 572 = 312 \cdot 1 + 260 && (1.3)\\
(312,260) \quad & 312 = 260 \cdot 1 + 52 && (1.4)\\
(260,52) \quad & 260 = 52 \cdot 5 + 0. && (1.5)
\end{aligned}
$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.3

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:

$$
\begin{aligned}
(2600,2028) \quad & 2600 = 2028 \cdot 1 + 572 && (1.1)\\
(2028,572) \quad & 2028 = 572 \cdot 3 + 312 && (1.2)\\
(572,312) \quad & 572 = 312 \cdot 1 + 260 && (1.3)\\
(312,260) \quad & 312 = 260 \cdot 1 + 52 && (1.4)\\
(260,52) \quad & 260 = 52 \cdot 5 + 0. && (1.5)
\end{aligned}
$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.3

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:

$$
\begin{aligned}
(2600,2028) \quad & 2600 = 2028 \cdot 1 + 572 && (1.1)\\
(2028,572) \quad & 2028 = 572 \cdot 3 + 312 && (1.2)\\
(572,312) \quad & 572 = 312 \cdot 1 + 260 && (1.3)\\
(312,260) \quad & 312 = 260 \cdot 1 + 52 && (1.4)\\
(260,52) \quad & 260 = 52 \cdot 5 + 0. && (1.5)
\end{aligned}
$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1).

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

Example 1.3

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:

$$
\begin{aligned}
&(2600,2028) && 2600 = 2028 \cdot 1 + 572 && (1.1)\\
&(2028,572) && 2028 = 572 \cdot 3 + 312 && (1.2)\\
&(572,312) && 572 = 312 \cdot 1 + 260 && (1.3)\\
&(312,260) && 312 = 260 \cdot 1 + 52 && (1.4)\\
&(260,52) && 260 = 52 \cdot 5 + 0. && (1.5)
\end{aligned}
$$

This gives $\gcd(2600, 2028) = 52$, as we found in Example 1.1.

To find the integers x, y we work back from (1.4) to (1.1). Thus $52 = 2600 \cdot (-7) + 2028 \cdot 9$ so we may take $x = -7$ and $y = 9$.

Example 1.4

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

$$(2028, 626) \qquad 2028 = 626 \cdot 3 + 150 \tag{1.6}$$

(1.7)

(1.8)

(1.9)

(1.10)

(1.11)

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

Example 1.4

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

$$(2028, 626) \qquad 2028 = 626 \cdot 3 + 150 \tag{1.6}$$

(1.7)

(1.8)

(1.9)

(1.10)

(1.11)

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

Example 1.4

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

$$(2028, 626) \qquad 2028 = 626 \cdot 3 + 150 \tag{1.6}$$

$$(626, 150) \qquad 626 = 150 \cdot 4 + 26 \tag{1.7}$$

$$\tag{1.8}$$

$$\tag{1.9}$$

$$\tag{1.10}$$

$$\tag{1.11}$$

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

Example 1.4

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

$$
\begin{aligned}
(2028, 626) \quad & 2028 = 626 \cdot 3 + 150 && (1.6)\\
(626, 150) \quad & 626 = 150 \cdot 4 + 26 && (1.7)\\
(150, 26) \quad & 150 = 26 \cdot 5 + 20 && (1.8)\\
& && (1.9)\\
& && (1.10)\\
& && (1.11)
\end{aligned}
$$

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

Example 1.4

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

$$
\begin{aligned}
(2028, 626) \quad & 2028 = 626 \cdot 3 + 150 && (1.6)\\
(626, 150) \quad & 626 = 150 \cdot 4 + 26 && (1.7)\\
(150, 26) \quad & 150 = 26 \cdot 5 + 20 && (1.8)\\
(26, 20) \quad & 26 = 20 \cdot 1 + 6 && (1.9)\\
& && (1.10)\\
& && (1.11)
\end{aligned}
$$

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

Example 1.4

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

$$
\begin{aligned}
(2028, 626) \quad & 2028 = 626 \cdot 3 + 150 && (1.6)\\
(626, 150) \quad & 626 = 150 \cdot 4 + 26 && (1.7)\\
(150, 26) \quad & 150 = 26 \cdot 5 + 20 && (1.8)\\
(26, 20) \quad & 26 = 20 \cdot 1 + 6 && (1.9)\\
(20, 6) \quad & 20 = 6 \cdot 3 + 2 && (1.10)\\
& && (1.11)
\end{aligned}
$$

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

Example 1.4

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

$$
\begin{aligned}
(2028,626) \quad & 2028 = 626 \cdot 3 + 150 && (1.6)\\
(626,150) \quad & 626 = 150 \cdot 4 + 26 && (1.7)\\
(150,26) \quad & 150 = 26 \cdot 5 + 20 && (1.8)\\
(26,20) \quad & 26 = 20 \cdot 1 + 6 && (1.9)\\
(20,6) \quad & 20 = 6 \cdot 3 + 2 && (1.10)\\
(6,2) \quad & 6 = 2 \cdot 3 + 0. && (1.11)
\end{aligned}
$$

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

Example 1.4

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

$$
\begin{aligned}
(2028,626) \quad & 2028 = 626 \cdot 3 + 150 && (1.6)\\
(626,150) \quad & 626 = 150 \cdot 4 + 26 && (1.7)\\
(150,26) \quad & 150 = 26 \cdot 5 + 20 && (1.8)\\
(26,20) \quad & 26 = 20 \cdot 1 + 6 && (1.9)\\
(20,6) \quad & 20 = 6 \cdot 3 + 2 && (1.10)\\
(6,2) \quad & 6 = 2 \cdot 3 + 0. && (1.11)
\end{aligned}
$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$2 = 20 \cdot 1 - 6 \cdot 3 \qquad \text{from (1.10)}$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$2 = 20 \cdot 1 - 6 \cdot 3 \qquad \text{from (1.10)}$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$\begin{aligned} 2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (1.10)} \\ &= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (1.9)} \end{aligned}$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (1.10)} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (1.9)} \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (1.8)}
\end{aligned}
$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (1.10)} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (1.9)} \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (1.8)} \\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from (1.7)}
\end{aligned}
$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (1.10)} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (1.9)} \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (1.8)} \\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from (1.7)} \\
&= (2028 - 626 \cdot 3) \cdot 96 - 626 \cdot 23 = 2028 \cdot 96 - 626 \cdot 311 && \text{from (1.6).}
\end{aligned}
$$

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

To find the integers x, y we work back from (1.10) to (1.6) to find an expression for 2.

$$
\begin{aligned}
2 &= 20 \cdot 1 - 6 \cdot 3 && \text{from (1.10)} \\
&= 20 \cdot 1 - 3 \cdot (26 \cdot 1 - 20 \cdot 1) = 20 \cdot 4 - 26 \cdot 3 && \text{from (1.9)} \\
&= (150 \cdot 1 - 26 \cdot 5) \cdot 4 - 26 \cdot 3 = 150 \cdot 4 - 26 \cdot 23 && \text{from (1.8)} \\
&= 150 \cdot 4 - (626 - 150 \cdot 4) \cdot 23 = 150 \cdot 96 - 626 \cdot 23 && \text{from (1.7)} \\
&= (2028 - 626 \cdot 3) \cdot 96 - 626 \cdot 23 = 2028 \cdot 96 - 626 \cdot 311 && \text{from (1.6).}
\end{aligned}
$$

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

Integer arithmetic

Laws of integer arithmetic (not examinable).

Let x, y and z be integers.

1. $x + 0 = x = 0 + x$.
2. For every integer n there is an integer $-n$ such that $n + (-n) = 0$.
3. $(x + y) + z = x + (y + z)$.
4. $x + y = y + x$.
5. $x \cdot 1 = x = 1 \cdot x$.
6. $(xy)z = x(yz)$.
7. $xy = yx$.
8. $(x + y)z = xz + yz$.

Subtracting n from x is the same as adding $-n$ to x: so subtraction is a convenient operation but is not essential.

Integer arithmetic

Laws of integer arithmetic (not examinable).

Let x, y and z be integers.

1. $x + 0 = x = 0 + x$.
2. For every integer n there is an integer $-n$ such that $n + (-n) = 0$.
3. $(x + y) + z = x + (y + z)$.
4. $x + y = y + x$.
5. $x \cdot 1 = x = 1 \cdot x$.
6. $(xy)z = x(yz)$.
7. $xy = yx$.
8. $(x + y)z = xz + yz$.

Subtracting n from x is the same as adding $-n$ to x: so subtraction is a convenient operation but is not essential.

Integer arithmetic: order

The integers are **ordered** by a relation denoted $\leq$ which respects addition and multiplication: that is the following laws hold.

1. If $a \leq b$ and $c \leq d$ then $a + c \leq b + d$;
2. If $a \leq b$ and $0 < c$ then $ac \leq bc$.

Here "$a < b$" is shorthand for "$a \leq b$ and $a \neq b$".

Integer arithmetic: consequences

In fact all these laws apply to arithmetic with rational and real numbersas well as integers. From these basic laws we can derive all the other familiar properties of arithmetic such as (for integers x, y and z)

$$x + z = y + z \Leftrightarrow x = y.$$

$$x + y = 0 \Leftrightarrow x = -y.$$

$$x(y + z) = xy + xz.$$

$$(-x)y = x(-y) = -(xy).$$

$$(-x)(-y) = xy.$$

$$x \cdot 0 = 0.$$

$$\text{if } x > 0 \text{ and } y > 0 \text{ then } xy > 0.$$

$$\text{if } x > 0 \text{ and } y < 0 \text{ then } xy < 0.$$

(Again these are **not examinable**.)

Integer arithmetic: consequences

In fact all these laws apply to arithmetic with rational and real numbersas well as integers. From these basic laws we can derive all the other familiar properties of arithmetic such as (for integers x, y and z)

$$x + z = y + z \Leftrightarrow x = y.$$

$$x + y = 0 \Leftrightarrow x = -y.$$

$$x(y + z) = xy + xz.$$

$$(-x)y = x(-y) = -(xy).$$

$$(-x)(-y) = xy.$$

$$x \cdot 0 = 0.$$

$$\text{if } x > 0 \text{ and } y > 0 \text{ then } xy > 0.$$

$$\text{if } x > 0 \text{ and } y < 0 \text{ then } xy < 0.$$

(Again these are **not examinable**.)

Integer arithmetic: consequences

In fact all these laws apply to arithmetic with rational and real numbersas well as integers. From these basic laws we can derive all the other familiar properties of arithmetic such as (for integers x, y and z)

$$x + z = y + z \Leftrightarrow x = y.$$

$$x + y = 0 \Leftrightarrow x = -y.$$

$$x(y + z) = xy + xz.$$

$$(-x)y = x(-y) = -(xy).$$

$$(-x)(-y) = xy.$$

$$x \cdot 0 = 0.$$

$$\text{if } x > 0 \text{ and } y > 0 \text{ then } xy > 0.$$

$$\text{if } x > 0 \text{ and } y < 0 \text{ then } xy < 0.$$

(Again these are **not examinable**.)

If and only if

The notation $\Leftrightarrow$ above is shorthand for the phrase “if and only if”.

If and only if

The notation $\Leftrightarrow$ above is shorthand for the phrase “if and only if”.

To say “$x + z = y + z$ if and only if $x = y$” means two things:

If and only if

The notation $\Leftrightarrow$ above is shorthand for the phrase “if and only if”.

To say “$x + z = y + z$ if and only if $x = y$” means two things:

1. if $x + z = y + z$ then $x = y$ and
2.

If and only if

The notation $\Leftrightarrow$ above is shorthand for the phrase "if and only if".

To say "$x + z = y + z$ if and only if $x = y$" means two things:

1. if $x + z = y + z$ then $x = y$ and
2. if $x = y$ then $x + z = y + z$.

If and only if

The notation $\Leftrightarrow$ above is shorthand for the phrase "if and only if".

To say "$x + z = y + z$ if and only if $x = y$" means two things:

1. if $x + z = y + z$ then $x = y$ and
2. if $x = y$ then $x + z = y + z$.

The second statement is the converse of the first.

Frog people

More generally, the converse of
“If A is true then B is true” is
“If B is true then A is true”.

Frog people

More generally, the converse of
“If A is true then B is true” is
“If B is true then A is true”.
It is possible that a true statement has a converse which is false.
This is apparent in everyday life.

Frog people

More generally, the converse of
“If A is true then B is true” is
“If B is true then A is true”.
It is possible that a true statement has a converse which is false.
This is apparent in everyday life.
The statement “If I am a frog then I can swim” can be regarded as true.

Frog people

More generally, the converse of
“If A is true then B is true” is
“If B is true then A is true”.
It is possible that a true statement has a converse which is false.
This is apparent in everyday life.
The statement “If I am a frog then I can swim” can be regarded as true.
The converse is “If I can swim then I am a frog”, and this is commonly regarded as false.

Frog people

More generally, the converse of
“If A is true then B is true” is
“If B is true then A is true”.
It is possible that a true statement has a converse which is false.
This is apparent in everyday life.
The statement “If I am a frog then I can swim” can be regarded as true.
The converse is “If I can swim then I am a frog”, and this is commonly regarded as false.
Mathematical examples are easy to find.

Synonyms

There are several different ways of saying things like “if ... then ...” and “... if and only if ...”.

Synonyms

There are several different ways of saying things like "if ... then ..." and "... if and only if ...".

The symbol $\Rightarrow$ is read "implies". All the entries on a given line of the following table mean the same thing: entries on different lines do not mean the same thing.

Synonyms

There are several different ways of saying things like “if ... then ...” and “... if and only if ...”.

The symbol $\Rightarrow$ is read “implies”. All the entries on a given line of the following table mean the same thing: entries on different lines do not mean the same thing.

if A then B	$A \Rightarrow B$	B if A

Synonyms

There are several different ways of saying things like "if ... then ..." and "... if and only if ...".

The symbol $\Rightarrow$ is read "implies". All the entries on a given line of the following table mean the same thing: entries on different lines do not mean the same thing.

if A then B	$A \Rightarrow B$	B if A
if B then A	$A \Leftarrow B$	A if B

Synonyms

There are several different ways of saying things like “if ... then ...” and “... if and only if ...”.

The symbol $\Rightarrow$ is read “implies”. All the entries on a given line of the following table mean the same thing: entries on different lines do not 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

What makes integer arithmetic different from arithmetic with real or rational numbers?

First a definition.

Definition 1.5

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

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "modulus" we mean what it says above, nothing more, nothing less.

The definition of modulus above is what is known as a definition by cases.

What makes integer arithmetic different from arithmetic with real or rational numbers?
First a definition.

Definition 1.5

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

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "modulus" we mean what it says above, nothing more, nothing less.

The definition of modulus above is what is known as a definition by cases.

What makes integer arithmetic different from arithmetic with real or rational numbers?
First a definition.

Definition 1.5

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

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "modulus" we mean what it says above, nothing more, nothing less.

The definition of modulus above is what is known as a definition by cases.

What makes integer arithmetic different from arithmetic with real or rational numbers?
First a definition.

Definition 1.5

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

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

A definition establishes once and for all the meaning of a word. From now on whenever we say “modulus” we mean what it says above, nothing more, nothing less.

The definition of modulus above is what is known as a definition by cases.

What makes integer arithmetic different from arithmetic with real or rational numbers?
First a definition.

Definition 1.5

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

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "modulus" we mean what it says above, nothing more, nothing less.

The definition of modulus above is what is known as a definition by cases.

From the definition:

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

Theorem 1.6 (**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. It's the same as saying that we can't have fractions like $3/0$ ...

(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.
For example if we have q and r with $0 \leq r < 32$ such that $121 = 32q + r$ then q **must** be 3 and r **must** be 25.
This is not surprising if you believe in fractions: ...

(3) Does the Theorem work in other settings?

Theorem 1.6 (**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. It's the same as saying that we can't have fractions like $3/0$ ...

(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.
For example if we have q and r with $0 \leq r < 32$ such that $121 = 32q + r$ then q **must** be 3 and r **must** be 25.
This is not surprising if you believe in fractions: ...

(3) Does the Theorem work in other settings?

Theorem 1.6 (**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. It's the same as saying that we can't have fractions like $3/0$ ...

(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.

For example if we have q and r with $0 \leq r < 32$ such that $121 = 32q + r$ then q **must** be 3 and r **must** be 25.
This is not surprising if you believe in fractions: ...

(3) Does the Theorem work in other settings?

Theorem 1.6 (**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. It's the same as saying that we can't have fractions like $3/0$ ...

(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.
For example if we have q and r with $0 \leq r < 32$ such that $121 = 32q + r$ then q **must** be 3 and r **must** be 25.
This is not surprising if you believe in fractions: ...

(3) Does the Theorem work in other settings?

Theorem 1.6 (**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. It's the same as saying that we can't have fractions like $3/0$ ...

(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.
For example if we have q and r with $0 \leq r < 32$ such that $121 = 32q + r$ then q **must** be 3 and r **must** be 25.
This is not surprising if you believe in fractions: ...

(3) Does the Theorem work in other settings?

Theorem 1.6 (**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. It's the same as saying that we can't have fractions like $3/0$ ...

(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.
For example if we have q and r with $0 \leq r < 32$ such that $121 = 32q + r$ then q **must** be 3 and r **must** be 25.
This is not surprising if you believe in fractions: ...

(3) Does the Theorem work in other settings?

Suppose for example we were to work with rational numbers instead of integers.

If b and a are rational with $a > 0$ then I can pick any r I like, in the given range $0 \leq r < |a|$, and obtain $b = aq + r$ by setting $q = (b - r)/a$. For example ...

Thus q and r are not unique and the Division Algorithm does not hold.

More dramatic failure of the Division Algorithm is exhibited in some other situations. For example in the set of polynomials in two variables x and y with integer coefficients it's easy to find polynomials f and g for which there is no way of writing $f = g \cdot q + r$ with r in any meaningful way "less than" g.

Suppose for example we were to work with rational numbers instead of integers.
If b and a are rational with $a > 0$ then I can pick any r I like, in the given range $0 \leq r < |a|$, and obtain $b = aq + r$ by setting $q = (b - r)/a$. For example ...
Thus q and r are not unique and the Division Algorithm does not hold.
More dramatic failure of the Division Algorithm is exhibited in some other situations. For example in the set of polynomials in two variables x and y with integer coefficients it's easy to find polynomials f and g for which there is no way of writing $f = g \cdot q + r$ with r in any meaningful way "less than" g.

Suppose for example we were to work with rational numbers instead of integers.
If b and a are rational with $a > 0$ then I can pick any r I like, in the given range $0 \leq r < |a|$, and obtain $b = aq + r$ by setting $q = (b - r)/a$. For example ...
Thus q and r are not unique and the Division Algorithm does not hold.
More dramatic failure of the Division Algorithm is exhibited in some other situations. For example in the set of polynomials in two variables x and y with integer coefficients it's easy to find polynomials f and g for which there is no way of writing $f = g \cdot q + r$ with r in any meaningful way "less than" g.

Suppose for example we were to work with rational numbers instead of integers.
If b and a are rational with $a > 0$ then I can pick any r I like, in the given range $0 \leq r < |a|$, and obtain $b = aq + r$ by setting $q = (b - r)/a$. For example ...
Thus q and r are not unique and the Division Algorithm does not hold.
More dramatic failure of the Division Algorithm is exhibited in some other situations. For example in the set of polynomials in two variables x and y with integer coefficients it's easy to find polynomials f and g for which there is no way of writing $f = g \cdot q + r$ with r in any meaningful way "less than" g.

Divisibility in the integers

Definition 1.7

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "divides" we mean what it says above, nothing more, nothing less.

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".

Divisibility in the integers

Definition 1.7

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "divides" we mean what it says above, nothing more, nothing less.

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".

Divisibility in the integers

Definition 1.7

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "divides" we mean what it says above, nothing more, nothing less.

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".

Divisibility in the integers

Definition 1.7

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

A definition establishes once and for all the meaning of a word. From now on whenever we say "divides" we mean what it says above, nothing more, nothing less.

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 1.8

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.

Also it's "obvious" $7 \nmid 18$ and $-11 \nmid 32$: but these are not immediate consequences of the definition of division.
If If $7|18$ then ...

Example 1.8

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.

Also it's "obvious" $7 \nmid 18$ and $-11 \nmid 32$: but these are not immediate consequences of the definition of division.
If If $7|18$ then ...

Example 1.8

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.

Also it's "obvious" $7 \nmid 18$ and $-11 \nmid 32$: but these are not immediate consequences of the definition of division.

If If $7|18$ then ...

Example 1.8

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.

Also it's "obvious" $7 \nmid 18$ and $-11 \nmid 32$: but these are not immediate consequences of the definition of division.
If If $7|18$ then ...

Notation.

The expression "$3|6$" means that there is an integer q such that $6 = 3q$.

Notation.

The expression "$3|6$" means that there is an integer q such that $6 = 3q$.

The expression "$3/6$" denotes a rational number.

Notation.

The expression "$3|6$" means that there is an integer q such that $6 = 3q$.

The expression "$3/6$" denotes a rational number.

Another way of saying $a|b$ would be to say "b/a is an integer, or $a = b = 0$", but this is more complicated in at least two ways.

Notation.

The expression "$3|6$" means that there is an integer q such that $6 = 3q$.

The expression "$3/6$" denotes a rational number.

Another way of saying $a|b$ would be to say "b/a is an integer, or $a = b = 0$", but this is more complicated in at least two ways.

Take care not to confuse $a|b$ with a/b or b/a.

Example 1.9

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

In Example 1.9 we have proved something is true for all integers.

Example 1.10

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

Example 1.9

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

In Example 1.9 we have proved something is true for all integers.

Example 1.10

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

Example 1.9

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

In Example 1.9 we have proved something is true for all integers.

To prove this it is **not** enough to find an example of some integer n for which the statement is true.

Example 1.10

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

Example 1.9

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

In Example 1.9 we have proved something is true for all integers.

To prove this it is **not** enough to find an example of some integer n for which the statement is true.

On the other hand if you are asked to prove that there exist integers x and y such that $2600x + 2028y = 52$ then it would be enough to find an example: say $x = -7$ and $y = 9$, as in Example 1.3.

Example 1.10

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

Example 1.9

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

In Example 1.9 we have proved something is true for all integers.

To prove this it is **not** enough to find an example of some integer n for which the statement is true.

On the other hand if you are asked to prove that there exist integers x and y such that $2600x + 2028y = 52$ then it would be enough to find an example: say $x = -7$ and $y = 9$, as in Example 1.3.

Example 1.10

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

Example 1.11

From the Division Algorithm, 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 1.6) to partition of integers into odd and even.

Example 1.12

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 1.11

From the Division Algorithm, 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 1.6) to partition of integers into odd and even.

Example 1.12

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 1.11

From the Division Algorithm, 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 1.6) to partition of integers into odd and even.

Example 1.12

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 1.11

From the Division Algorithm, 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 1.6) to partition of integers into odd and even.

Example 1.12

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 1.13

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

Example 1.14

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

Example 1.13

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

Example 1.14

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

Common Divisors

Definition 1.15

Let a and b be integers. An integer c such that $c|a$ and $c|b$ is called a **common divisor** of a and b.

Definition 1.16

Let a and b be integers, not both 0. The **greatest common divisor** of a and b is the integer d such that

1. $d|a$ and $d|b$ and
2. if c is any common divisor of a and b then $d \geq c$.

We write $\gcd(a,b)$ for the greatest common divisor of a and b.

Common Divisors

Definition 1.15

Let a and b be integers. An integer c such that $c|a$ and $c|b$ is called a **common divisor** of a and b.

Definition 1.16

Let a and b be integers, not both 0. The **greatest common divisor** of a and b is the integer d such that

1. $d|a$ and $d|b$ and
2. if c is any common divisor of a and b then $d \geq c$.

We write $\gcd(a,b)$ for the greatest common divisor of a and b.

Example 1.17

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

Why are the gcd's are both the same?

Lemma 1.18

Let s, t and u be integers, which are not all zero, such that

$$s = tq + u,$$

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

> A lemma is a lesser result: not important enough to be given the grand title of theorem. Lemmas are often small steps made on the way to establishing a theorem.

Example 1.17

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

Why are the gcd's are both the same?

Lemma 1.18

Let s, t and u be integers, which are not all zero, such that

$$s = tq + u,$$

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

> A lemma is a lesser result: not important enough to be given the grand title of theorem. Lemmas are often small steps made on the way to establishing a theorem.

Example 1.17

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

Why are the gcd's are both the same?

Lemma 1.18

Let s, t and u be integers, which are not all zero, such that

$$s = tq + u,$$

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

A lemma is a lesser result: not important enough to be given the grand title of theorem. Lemmas are often small steps made on the way to establishing a theorem.

Example 1.17

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

Why are the gcd's are both the same?

Lemma 1.18

Let s, t and u be integers, which are not all zero, such that

$$s = tq + u,$$

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

A lemma is a lesser result: not important enough to be given the grand title of theorem. Lemmas are often small steps made on the way to establishing a theorem.

Strategy of the proof

Strategy:

Step(1) Show that if c is a common divisor or s and t then c is a common divisor of t and u.

Step(2) Show that if c' is a common divisor or t and u then c' is a common divisor of s and t.

Step(3) From Steps (1) and (2) it's clear that 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 common divisors are thus equal.

Another way of putting this is to write $d = \gcd(s,t)$ and $d' = \gcd(t,u)$

and then say that Step(1) shows that d is a common divisor of t and u so $d \leq d'$.

Moreover Step(2) shows that d' is a common divisor of s and t, so $d' \leq d$. As $d \leq d'$ and $d' \leq d$ we have $d = d'$.

Strategy of the proof

Strategy:

Step(1) Show that if c is a common divisor or s and t then c is a common divisor of t and u.

Step(2) Show that if c' is a common divisor or t and u then c' is a common divisor of s and t.

Step(3) From Steps (1) and (2) it's clear that 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 common divisors are thus equal.

Another way of putting this is to write $d = \gcd(s,t)$ and $d' = \gcd(t,u)$

and then say that Step(1) shows that d is a common divisor of t and u so $d \leq d'$.

Moreover Step(2) shows that d' is a common divisor of s and t, so $d' \leq d$. As $d \leq d'$ and $d' \leq d$ we have $d = d'$.

Strategy of the proof

Strategy:

Step(1) Show that if c is a common divisor or s and t then c is a common divisor of t and u.

Step(2) Show that if c' is a common divisor or t and u then c' is a common divisor of s and t.

Step(3) From Steps (1) and (2) it's clear that 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 common divisors are thus equal.

Another way of putting this is to write $d = \gcd(s,t)$ and $d' = \gcd(t,u)$

and then say that Step(1) shows that d is a common divisor of t and u so $d \leq d'$.

Moreover Step(2) shows that d' is a common divisor of s and t, so $d' \leq d$. As $d \leq d'$ and $d' \leq d$ we have $d = d'$.

Strategy of the proof

Strategy:

Step(1) Show that if c is a common divisor or s and t then c is a common divisor of t and u.

Step(2) Show that if c' is a common divisor or t and u then c' is a common divisor of s and t.

Step(3) From Steps (1) and (2) it's clear that 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 common divisors are thus equal.

Another way of putting this is to write $d = \gcd(s,t)$ and $d' = \gcd(t,u)$

and then say that Step(1) shows that d is a common divisor of t and u so $d \leq d'$.

Moreover Step(2) shows that d' is a common divisor of s and t, so $d' \leq d$. As $d \leq d'$ and $d' \leq d$ we have $d = d'$.

Strategy of the proof

Strategy:

Step(1) Show that if c is a common divisor or s and t then c is a common divisor of t and u.

Step(2) Show that if c' is a common divisor or t and u then c' is a common divisor of s and t.

Step(3) From Steps (1) and (2) it's clear that 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 common divisors are thus equal.

Another way of putting this is to write $d = \gcd(s,t)$ and $d' = \gcd(t,u)$

and then say that Step(1) shows that d is a common divisor of t and u so $d \leq d'$.

Moreover Step(2) shows that d' is a common divisor of s and t, so $d' \leq d$. As $d \leq d'$ and $d' \leq d$ we have $d = d'$.

Strategy of the proof

Strategy:

Step(1) Show that if c is a common divisor or s and t then c is a common divisor of t and u.

Step(2) Show that if c' is a common divisor or t and u then c' is a common divisor of s and t.

Step(3) From Steps (1) and (2) it's clear that 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 common divisors are thus equal.

Another way of putting this is to write $d = \gcd(s,t)$ and $d' = \gcd(t,u)$

and then say that Step(1) shows that d is a common divisor of t and u so $d \leq d'$.

Moreover Step(2) shows that d' is a common divisor of s and t, so $d' \leq d$. As $d \leq d'$ and $d' \leq d$ we have $d = d'$.

Example 1.19

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

Lemma 1.20

1. $n|n$, *for all integers* n.
2. $n|0$, *for all integers* n.
3. *If* m *and* n *are integers,* $m|n$ *and* $n > 0$ *then* $m \leq n$.
4. *If* m *and* n *are positive integers and* $m|n$ *then* $\gcd(m,n) = m$.

Example 1.19

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

Lemma 1.20

1. $n|n$, *for all integers* n.
2. $n|0$, *for all integers* n.
3. *If* m *and* n *are integers,* $m|n$ *and* $n > 0$ *then* $m \leq n$.
4. *If* m *and* n *are positive integers and* $m|n$ *then* $\gcd(m,n) = m$.

Example 1.19

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

Lemma 1.20

1. $n|n$, *for all integers* n.
2. $n|0$, *for all integers* n.
3. *If* m *and* n *are integers,* $m|n$ *and* $n > 0$ *then* $m \leq n$.
4. *If* m *and* n *are positive integers and* $m|n$ *then* $\gcd(m,n) = m$.

Example 1.19

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

Lemma 1.20

1. $n|n$, *for all integers* n.
2. $n|0$, *for all integers* n.
3. *If* m *and* n *are integers,* $m|n$ *and* $n > 0$ *then* $m \leq n$.
4. *If* m *and* n *are positive integers and* $m|n$ *then* $\gcd(m,n) = m$.

Example 1.19

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

Lemma 1.20

1. $n|n$, *for all integers* n.
2. $n|0$, *for all integers* n.
3. *If* m *and* n *are integers,* $m|n$ *and* $n > 0$ *then* $m \leq n$.
4. *If* m *and* n *are positive integers and* $m|n$ *then* $\gcd(m,n) = m$.

Proof by Contradiction

The proof of the last part of the Lemma above is known as proof by contradiction. This always works as follows.

Proof by Contradiction

The proof of the last part of the Lemma above is known as proof by contradiction. This always works as follows.

Step(1) **Start with some statement to be proved.** In the Lemma this is "If $m|n$ and $n > 0$ then $m \leq n$."

Proof by Contradiction

The proof of the last part of the Lemma above is known as proof by contradiction. This always works as follows.

Step(1) **Start with some statement to be proved.** In the Lemma this is "If $m|n$ and $n > 0$ then $m \leq n$."

Step(2) **Assume the negation of what is to be proved.** In the Lemma this is that there exist integers m, n such that $m|n$ and $n > 0$ and $m > n$.

Proof by Contradiction

The proof of the last part of the Lemma above is known as proof by contradiction. This always works as follows.

Step(1) **Start with some statement to be proved.** In the Lemma this is "If $m|n$ and $n > 0$ then $m \leq n$."

Step(2) **Assume the negation of what is to be proved.** In the Lemma this is that there exist integers m, n such that $m|n$ and $n > 0$ and $m > n$.

Step(3) **Derive some consequences of the assumption.** As a result we find that $n = mq$, with $q \geq 1$.

Proof by Contradiction

The proof of the last part of the Lemma above is known as proof by contradiction. This always works as follows.

Step(1) **Start with some statement to be proved.** In the Lemma this is "If $m|n$ and $n > 0$ then $m \leq n$."

Step(2) **Assume the negation of what is to be proved.** In the Lemma this is that there exist integers m, n such that $m|n$ and $n > 0$ and $m > n$.

Step(3) **Derive some consequences of the assumption.** As a result we find that $n = mq$, with $q \geq 1$.

Step(4) **Show that something we've derived is false.** This means that $n \geq m$, which together with $m > n$ makes $n > n$, which is impossible.

Proof by Contradiction

The proof of the last part of the Lemma above is known as proof by contradiction. This always works as follows.

Step(1) **Start with some statement to be proved.** In the Lemma this is "If $m|n$ and $n > 0$ then $m \leq n$."

Step(2) **Assume the negation of what is to be proved.** In the Lemma this is that there exist integers m, n such that $m|n$ and $n > 0$ and $m > n$.

Step(3) **Derive some consequences of the assumption.** As a result we find that $n = mq$, with $q \geq 1$.

Step(4) **Show that something we've derived is false.** This means that $n \geq m$, which together with $m > n$ makes $n > n$, which is impossible.

Step(5) **Conclude that the result holds.** It cannot happen that $m|n$ and $n > 0$ and $m > n$ because this forces $n > n$, which is impossible. The conclusion is that whenever $m|n$ and $n > 0$ then $m \leq n$.

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

Stringing all these facts together we have

$$2 = \gcd(6, 2)$$

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

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

Stringing all these facts together we have

$$2 = \gcd(6, 2)$$

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

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

Stringing all these facts together we have

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

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

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

Stringing all these facts together we have

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

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

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

Stringing all these facts together we have

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

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

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

Stringing all these facts together we have

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

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

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

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

Why the Euclidean Algorithm works

Example 1.21

Consider the Equations (1.6)–(1.11).

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 1.22

Consider the Equations (1.1)–(1.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{using Equation (1.1)}$$

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

Example 1.22

Consider the Equations (1.1)–(1.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{using Equation (1.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{using Equation (1.2)}$$

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

Example 1.22

Consider the Equations (1.1)–(1.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{using Equation (1.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{using Equation (1.2)}$$
$$\gcd(572, 312) = \gcd(312, 260), \text{using Equation (1.3)}$$

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

Example 1.22

Consider the Equations (1.1)–(1.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{using Equation (1.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{using Equation (1.2)}$$
$$\gcd(572, 312) = \gcd(312, 260), \text{using Equation (1.3)}$$
$$\gcd(312, 260) = \gcd(260, 52), \text{using Equation (1.4).}$$

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

Example 1.22

Consider the Equations (1.1)–(1.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{using Equation (1.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{using Equation (1.2)}$$
$$\gcd(572, 312) = \gcd(312, 260), \text{using Equation (1.3)}$$
$$\gcd(312, 260) = \gcd(260, 52), \text{using Equation (1.4).}$$

From Equation (1.5) we see that $52|260$ so $\gcd(52, 260) = 52$.
that is $\gcd(2600, 2028) = 52$.

Example 1.22

Consider the Equations (1.1)–(1.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{using Equation (1.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{using Equation (1.2)}$$
$$\gcd(572, 312) = \gcd(312, 260), \text{using Equation (1.3)}$$
$$\gcd(312, 260) = \gcd(260, 52), \text{using Equation (1.4).}$$

From Equation (1.5) 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 $\gcd(2600, 2028) = 52$.

Example 1.22

Consider the Equations (1.1)–(1.5).

$$\gcd(2600, 2028) = \gcd(2028, 572), \text{using Equation (1.1)}$$
$$\gcd(2028, 572) = \gcd(572, 312), \text{using Equation (1.2)}$$
$$\gcd(572, 312) = \gcd(312, 260), \text{using Equation (1.3)}$$
$$\gcd(312, 260) = \gcd(260, 52), \text{using Equation (1.4).}$$

From Equation (1.5) 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 1.2, 1.3 and 1.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

Theorem 1.23

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.

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 1.2, 1.3 and 1.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

Theorem 1.23

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.

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 1.2, 1.3 and 1.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

Theorem 1.23

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.

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 1.2, 1.3 and 1.4, to find integers x and y such that $ax + by = \gcd(a, b)$.

Theorem 1.23

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

We began by looking at batering with apples, cakes and loaves. This led to finding integer solutions to equations like $1 + 11y = 15x$.

Equations of this form, where we seek integer solutions (and the coefficients are integers) are called **Diophantine equations**.

Here we shall see how to find solutions to some linear Diophantine equations.

An application

We began by looking at batering with apples, cakes and loaves. This led to finding integer solutions to equations like $1 + 11y = 15x$.

Equations of this form, where we seek integer solutions (and the coefficients are integers) are called **Diophantine equations**.

Here we shall see how to find solutions to some linear Diophantine equations.

An application

We began by looking at batering with apples, cakes and loaves. This led to finding integer solutions to equations like $1 + 11y = 15x$.
Equations of this form, where we seek integer solutions (and the coefficients are integers) are called **Diophantine equations**.
Here we shall see how to find solutions to some linear Diophantine equations.

Example 1.24

Find integers x and y such that $2600x + 2028y = 104$.

Example 1.24

Find integers x and y such that $2600x + 2028y = 104$.

In Example 1.3 we ran the Euclidean Algorithm and found $\gcd(2600, 2028) = 52$.

Example 1.24

Find integers x and y such that $2600x + 2028y = 104$.

In Example 1.3 we ran the Euclidean Algorithm and found $\gcd(2600, 2028) = 52$.

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

$$2600 \cdot (-7) + 2028 \cdot 9 = 52. \tag{1.12}$$

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$(12378, 3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{1.13}$$

$$\tag{1.14}$$

$$\tag{1.15}$$

$$\tag{1.16}$$

$$\tag{1.17}$$

$$\tag{1.18}$$

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$(12378, 3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{1.13}$$

$$\tag{1.14}$$

$$\tag{1.15}$$

$$\tag{1.16}$$

$$\tag{1.17}$$

$$\tag{1.18}$$

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$(12378, 3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{1.13}$$

(1.14)

(1.15)

(1.16)

(1.17)

(1.18)

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$(12378, 3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{1.13}$$

$$(3054, 162) \qquad 3054 = 162 \cdot 18 + 138 \tag{1.14}$$

(1.15)

(1.16)

(1.17)

(1.18)

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$(12378, 3054) \qquad 12378 = 3054 \cdot 4 + 162 \tag{1.13}$$

$$(3054, 162) \qquad 3054 = 162 \cdot 18 + 138 \tag{1.14}$$

$$(162, 138) \qquad 162 = 138 \cdot 1 + 24 \tag{1.15}$$

$$\tag{1.16}$$

$$\tag{1.17}$$

$$\tag{1.18}$$

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$
\begin{aligned}
(12378, 3054) \quad & 12378 = 3054 \cdot 4 + 162 && (1.13)\\
(3054, 162) \quad & 3054 = 162 \cdot 18 + 138 && (1.14)\\
(162, 138) \quad & 162 = 138 \cdot 1 + 24 && (1.15)\\
(138, 24) \quad & 138 = 24 \cdot 5 + 18 && (1.16)\\
& && (1.17)\\
& && (1.18)
\end{aligned}
$$

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$
\begin{aligned}
(12378, 3054) \quad & 12378 = 3054 \cdot 4 + 162 && (1.13)\\
(3054, 162) \quad & 3054 = 162 \cdot 18 + 138 && (1.14)\\
(162, 138) \quad & 162 = 138 \cdot 1 + 24 && (1.15)\\
(138, 24) \quad & 138 = 24 \cdot 5 + 18 && (1.16)\\
(24, 18) \quad & 24 = 18 \cdot 1 + 6 && (1.17)\\
& && (1.18)
\end{aligned}
$$

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$
\begin{aligned}
(12378, 3054) \quad & 12378 = 3054 \cdot 4 + 162 && (1.13)\\
(3054, 162) \quad & 3054 = 162 \cdot 18 + 138 && (1.14)\\
(162, 138) \quad & 162 = 138 \cdot 1 + 24 && (1.15)\\
(138, 24) \quad & 138 = 24 \cdot 5 + 18 && (1.16)\\
(24, 18) \quad & 24 = 18 \cdot 1 + 6 && (1.17)\\
(18, 6) \quad & 18 = 3 \cdot 6 + 0. && (1.18)
\end{aligned}
$$

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

Example 1.25

Find integers x and y such that $-72 = 12378x - 3054y$.

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

$$(12378, 3054) \qquad 12378 = 3054 \cdot 4 + 162 \qquad (1.13)$$

$$(3054, 162) \qquad 3054 = 162 \cdot 18 + 138 \qquad (1.14)$$

$$(162, 138) \qquad 162 = 138 \cdot 1 + 24 \qquad (1.15)$$

$$(138, 24) \qquad 138 = 24 \cdot 5 + 18 \qquad (1.16)$$

$$(24, 18) \qquad 24 = 18 \cdot 1 + 6 \qquad (1.17)$$

$$(18, 6) \qquad 18 = 3 \cdot 6 + 0. \qquad (1.18)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Next we work back from (1.17) to (1.13) to find integers u, v such that

$$6 = 12378u + 3054v.$$

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 && \text{from (1.17)} \\
&= 24 - (138 - 24 \cdot 5) = 24 \cdot 6 - 138 && \text{from (1.16)} \\
&= (162 - 138) \cdot 6 - 138 = 162 \cdot 6 - 138 \cdot 7 && \text{from (1.15)} \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= 162 \cdot 132 - 3054 \cdot 7 && \text{from (1.14)} \\
&= (12738 - 3054 \cdot 4) \cdot 132 - 3054 \cdot 7 \\
&= 12378 \cdot 132 - 3054 \cdot 535 && \text{from (1.13).}
\end{aligned}$$

Thus

$$6 = 12378 \cdot 132 + 3054 \cdot (-535) \qquad (1.19)$$

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

Existence of solutions

Lemma 1.26

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

$$ax + by = c \tag{1.20}$$

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

This is an example of an “if and only if” statement.

Existence of solutions

Lemma 1.26

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

$$ax + by = c \tag{1.20}$$

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

This is an example of an “if and only if” statement.

Existence of solutions

Lemma 1.26

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

$$ax + by = c \tag{1.20}$$

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

This is an example of an "if and only if" statement.

The Lemma says two things:

1. "If $ax + by = c$ has a solution then $\gcd(a, b) | c$" and
2. "If $\gcd(a, b) | c$ then the equation $ax + by = c$ has a solution."

Existence of solutions

Lemma 1.26

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

$$ax + by = c \tag{1.20}$$

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

This is an example of an "if and only if" statement.

The Lemma says two things:

1. "If $ax + by = c$ has a solution then $\gcd(a, b) | c$" and
2. "If $\gcd(a, b) | c$ then the equation $ax + by = c$ has a solution."

Both must be proved, because it can happen that a true statement has a converse which is false ("e.g. "If you are a crocodile then you have big teeth and a long tail.")

Example 1.27

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

Example 1.28

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.

Example 1.27

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

Example 1.28

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.

Example 1.27

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

Example 1.28

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.

Example 1.27

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

Example 1.28

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.

Concluding remarks

Fix integers a and b and let $d = \gcd(a,b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d|c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a,b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a, b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d \mid c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a, b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a, b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d \mid c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a, b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a,b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d|c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a,b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a,b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d|c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a,b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a, b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d \mid c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a, b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a, b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d|c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a, b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a, b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d|c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a, b)$ in this case?

Concluding remarks

Fix integers a and b and let $d = \gcd(a, b)$.

Lemma 1.26 tells us that the equation $ax + by = c$ has a solution if and only if $d|c$. So

1. there is a solution if $d = c$ and
2. there is no solution if $0 < c < d$.

Conclusion: d is the smallest positive integer that can be written in the form $ax + by$, with $x, y \in \mathbb{Z}$.

Now suppose that for our choice of a, b there exist integers u and v such that $au + bv = 1$.

e.g. take $a = 25132$ and $b = 15079$, then $3a - 5b = 1$.

What can we say about $\gcd(a, b)$ in this case?

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 1.7 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) understand the strategy of the proof of Lemma 1.18 and be able to apply it to other situations;

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

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

More Apples and Wine

The professor has been awarded a pay increase and decides to throw a party. He wants French wine for this party. Unfortunately in this department the pay is in bottles of English wine. Lecturers in Classics are paid in French wine and apples; so the professor wishes to trade English wine for apples and French wine.

The prof still wants to eat six apples, as it happens.

Can the professor buy sufficient wine to make a really memorable party?

More Apples and Wine

The professor has been awarded a pay increase and decides to throw a party. He wants French wine for this party. Unfortunately in this department the pay is in bottles of English wine. Lecturers in Classics are paid in French wine and apples; so the professor wishes to trade English wine for apples and French wine.

The prof still wants to eat six apples, as it happens.

Can the professor buy sufficient wine to make a really memorable party?

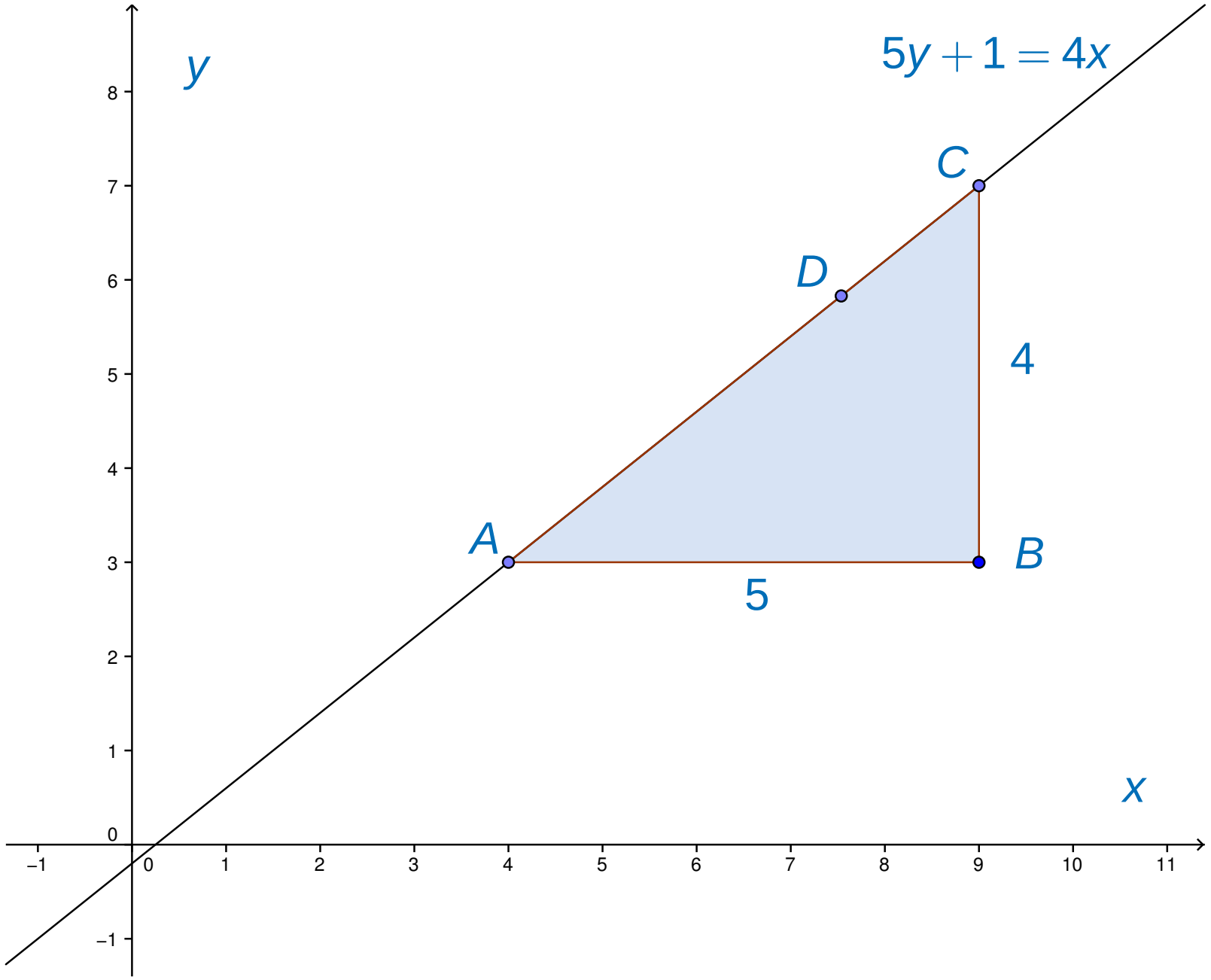
More Apples and Wine

The professor has been awarded a pay increase and decides to throw a party. He wants French wine for this party. Unfortunately in this department the pay is in bottles of English wine. Lecturers in Classics are paid in French wine and apples; so the professor wishes to trade English wine for apples and French wine.

The prof still wants to eat six apples, as it happens.

Can the professor buy sufficient wine to make a really memorable party?

Solutions to a bartering problem



Section overview

In this section we'll develop enough of the theory of integers to enable us to write down a formula which tells us exactly which values of x and y are solutions to equations of this type for which we seek integer solutions (linear Diophantine equations). The main new idea we need is that of pairs of "coprime" numbers.

Section overview

In this section we'll develop enough of the theory of integers to enable us to write down a formula which tells us exactly which values of x and y are solutions to equations of this type for which we seek integer solutions (linear Diophantine equations). The main new idea we need is that of pairs of "coprime" numbers.

Greatest common divisors again

The Euclidean Algorithm, run on natural numbers a and b, gives not only $\gcd(a,b)$ but also integers u and v such that

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

This gave us Theorem 1.23:

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

The Euclidean Algorithm, run on natural numbers a and b, gives not only $\gcd(a,b)$ but also integers u and v such that

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

This gave us Theorem 1.23:

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

The Euclidean Algorithm, run on natural numbers a and b, gives not only $\gcd(a,b)$ but also integers u and v such that

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

This gave us Theorem 1.23:

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 1.23

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 $\gcd(a, b)$.

Second proof of Theorem 1.23

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 $\gcd(a, b)$.

Second proof of Theorem 1.23

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 $\gcd(a, b)$.

Second proof of Theorem 1.23

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.

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

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{2.1}$$

Now, using the Division Algorithm, we can write

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

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

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

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{2.1}$$

Now, using the Division Algorithm, we can write

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

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

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

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{2.1}$$

Now, using the Division Algorithm, we can write

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

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

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

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{2.1}$$

Now, using the Division Algorithm, we can write

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

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

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

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{2.1}$$

Now, using the Division Algorithm, we can write

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

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

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

$$s = ak + bl, \text{ for some } k, l \in \mathbb{Z}. \tag{2.1}$$

Now, using the Division Algorithm, we can write

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

Substituting for s using (2.1) 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 $s|b$.

Substituting for s using (2.1) 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 $s|b$.

Substituting for s using (2.1) 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 $s|b$.

Substituting for s using (2.1) 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 $s|b$.

Substituting for s using (2.1) 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 $c|b$.

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

Substitution in (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 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 1.23 follows.

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

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

Substitution in (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 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 1.23 follows.

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

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

Substitution in (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 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 1.23 follows.

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

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

Substitution in (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 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 1.23 follows.

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

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

Substitution in (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 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 1.23 follows.

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

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

Substitution in (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 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 1.23 follows.

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

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

Substitution in (2.1) gives

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

Therefore $c|s$ and from Lemma 1.20.3 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 1.23 follows.

Coprime integers

Definition 2.1

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

Example 2.2

6 and 35 are coprime and

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

What about

$$11375 \cdot 3085622 - 7469451 \cdot 4699 = 1?$$

We have u and v such that $11375u + 7469451v = 1$.

Does this mean $\gcd(11375, 7469451) = 1$?

Coprime integers

Definition 2.1

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

Example 2.2

6 and 35 are coprime and

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

What about

$$11375 \cdot 3085622 - 7469451 \cdot 4699 = 1?$$

We have u and v such that $11375u + 7469451v = 1$.

Does this mean $\gcd(11375, 7469451) = 1$?

Coprime integers

Definition 2.1

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

Example 2.2

6 and 35 are coprime and

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

What about

$$11375 \cdot 3085622 - 7469451 \cdot 4699 = 1?$$

We have u and v such that $11375u + 7469451v = 1$.

Does this mean $\gcd(11375, 7469451) = 1$?

Coprime integers

Definition 2.1

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

Example 2.2

6 and 35 are coprime and

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

What about

$$11375 \cdot 3085622 - 7469451 \cdot 4699 = 1?$$

We have u and v such that $11375u + 7469451v = 1$.

Does this mean $\gcd(11375, 7469451) = 1$?

Coprime integers

Definition 2.1

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

Example 2.2

6 and 35 are coprime and

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

What about

$$11375 \cdot 3085622 - 7469451 \cdot 4699 = 1?$$

We have u and v such that $11375u + 7469451v = 1$.

Does this mean $\gcd(11375, 7469451) = 1$?

Corollary 2.3

Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.

> A corollary is something which follows easily from a previously proven fact.

Proof. This is an if and only if proof so has two halves.

ep(1)

> Prove that if a and b are coprime then there exist integers u and v such that $au + bv = 1$.

Corollary 2.3

Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.

> A corollary is something which follows easily from a previously proven fact.

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 $au + bv = 1$.

Corollary 2.3

Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.

> A corollary is something which follows easily from a previously proven fact.

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 $au + bv = 1$.

Corollary 2.3

Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.

> A corollary is something which follows easily from a previously proven fact.

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 $au + bv = 1$.

Corollary 2.3

Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.

> A corollary is something which follows easily from a previously proven fact.

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 1.23 that such u and v exist.

Corollary 2.3

Integers a and b are coprime if and only if there exist integers u and v such that $au + bv = 1$.

> A corollary is something which follows easily from a previously proven fact.

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 1.23 that such u and v exist.

This completes Step (1)

Step(2) Prove that if there exist integers u and v such that $au + bv = 1$ then $\gcd(a, b) = 1$.

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 $au + bv = 1$.

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

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

We have $d = 1$, so a and b are coprime, as required.

Euclid's Lemma

Lemma 2.4

Let a, b and c be integers with $\gcd(a, b) = 1$. If $a|bc$ then $a|c$.

Application to solving equations

A Linear Diophantine Equation is one of the form

$$ax + by = c,$$

where a, b and c are integers and we seek integer solutions.

Lemma 1.26 states that such an equation has a solution if and only if $\gcd(a,b)|c$.

Application to solving equations

A Linear Diophantine Equation is one of the form

$$ax + by = c,$$

where a, b and c are integers and we seek integer solutions.

Lemma 1.26 states that such an equation has a solution if and only if $\gcd(a,b)|c$.

Theorem 2.5

Let a, b, c be integers and let $d = \gcd(a, b)$. The equation

$$ax + by = c \tag{2.2}$$

has an integer solution if and only if $d \mid c$.

If $d \mid c$ then equation (2.2) 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

$$u_1 = u_0 + (b/d)t$$

and

$$v_1 = v_0 - (a/d)t,$$

for some $t \in \mathbb{Z}$.

Theorem 2.5

Let a, b, c be integers and let $d = \gcd(a, b)$. The equation

$$ax + by = c \tag{2.2}$$

has an integer solution if and only if $d \mid c$.

If $d \mid c$ then equation (2.2) 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

$$u_1 = u_0 + (b/d)t$$

and

$$v_1 = v_0 - (a/d)t,$$

for some $t \in \mathbb{Z}$.

Theorem 2.5

Let a, b, c be integers and let $d = \gcd(a, b)$. The equation

$$ax + by = c \tag{2.2}$$

has an integer solution if and only if $d \mid c$.

If $d \mid c$ then equation (2.2) 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

$$u_1 = u_0 + (b/d)t$$

and

$$v_1 = v_0 - (a/d)t,$$

for some $t \in \mathbb{Z}$.

Example 1.22 continued

Example 2.6

$\gcd(2600, 2028) = 52$ 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

Example 1.22 continued

Example 2.6

$\gcd(2600, 2028) = 52$ 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

Example 1.22 continued

Example 2.6

$\gcd(2600, 2028) = 52$ 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

Example 2.7

Find all integer solutions to the equation $63x + 12y = 18$.

List all solutions with $x > -12$ and $y > 6$.

From Example 1.2 we have $\gcd(63, 12) = 3$ and as $3|18$ the equation has solutions.

In Example 1.2 we also found that $63 \cdot 1 + 12 \cdot (-5) = 3$.

Example 2.7

Find all integer solutions to the equation $63x + 12y = 18$.

List all solutions with $x > -12$ and $y > 6$.

From Example 1.2 we have $\gcd(63, 12) = 3$ and as $3|18$ the equation has solutions.

In Example 1.2 we also found that $63 \cdot 1 + 12 \cdot (-5) = 3$.

Example 2.7

Find all integer solutions to the equation $63x + 12y = 18$.

List all solutions with $x > -12$ and $y > 6$.

From Example 1.2 we have $\gcd(63, 12) = 3$ and as $3|18$ the equation has solutions.

In Example 1.2 we also found that $63 \cdot 1 + 12 \cdot (-5) = 3$.

Example 2.7

Find all integer solutions to the equation $63x + 12y = 18$.

List all solutions with $x > -12$ and $y > 6$.

From Example 1.2 we have $\gcd(63, 12) = 3$ and as $3|18$ the equation has solutions.

In Example 1.2 we also found that $63 \cdot 1 + 12 \cdot (-5) = 3$.

Example 2.8

Find the general form for integer solutions to the equation $12378x + 3054y = 42$.

Find all solutions x, y with $x > 0$ and $y > -2000$.

Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions.

In the given example we also found
$12378 \cdot 132 + 3054 \cdot (-535) = 6$.

Multiplying through by 7 gives
$12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$.

This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

Example 2.8

Find the general form for integer solutions to the equation $12378x + 3054y = 42$.

Find all solutions x, y with $x > 0$ and $y > -2000$.

Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions.

In the given example we also found
$12378 \cdot 132 + 3054 \cdot (-535) = 6$.

Multiplying through by 7 gives
$12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$.

This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

Example 2.8

Find the general form for integer solutions to the equation $12378x + 3054y = 42$.

Find all solutions x, y with $x > 0$ and $y > -2000$.

Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions.

In the given example we also found
$12378 \cdot 132 + 3054 \cdot (-535) = 6$.

Multiplying through by 7 gives
$12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$.

This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

Example 2.8

Find the general form for integer solutions to the equation $12378x + 3054y = 42$.

Find all solutions x, y with $x > 0$ and $y > -2000$.

Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions.

In the given example we also found
$12378 \cdot 132 + 3054 \cdot (-535) = 6$.

Multiplying through by 7 gives
$12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$.

This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

Example 2.8

Find the general form for integer solutions to the equation $12378x + 3054y = 42$.

Find all solutions x, y with $x > 0$ and $y > -2000$.

Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions.

In the given example we also found $12378 \cdot 132 + 3054 \cdot (-535) = 6$.

Multiplying through by 7 gives $12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$.

This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

Example 2.8

Find the general form for integer solutions to the equation $12378x + 3054y = 42$.

Find all solutions x, y with $x > 0$ and $y > -2000$.

Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions.

In the given example we also found $12378 \cdot 132 + 3054 \cdot (-535) = 6$.

Multiplying through by 7 gives $12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$.

This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

Example 2.8

Find the general form for integer solutions to the equation $12378x + 3054y = 42$.

Find all solutions x, y with $x > 0$ and $y > -2000$.

Find all solutions with $x > 0$ and $y > 0$.

In Example 1.25 we found that $\gcd(12378, 3054) = 6$ and since $6|42$ this equation has solutions.

In the given example we also found $12378 \cdot 132 + 3054 \cdot (-535) = 6$.

Multiplying through by 7 gives $12378 \cdot 132 \cdot 7 + 3054 \cdot (-535) \cdot 7 = 42$.

This gives a particular solution

$$x = 132 \cdot 7 = 924 \text{ and } y = (-535) \cdot 7 = -3745.$$

For the general form of the solution, in this case we have $a/d = 12378/6 = 2063$ and $b/d = 3054/6 = 509$.

The general form of the solution is therefore

$$x = 924 + 509t \text{ and } y = -3745 - 2063t,$$

for $t \in \mathbb{Z}$.

(We can check this is correct: with $t = 1$ we verify that $12373 \cdot 1433 + 3054(-5808) = 42$.)

For the general form of the solution, in this case we have $a/d = 12378/6 = 2063$ and $b/d = 3054/6 = 509$.

The general form of the solution is therefore

$$x = 924 + 509t \text{ and } y = -3745 - 2063t,$$

for $t \in \mathbb{Z}$.

(We can check this is correct: with $t = 1$ we verify that $12373 \cdot 1433 + 3054(-5808) = 42$.)

For the general form of the solution, in this case we have $a/d = 12378/6 = 2063$ and $b/d = 3054/6 = 509$.

The general form of the solution is therefore

$$x = 924 + 509t \text{ and } y = -3745 - 2063t,$$

for $t \in \mathbb{Z}$.

(We can check this is correct: with $t = 1$ we verify that $12373 \cdot 1433 + 3054(-5808) = 42$.)

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

For solutions with $x > 0$ we require $924 + 509t > 0$, that is $t > -924/509$.

As t is an integer we therefore require $t \geq -1$.

We have solutions with $y > -2000$ if and only if $-3745 - 2063t > -2000$

if and only if $3754 + 2063t < 2000$

if and only if $t < -1754/2063$

if and only if $t \leq -1$.

Therefore there is a unique solution with $x > 0$ and $y < -2000$, which we obtain by setting $t = -1$,

namely

$$x = 415, y = -1682.$$

We have solutions with $y > 0$ if and only if $3754 + 2063t < 0$

if and only if $t < -3754/2000$

if and only if $t \leq -2$.

Thus to obtain a solution with $x, y > 0$ we need both $t \geq -1$ and $t \leq -2$.

There are no such t so there are no solutions with $x, y > 0$.

We have solutions with $y > 0$ if and only if $3754 + 2063t < 0$

if and only if $t < -3754/2000$

if and only if $t \leq -2$.

Thus to obtain a solution with $x, y > 0$ we need both $t \geq -1$ and $t \leq -2$.

There are no such t so there are no solutions with $x, y > 0$.

We have solutions with $y > 0$ if and only if $3754 + 2063t < 0$

if and only if $t < -3754/2000$

if and only if $t \leq -2$.

Thus to obtain a solution with $x, y > 0$ we need both $t \geq -1$ and $t \leq -2$.

There are no such t so there are no solutions with $x, y > 0$.

We have solutions with $y > 0$ if and only if $3754 + 2063t < 0$

if and only if $t < -3754/2000$

if and only if $t \leq -2$.

Thus to obtain a solution with $x, y > 0$ we need both $t \geq -1$ and $t \leq -2$.

There are no such t so there are no solutions with $x, y > 0$.

We have solutions with $y > 0$ if and only if $3754 + 2063t < 0$

if and only if $t < -3754/2000$

if and only if $t \leq -2$.

Thus to obtain a solution with $x, y > 0$ we need both $t \geq -1$ and $t \leq -2$.

There are no such t so there are no solutions with $x, y > 0$.

Objectives

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

(i) recall Theorem 1.23 and understand its proof;

(ii) define a coprime pair of integers;

(iii) recall Corollary 2.3 and Euclid's Lemma and understand their proofs;

(iv) find the general form of the solution of a linear Diophantine equation in two variables.

Proof by induction

Proof by induction is a method of proving that a sequence of statements, one for each positive integer, are all true.

We could use induction to prove for example that

$$3|(n^3 - n), \text{ for all integers } n \geq 1,$$

(which we already know because by Example 1.13)

or that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \text{ for all integers } n \geq 1,$$

In the first case we have to prove something for all values of n, namely ...

In Example 1.13 we used the Division Algorithm to prove all these to be true.

In this chapter we'll see a different method of proof.

Proof by induction

Proof by induction is a method of proving that a sequence of statements, one for each positive integer, are all true.

We could use induction to prove for example that

$$3|(n^3 - n), \text{ for all integers } n \geq 1,$$

(which we already know because by Example 1.13)

or that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \text{ for all integers } n \geq 1,$$

In the first case we have to prove something for all values of n, namely ...

In Example 1.13 we used the Division Algorithm to prove all these to be true.

In this chapter we'll see a different method of proof.

Proof by induction

Proof by induction is a method of proving that a sequence of statements, one for each positive integer, are all true.

We could use induction to prove for example that

$$3|(n^3 - n), \text{ for all integers } n \geq 1,$$

(which we already know because by Example 1.13)

or that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \text{ for all integers } n \geq 1,$$

In the first case we have to prove something for all values of n, namely ...

In Example 1.13 we used the Division Algorithm to prove all these to be true.

In this chapter we'll see a different method of proof.

Proof by induction

Proof by induction is a method of proving that a sequence of statements, one for each positive integer, are all true.

We could use induction to prove for example that

$$3|(n^3 - n), \text{ for all integers } n \geq 1,$$

(which we already know because by Example 1.13)

or that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \text{ for all integers } n \geq 1,$$

In the first case we have to prove something for all values of n, namely ...

In Example 1.13 we used the Division Algorithm to prove all these to be true.

In this chapter we'll see a different method of proof.

Proof by induction

Proof by induction is a method of proving that a sequence of statements, one for each positive integer, are all true.

We could use induction to prove for example that

$$3|(n^3 - n), \text{ for all integers } n \geq 1,$$

(which we already know because by Example 1.13)

or that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \text{ for all integers } n \geq 1,$$

In the first case we have to prove something for all values of n, namely ...

In Example 1.13 we used the Division Algorithm to prove all these to be true.

In this chapter we'll see a different method of proof.

Proof by induction

Proof by induction is a method of proving that a sequence of statements, one for each positive integer, are all true.

We could use induction to prove for example that

$$3|(n^3 - n), \text{ for all integers } n \geq 1,$$

(which we already know because by Example 1.13)

or that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \text{ for all integers } n \geq 1,$$

In the first case we have to prove something for all values of n, namely ...

In Example 1.13 we used the Division Algorithm to prove all these to be true.

In this chapter we'll see a different method of proof.

In the second case above we have to prove that the entries in the second and third columns of the table below are equal, on every line.

n	sum of first n odd numbers	n^2
1	1	1×1
2	$1+3=4$	2×2
3	$1+3+5=9$	3×3
4	$1+3+5+7=16$	4×4
5	$1+3+5+7+9=25$	5×5
$\vdots$	$\vdots$	$\vdots$
100	$1+\cdots+199$	10000
$\vdots$	$\vdots$	$\vdots$
k	$1+\cdots+(2k-1)$	k^2
$\vdots$	$\vdots$	$\vdots$

Does this hold for all positive integers?

In the second case above we have to prove that the entries in the second and third columns of the table below are equal, on every line.

n	sum of first n odd numbers	n^2
1	1	1×1
2	$1+3=4$	2×2
3	$1+3+5=9$	3×3
4	$1+3+5+7=16$	4×4
5	$1+3+5+7+9=25$	5×5
$\vdots$	$\vdots$	$\vdots$
100	$1+\cdots+199$	10000
$\vdots$	$\vdots$	$\vdots$
k	$1+\cdots+(2k-1)$	k^2
$\vdots$	$\vdots$	$\vdots$

Does this hold for all positive integers?

The idea

Recall that the **natural numbers** are the positive integers, $0, 1, 2, \cdots$.

These have the property that if we begin at 1 and keep adding 1 then we eventually form a list which contains **every** natural number.

Therefore if we have a sequence of statements, one corresponding to each natural number, and

1. we can prove the first one is true (the case $n = 1$)and
2. we can show that if the kth one is true then the $k + 1$st is also true (for any $k \geq 1$)

then all the statements must be true.

The idea

Recall that the **natural numbers** are the positive integers, $0, 1, 2, \cdots$.

These have the property that if we begin at 1 and keep adding 1 then we eventually form a list which contains **every** natural number.

Therefore if we have a sequence of statements, one corresponding to each natural number, and

1. we can prove the first one is true (the case $n = 1$)and
2. we can show that if the kth one is true then the $k + 1$st is also true (for any $k \geq 1$)

then all the statements must be true.

The idea

Recall that the **natural numbers** are the positive integers, $0, 1, 2, \cdots$.

These have the property that if we begin at 1 and keep adding 1 then we eventually form a list which contains **every** natural number.

Therefore if we have a sequence of statements, one corresponding to each natural number, and

1. we can prove the first one is true (the case $n = 1$)and
2. we can show that if the kth one is true then the $k + 1$st is also true (for any $k \geq 1$)

then all the statements must be true.

The idea

Recall that the **natural numbers** are the positive integers, $0, 1, 2, \cdots$.

These have the property that if we begin at 1 and keep adding 1 then we eventually form a list which contains **every** natural number.

Therefore if we have a sequence of statements, one corresponding to each natural number, and

1. we can prove the first one is true (the case $n = 1$)and
2. we can show that if the kth one is true then the $k + 1$st is also true (for any $k \geq 1$)

then all the statements must be true.

The idea

Recall that the **natural numbers** are the positive integers, $0, 1, 2, \cdots$.

These have the property that if we begin at 1 and keep adding 1 then we eventually form a list which contains **every** natural number.

Therefore if we have a sequence of statements, one corresponding to each natural number, and

1. we can prove the first one is true (the case $n = 1$)and
2. we can show that if the kth one is true then the $k + 1$st is also true (for any $k \geq 1$)

then all the statements must be true.

The idea

Recall that the **natural numbers** are the positive integers, $0, 1, 2, \cdots$.

These have the property that if we begin at 1 and keep adding 1 then we eventually form a list which contains **every** natural number.

Therefore if we have a sequence of statements, one corresponding to each natural number, and

1. we can prove the first one is true (the case $n = 1$)and
2. we can show that if the kth one is true then the $k + 1$st is also true (for any $k \geq 1$)

then all the statements must be true.

Example 3.1

Prove by induction that $3|(n^3 - n)$, for all $n \geq 1$.

Solution.

First we need to prove the statement holds in the case $n = 1$. This is easy as when $n = 1$ we have $n^3 - n = 0$ and $3|0$.

Now we need to show that if the kth statement holds then so does the $k+1$st. For clarity write out what we are assuming and what it is we have to prove, namely:

We assume that $3|k^3 - k$, as this is the case $n = k$ of our statements.

We shall show that in this case $3|(k+1)^3 - (k+1)$, which is the case $n = k+1$. ....

We may now conclude, using induction, that $3|n^3 - n$, for all $n \geq 1$.

Example 3.1

Prove by induction that $3|(n^3 - n)$, for all $n \geq 1$.

Solution.

First we need to prove the statement holds in the case $n = 1$.
This is easy as when $n = 1$ we have $n^3 - n = 0$ and $3|0$.

Now we need to show that if the kth statement holds then so does the $k+1$st. For clarity write out what we are assuming and what it is we have to prove, namely:

We assume that $3|k^3 - k$, as this is the case $n = k$ of our statements.

We shall show that in this case $3|(k+1)^3 - (k+1)$, which is the case $n = k+1$. ....

We may now conclude, using induction, that $3|n^3 - n$, for all $n \geq 1$.

Example 3.1

Prove by induction that $3|(n^3 - n)$, for all $n \geq 1$.

Solution.
First we need to prove the statement holds in the case $n = 1$. This is easy as when $n = 1$ we have $n^3 - n = 0$ and $3|0$.

Now we need to show that if the kth statement holds then so does the $k+1$st. For clarity write out what we are assuming and what it is we have to prove, namely:

We assume that $3|k^3 - k$, as this is the case $n = k$ of our statements.

We shall show that in this case $3|(k+1)^3 - (k+1)$, which is the case $n = k+1$. ....

We may now conclude, using induction, that $3|n^3 - n$, for all $n \geq 1$.

Example 3.1

Prove by induction that $3|(n^3 - n)$, for all $n \geq 1$.

Solution.
First we need to prove the statement holds in the case $n = 1$.
This is easy as when $n = 1$ we have $n^3 - n = 0$ and $3|0$.

Now we need to show that if the kth statement holds then so does the $k+1$st. For clarity write out what we are assuming and what it is we have to prove, namely:

We assume that $3|k^3 - k$, as this is the case $n = k$ of our statements.

We shall show that in this case $3|(k+1)^3 - (k+1)$, which is the case $n = k+1$. ....

We may now conclude, using induction, that $3|n^3 - n$, for all $n \geq 1$.

Example 3.1

Prove by induction that $3|(n^3 - n)$, for all $n \geq 1$.

Solution.
First we need to prove the statement holds in the case $n = 1$. This is easy as when $n = 1$ we have $n^3 - n = 0$ and $3|0$.

Now we need to show that if the kth statement holds then so does the $k+1$st. For clarity write out what we are assuming and what it is we have to prove, namely:

We assume that $3|k^3 - k$, as this is the case $n = k$ of our statements.

We shall show that in this case $3|(k+1)^3 - (k+1)$, which is the case $n = k+1$. ....

We may now conclude, using induction, that $3|n^3 - n$, for all $n \geq 1$.

Example 3.1

Prove by induction that $3|(n^3 - n)$, for all $n \geq 1$.

Solution.
First we need to prove the statement holds in the case $n = 1$. This is easy as when $n = 1$ we have $n^3 - n = 0$ and $3|0$.

Now we need to show that if the kth statement holds then so does the $k+1$st. For clarity write out what we are assuming and what it is we have to prove, namely:

We assume that $3|k^3 - k$, as this is the case $n = k$ of our statements.

We shall show that in this case $3|(k+1)^3 - (k+1)$, which is the case $n = k+1$. ....

We may now conclude, using induction, that $3|n^3 - n$, for all $n \geq 1$.

The Principle of proof by induction

Suppose that we have a sequence of statements $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... one for each positive integer n.

For example $P(n)$ might be "$3|n^3 - n$" as in the first example above, or it could be "the sum of the first n odd positive integers equals n^2", as in the second example.

The **Principle of Induction**.

Assume it can be shown

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

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

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

The Principle of proof by induction

Suppose that we have a sequence of statements $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... one for each positive integer n.

For example $P(n)$ might be "$3|n^3 - n$" as in the first example above, or it could be "the sum of the first n odd positive integers equals n^2", as in the second example.

The **Principle of Induction**.

Assume it can be shown

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

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

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

The Principle of proof by induction

Suppose that we have a sequence of statements $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... one for each positive integer n.

For example $P(n)$ might be "$3|n^3 - n$" as in the first example above, or it could be "the sum of the first n odd positive integers equals n^2", as in the second example.

The **Principle of Induction**.

Assume it can be shown

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

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

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

The Principle of proof by induction

Suppose that we have a sequence of statements $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... one for each positive integer n.

For example $P(n)$ might be "$3|n^3 - n$" as in the first example above, or it could be "the sum of the first n odd positive integers equals n^2", as in the second example.

The **Principle of Induction**.

Assume it can be shown

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

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

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

The Principle of proof by induction

Suppose that we have a sequence of statements $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... one for each positive integer n.

For example $P(n)$ might be "$3|n^3 - n$" as in the first example above, or it could be "the sum of the first n odd positive integers equals n^2", as in the second example.

The **Principle of Induction**.

Assume it can be shown

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

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

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

The Principle of proof by induction

Suppose that we have a sequence of statements $P(1)$, $P(2)$, $P(3)$, ..., $P(n)$, ... one for each positive integer n.

For example $P(n)$ might be "$3|n^3 - n$" as in the first example above, or it could be "the sum of the first n odd positive integers equals n^2", as in the second example.

The **Principle of Induction**.

Assume it can be shown

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

(2) that 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 3.2

Prove by induction that $1+3+5+\cdots+(2n-1)=n^2$, for all $n \geq 1$.

Solution. In the above notation $P(n)$ is the statement

$$1+3+5+\cdots+(2n-1)=n^2,$$

so statements $P(1)$, $P(2)$, ... , $P(5)$, $P(100)$ and $P(k)$ appear in the table above.

Proof by induction takes the following form.

Basis.
Show that $P(1)$ is true. This is the case $n=1$.

In this example when $n=1$ we have the statement $1=1^2$, obtained by replacing each occurrence of n in $P(n)$ with 1.

Since this is true the first part of the proof is complete.

Example 3.2

Prove by induction that $1+3+5+\cdots+(2n-1)=n^2$, for all $n \geq 1$.

Solution. In the above notation $P(n)$ is the statement

$$1+3+5+\cdots+(2n-1)=n^2,$$

so statements $P(1)$, $P(2)$, ... , $P(5)$, $P(100)$ and $P(k)$ appear in the table above.

Proof by induction takes the following form.

Basis.
Show that $P(1)$ is true. This is the case $n=1$.

In this example when $n=1$ we have the statement $1=1^2$, obtained by replacing each occurrence of n in $P(n)$ with 1.

Since this is true the first part of the proof is complete.

Example 3.2

Prove by induction that $1+3+5+\cdots+(2n-1)=n^2$, for all $n \geq 1$.

Solution. In the above notation $P(n)$ is the statement

$$1+3+5+\cdots+(2n-1)=n^2,$$

so statements $P(1)$, $P(2)$, ... , $P(5)$, $P(100)$ and $P(k)$ appear in the table above.

Proof by induction takes the following form.

Basis.
Show that $P(1)$ is true. This is the case $n=1$.

In this example when $n=1$ we have the statement $1=1^2$, obtained by replacing each occurrence of n in $P(n)$ with 1.

Since this is true the first part of the proof is complete.

Example 3.2

Prove by induction that $1+3+5+\cdots+(2n-1)=n^2$, for all $n \geq 1$.

Solution. In the above notation $P(n)$ is the statement

$$1+3+5+\cdots+(2n-1)=n^2,$$

so statements $P(1)$, $P(2)$, ... , $P(5)$, $P(100)$ and $P(k)$ appear in the table above.

Proof by induction takes the following form.

Basis.
Show that $P(1)$ is true. This is the case $n=1$.

In this example when $n=1$ we have the statement $1=1^2$, obtained by replacing each occurrence of n in $P(n)$ with 1.

Since this is true the first part of the proof is complete.

Example 3.2

Prove by induction that $1+3+5+\cdots+(2n-1)=n^2$, for all $n \geq 1$.

Solution. In the above notation $P(n)$ is the statement

$$1+3+5+\cdots+(2n-1)=n^2,$$

so statements $P(1)$, $P(2)$, ... , $P(5)$, $P(100)$ and $P(k)$ appear in the table above.

Proof by induction takes the following form.

Basis.
Show that $P(1)$ is true. This is the case $n=1$.

In this example when $n=1$ we have the statement $1=1^2$, obtained by replacing each occurrence of n in $P(n)$ with 1.

Since this is true the first part of the proof is complete.

Example 3.2

Prove by induction that $1+3+5+\cdots+(2n-1)=n^2$, for all $n \geq 1$.

Solution. In the above notation $P(n)$ is the statement

$$1+3+5+\cdots+(2n-1)=n^2,$$

so statements $P(1)$, $P(2)$, ... , $P(5)$, $P(100)$ and $P(k)$ appear in the table above.

Proof by induction takes the following form.

Basis.
Show that $P(1)$ is true. This is the case $n=1$.

In this example when $n=1$ we have the statement $1=1^2$, obtained by replacing each occurrence of n in $P(n)$ with 1.

Since this is true the first part of the proof is complete.

The inductive hypothesis (IH)

Now we assume the statement holds in the case $n = k$: that is we assume that $P(k)$ is true,

which in our example means we assume that

$$1 + 3 + \cdots + (2k - 1) = k^2,$$

where $k \geq 1$.

Note that we obtain this by replacing every occurence of n in $P(n)$ with k.

The inductive step

Next we must show that the statement holds in the case where $n = k + 1$. That is we must show that $P(k + 1)$ holds,

which in our case means that we must prove that

$$1 + 3 + \cdots + (2(k + 1) - 1) = (k + 1)^2.$$

(Again we obtain $P(k + 1)$ by replacing n with $k + 1$ throughout $P(n)$.)

The inductive hypothesis (IH)

Now we assume the statement holds in the case $n = k$: that is we assume that $P(k)$ is true,

which in our example means we assume that

$$1 + 3 + \cdots + (2k - 1) = k^2,$$

where $k \geq 1$.

Note that we obtain this by replacing every occurence of n in $P(n)$ with k.

The inductive step

Next we must show that the statement holds in the case where $n = k + 1$. That is we must show that $P(k + 1)$ holds,

which in our case means that we must prove that

$$1 + 3 + \cdots + (2(k + 1) - 1) = (k + 1)^2.$$

(Again we obtain $P(k + 1)$ by replacing n with $k + 1$ throughout $P(n)$.)

The inductive hypothesis (IH)

Now we assume the statement holds in the case $n = k$: that is we assume that $P(k)$ is true,

which in our example means we assume that

$$1 + 3 + \cdots + (2k - 1) = k^2,$$

where $k \geq 1$.

Note that we obtain this by replacing every occurence of n in $P(n)$ with k.

The inductive step

Next we must show that the statement holds in the case where $n = k + 1$. That is we must show that $P(k + 1)$ holds,

which in our case means that we must prove that

$$1 + 3 + \cdots + (2(k + 1) - 1) = (k + 1)^2.$$

(Again we obtain $P(k + 1)$ by replacing n with $k + 1$ throughout $P(n)$.)

The inductive hypothesis (IH)

Now we assume the statement holds in the case $n = k$: that is we assume that $P(k)$ is true,

which in our example means we assume that

$$1 + 3 + \cdots + (2k - 1) = k^2,$$

where $k \geq 1$.

Note that we obtain this by replacing every occurence of n in $P(n)$ with k.

The inductive step

Next we must show that the statement holds in the case where $n = k + 1$. That is we must show that $P(k + 1)$ holds,

which in our case means that we must prove that

$$1 + 3 + \cdots + (2(k + 1) - 1) = (k + 1)^2.$$

(Again we obtain $P(k + 1)$ by replacing n with $k + 1$ throughout $P(n)$.)

The inductive hypothesis (IH)

Now we assume the statement holds in the case $n = k$: that is we assume that $P(k)$ is true,

which in our example means we assume that

$$1 + 3 + \cdots + (2k - 1) = k^2,$$

where $k \geq 1$.

Note that we obtain this by replacing every occurence of n in $P(n)$ with k.

The inductive step

Next we must show that the statement holds in the case where $n = k + 1$. That is we must show that $P(k + 1)$ holds,

which in our case means that we must prove that

$$1 + 3 + \cdots + (2(k + 1) - 1) = (k + 1)^2.$$

(Again we obtain $P(k + 1)$ by replacing n with $k + 1$ throughout $P(n)$.)

Remarks

- In proof by induction we make the assumption that $P(k)$ holds for some $k \geq 1$ and then prove that $P(k+1)$ also holds. For the proof to be correct we must be sure this works for **all possible** values of k. If it fails for just one value of k then the proof does not work.
- Often there is more than one way of proving a statement, or sequence of statements. For instance Examples 1.13 and 3.1 both prove the same thing (almost). In this case the original proof seems better as it gives more insight into why the statement is true.

Remarks

- In proof by induction we make the assumption that $P(k)$ holds for some $k \geq 1$ and then prove that $P(k+1)$ also holds. For the proof to be correct we must be sure this works for **all possible** values of k. If it fails for just one value of k then the proof does not work.
- Often there is more than one way of proving a statement, or sequence of statements. For instance Examples 1.13 and 3.1 both prove the same thing (almost). In this case the original proof seems better as it gives more insight into why the statement is true.

Example 3.3

Prove by induction that

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1},$$

for all $n\in\mathbb{N}$.

Here $P(n)$ is the statement

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1}$$

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

Example 3.3

Prove by induction that

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1},$$

for all $n\in\mathbb{N}$.
Here $P(n)$ is the statement

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1}$$

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

Example 3.3

Prove by induction that

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1},$$

for all $n\in\mathbb{N}$.
Here $P(n)$ is the statement

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=1-\frac{1}{n+1}$$

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

Summation notation

Note: to save space we could write

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=\sum_{j=1}^{n}\frac{1}{j\times(j+1)}$$

in which case $P(n)$ would appear as

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

This requires care when writing out $P(k)$ and $P(k+1)$. As j is just a dummy variable it remains untouched and the rule is exactly as before: to obtain $P(k)$ replace n with k throughout $P(n)$.

Thus $P(k)$ appears as

$$\sum_{j=1}^{k}\frac{1}{j\times(j+1)}=1-\frac{1}{k+1}$$

as in the worked solution to the problem.

Summation notation

Note: to save space we could write

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=\sum_{j=1}^{n}\frac{1}{j\times(j+1)}$$

in which case $P(n)$ would appear as

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

This requires care when writing out $P(k)$ and $P(k+1)$. As j is just a dummy variable it remains untouched and the rule is exactly as before: to obtain $P(k)$ replace n with k throughout $P(n)$.

Thus $P(k)$ appears as

$$\sum_{j=1}^{k}\frac{1}{j\times(j+1)}=1-\frac{1}{k+1}$$

as in the worked solution to the problem.

Summation notation

Note: to save space we could write

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=\sum_{j=1}^{n}\frac{1}{j\times(j+1)}$$

in which case $P(n)$ would appear as

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

This requires care when writing out $P(k)$ and $P(k+1)$. As j is just a dummy variable it remains untouched and the rule is exactly as before: to obtain $P(k)$ replace n with k throughout $P(n)$.

Thus $P(k)$ appears as

$$\sum_{j=1}^{k}\frac{1}{j\times(j+1)}=1-\frac{1}{k+1}$$

as in the worked solution to the problem.

Summation notation

Note: to save space we could write

$$\frac{1}{1\times 2}+\frac{1}{2\times 3}+\frac{1}{3\times 4}+\cdots+\frac{1}{n(n+1)}=\sum_{j=1}^{n}\frac{1}{j\times(j+1)}$$

in which case $P(n)$ would appear as

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

This requires care when writing out $P(k)$ and $P(k+1)$. As j is just a dummy variable it remains untouched and the rule is exactly as before: to obtain $P(k)$ replace n with k throughout $P(n)$.

Thus $P(k)$ appears as

$$\sum_{j=1}^{k}\frac{1}{j\times(j+1)}=1-\frac{1}{k+1}$$

as in the worked solution to the problem.

The same applies to $P(k+1)$.

This notation will be used in problem class and assignment exercises.

The same applies to $P(k+1)$.

This notation will be used in problem class and assignment exercises.

Change of basis

It is possible to start induction at some point other than $n = 1$.
In this case we use the following version of the Principle of Induction.

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

$(1')$ that $P(s)$ is true and

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

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

Change of basis

It is possible to start induction at some point other than $n = 1$. In this case we use the following version of the Principle of Induction.

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

$(1')$ that $P(s)$ is true and

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

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

Change of basis

It is possible to start induction at some point other than $n = 1$. In this case we use the following version of the Principle of Induction.

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

($1'$) that $P(s)$ is true and

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

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

Change of basis

It is possible to start induction at some point other than $n = 1$. In this case we use the following version of the Principle of Induction.

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

(1′) that $P(s)$ is true and

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

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

Change of basis

It is possible to start induction at some point other than $n = 1$. In this case we use the following version of the Principle of Induction.

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

(1′) that $P(s)$ is true and

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

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

Change of basis

It is possible to start induction at some point other than $n = 1$. In this case we use the following version of the Principle of Induction.

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

$(1')$ that $P(s)$ is true and

$(2')$ that 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 3.4 (Bernoulli's Inequality)

Prove that

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

Example 3.5

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 $n = 9$.

In fact, for any positive integer t and sufficiently large n we have $2^n > n^t$. In our proof $t = 3$ and we show exactly what "sufficiently large" means in this case.

Example 3.5

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 $n = 9$.

In fact, for any positive integer t and sufficiently large n we have $2^n > n^t$. In our proof $t = 3$ and we show exactly what "sufficiently large" means in this case.

Example 3.5

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 $n = 9$.

In fact, for any positive integer t and sufficiently large n we have $2^n > n^t$. In our proof $t = 3$ and we show exactly what "sufficiently large" means in this case.

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;

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 4.1

A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p.

An integer greater than one which is not prime is called **composite**.

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 4.1

A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p.

An integer greater than one which is not prime is called **composite**.

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 4.1

A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p.

An integer greater than one which is not prime is called **composite**.

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 4.1

A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p.

An integer greater than one which is not prime is called **composite**.

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 4.1

A positive integer $p > 1$ is called a **prime** if the only positive divisors of p are 1 and p.

An integer greater than one 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

1 is neither prime nor 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

1 is neither prime nor 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

1 is neither prime nor 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

1 is neither prime nor 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

1 is neither prime nor 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.

1 is neither prime nor 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.

1 is neither prime nor composite.

The prime divisor property

A fundamental property of prime numbers is the following.

Theorem 4.2

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 4.2

If p is a prime and $p|ab$ then $p|a$ or $p|b$.

Example 4.3

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 4.3

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 4.3

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 4.3

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 4.3

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 4.3

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 4.3

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 4.3

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 4.4

If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Corollary 4.4

If p is prime and $p|a_1 \cdots a_n$ then $p|a_i$, for some i.

Inductive Step: Suppose that $p | a_1 \cdots a_{n+1}$.

Inductive Step: Suppose that $p | a_1 \cdots a_{n+1}$.

Let

$$a = a_1 \cdots a_n \text{ and } b = a_{n+1}.$$

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 4.2, $p|a$ or $p|b$.

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 4.2, $p|a$ or $p|b$.

If $p|a$ the inductive hypothesis implies that $p|a_i$, for some i with $1 \leq i \leq n$.

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 4.2, $p|a$ 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 $p|a_{n+1}$.

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 4.2, $p|a$ 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.

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.

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 4.5

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'll see that all positive numbers > 1 are products of primes – and no number has more than one factorisation as a product of primes (if we count correctly).

Example 4.5

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'll see that all positive numbers > 1 are products of primes – and no number has more than one factorisation as a product of primes (if we count correctly).

Example 4.5

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'll see that all positive numbers > 1 are products of primes – and no number has more than one factorisation as a product of primes (if we count correctly).

Example 4.5

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'll see that all positive numbers > 1 are products of primes – and no number has more than one factorisation as a product of primes (if we count correctly).

Example 4.5

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'll see that all positive numbers > 1 are products of primes – and no number has more than one factorisation as a product of primes (if we count correctly).

Example 4.5

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'll see that all positive numbers > 1 are products of primes – and no number has more than one factorisation as a product of primes (if we count correctly).

The Fundamental Theorem of Arithmetic

Theorem 4.6

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.

The Fundamental Theorem of Arithmetic

Theorem 4.6

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.

The Fundamental Theorem of Arithmetic

Theorem 4.6

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.

Rational numbers and polynomials

Before continuing we shall pause to see that this theorem really did need proving: that it is not a universal truth that holds in all situations.

To begin with consider the rational numbers $\mathbb{Q}$.
We can factor 2 as

$$2 = 4 \cdot (1/2) = 8 \cdot (1/4) = \cdots = 2^n \cdot (1/2^{n-1}) = \cdots =$$

and in general as $2q \cdot (1/q)$, for any non-zero element $q \in \mathbb{Q}$.
Therefore there is no hope of anything like Theorem 4.6 holding in $\mathbb{Q}$.

To see how the uniqueness part of the Theorem might fail, even when we can factorise elements into products of primes, we could investigate arithmetic with polynomials, but we shall not go into that here.

Rational numbers and polynomials

Before continuing we shall pause to see that this theorem really did need proving: that it is not a universal truth that holds in all situations.

To begin with consider the rational numbers $\mathbb{Q}$.

We can factor 2 as

$$2 = 4 \cdot (1/2) = 8 \cdot (1/4) = \cdots = 2^n \cdot (1/2^{n-1}) = \cdots =$$

and in general as $2q \cdot (1/q)$, for any non-zero element $q \in \mathbb{Q}$. Therefore there is no hope of anything like Theorem 4.6 holding in $\mathbb{Q}$.

To see how the uniqueness part of the Theorem might fail, even when we can factorise elements into products of primes, we could investigate arithmetic with polynomials, but we shall not go into that here.

Rational numbers and polynomials

Before continuing we shall pause to see that this theorem really did need proving: that it is not a universal truth that holds in all situations.
To begin with consider the rational numbers $\mathbb{Q}$.
We can factor 2 as

$$2 = 4 \cdot (1/2) = 8 \cdot (1/4) = \cdots = 2^n \cdot (1/2^{n-1}) = \cdots =$$

and in general as $2q \cdot (1/q)$, for any non-zero element $q \in \mathbb{Q}$.
Therefore there is no hope of anything like Theorem 4.6 holding in $\mathbb{Q}$.

To see how the uniqueness part of the Theorem might fail, even when we can factorise elements into products of primes, we could investigate arithmetic with polynomials, but we shall not go into that here.

Rational numbers and polynomials

Before continuing we shall pause to see that this theorem really did need proving: that it is not a universal truth that holds in all situations.
To begin with consider the rational numbers $\mathbb{Q}$.
We can factor 2 as

$$2 = 4 \cdot (1/2) = 8 \cdot (1/4) = \cdots = 2^n \cdot (1/2^{n-1}) = \cdots =$$

and in general as $2q \cdot (1/q)$, for any non-zero element $q \in \mathbb{Q}$.
Therefore there is no hope of anything like Theorem 4.6 holding in $\mathbb{Q}$.

To see how the uniqueness part of the Theorem might fail, even when we can factorise elements into products of primes, we could investigate arithmetic with polynomials, but we shall not go into that here.

Rational numbers and polynomials

Before continuing we shall pause to see that this theorem really did need proving: that it is not a universal truth that holds in all situations.
To begin with consider the rational numbers $\mathbb{Q}$.
We can factor 2 as

$$2 = 4 \cdot (1/2) = 8 \cdot (1/4) = \cdots = 2^n \cdot (1/2^{n-1}) = \cdots =$$

and in general as $2q \cdot (1/q)$, for any non-zero element $q \in \mathbb{Q}$.
Therefore there is no hope of anything like Theorem 4.6 holding in $\mathbb{Q}$.

To see how the uniqueness part of the Theorem might fail, even when we can factorise elements into products of primes, we could investigate arithmetic with polynomials, but we shall not go into that here.

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

$$140 = 2^2 \cdot 5 \cdot 7 \text{ and}$$

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.

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

$$140 = 2^2 \cdot 5 \cdot 7 \text{ and}$$

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.

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

$$140 = 2^2 \cdot 5 \cdot 7 \text{ and}$$
$$2200 = 2^3 \cdot 5^2 \cdot 11.$$

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.

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

$$140 = 2^2 \cdot 5 \cdot 7 \text{ and}$$
$$2200 = 2^3 \cdot 5^2 \cdot 11.$$

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.

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

$$140 = 2^2 \cdot 5 \cdot 7 \text{ and}$$
$$2200 = 2^3 \cdot 5^2 \cdot 11.$$

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.

Collected prime factorisation

Corollary 4.7

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 $a_i \geq 1$.

The square root of 2

If n is a positive integer and has collected prime factorisation $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

then $n^2 = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$

An integer m is of the form n^2, for some integer n, if and only if every prime in the prime factorisation of m has even exponent.

Corollary 4.8

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

The square root of 2

If n is a positive integer and has collected prime factorisation $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

then $n^2 = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$

An integer m is of the form n^2, for some integer n, if and only if every prime in the prime factorisation of m has even exponent.

Corollary 4.8

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

The square root of 2

If n is a positive integer and has collected prime factorisation $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

then $n^2 = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$

An integer m is of the form n^2, for some integer n, if and only if every prime in the prime factorisation of m has even exponent.

Corollary 4.8

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

The square root of 2

If n is a positive integer and has collected prime factorisation $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

then $n^2 = (p_1^{\alpha_1} \cdots p_k^{\alpha_k})(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$

An integer m is of the form n^2, for some integer n, if and only if every prime in the prime factorisation of m has even exponent.

Corollary 4.8

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

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 4.9

An integer $n > 1$ is composite if and only if it has a prime divisor p such that $p \leq \sqrt{n}$.

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.

Lemma 4.9

An integer $n > 1$ is composite if and only if it has a prime divisor p such that $p \leq \sqrt{n}$.

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.

Lemma 4.9

An integer $n > 1$ is composite if and only if it has a prime divisor p such that $p \leq \sqrt{n}$.

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.

Lemma 4.9

An integer $n > 1$ is composite if and only if it has a prime divisor p such that $p \leq \sqrt{n}$.

Example 4.10

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.

Example 4.10

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.

Example 4.10

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.

Example 4.10

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 4.11

There are infinitely many primes.

The proof is by contradiction.

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 4.11

There are infinitely many primes.

The proof is by contradiction.

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 4.11

There are infinitely many primes.

The proof is by contradiction.

Objectives

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

(i) define prime and composite numbers;

(ii) recall the prime divisor property, Theorem 4.2, and understand its proof;

(iii) recall the Fundamental Theorem of Arithmetic, Theorem 4.6, and understand its proof;

(iv) recognise and write down the prime factorisation and standard form or collected prime factorisation of an integer;

(v) use the sieve of Eratosthenes;

(vi) recall the statement of Theorem 4.11 and understand its proof.

Casting Out Nines

This is a method of testing integers for divisibility by 9.

Procedure 5.1

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 5.1

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 5.1

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 5.1

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 5.1

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 5.2

Cast out Nines from 215763401.

Example 5.3

Check the computation

$$215763401 \times 51422218 = 11095032642643428.$$

Example 5.2

Cast out Nines from 215763401.

Example 5.3

Check the computation

$$215763401 \times 51422218 = 11095032642643428.$$

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 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 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 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 0, 1 or 2 after division by 3, and called them white, red or blue.

We saw 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.

Congruence

In the Red, White and Blue number system we collected together all integers which left remainder 0, 1 or 2 after division by 3, and called them white, red or blue.

We saw 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.

Congruence

In the Red, White and Blue number system we collected together all integers which left remainder 0, 1 or 2 after division by 3, and called them white, red or blue.

We saw that a and b are the same colour if and only if $3 \mid b - a$.

Generalising this from 3 to an arbitrary integer n leads us to the definition of congruence.

Definition 5.4

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 division by n.

Definition 5.4

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 division by n.

Definition 5.4

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 division by n.

Definition 5.4

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 division by n.

In fact, if

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \qquad (5.1)$$

then

$$b - a = n(p - q),$$

so $n|b - a$: that is $a \equiv b \pmod{n}$.

On the other hand if $a \equiv b \pmod{n}$ then $n|b - a$ so $b - a = np$, for some p.

In this case if $a = nq + r$, with $0 \leq r < n$, then $b = np + a$

so $b = n(p + q) + r$ and (5.1) holds.

In fact, if

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \qquad (5.1)$$

then

$$b - a = n(p - q),$$

so $n|b-a$: that is $a \equiv b \pmod{n}$.

On the other hand if $a \equiv b \pmod{n}$ then $n|b-a$ so $b-a = np$, for some p.

In this case if $a = nq + r$, with $0 \leq r < n$, then $b = np + a$

so $b = n(p+q) + r$ and (5.1) holds.

In fact, if

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \qquad (5.1)$$

then

$$b - a = n(p - q),$$

so $n|b - a$: that is $a \equiv b \pmod{n}$.

On the other hand if $a \equiv b \pmod{n}$ then $n|b - a$ so $b - a = np$, for some p.

In this case if $a = nq + r$, with $0 \leq r < n$, then $b = np + a$

so $b = n(p + q) + r$ and (5.1) holds.

In fact, if

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \qquad (5.1)$$

then

$$b - a = n(p - q),$$

so $n|b - a$: that is $a \equiv b \pmod{n}$.

On the other hand if $a \equiv b \pmod{n}$ then $n|b - a$ so $b - a = np$, for some p.

In this case if $a = nq + r$, with $0 \leq r < n$, then $b = np + a$

so $b = n(p + q) + r$ and (5.1) holds.

In fact, if

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \qquad (5.1)$$

then

$$b - a = n(p - q),$$

so $n|b - a$: that is $a \equiv b \pmod{n}$.

On the other hand if $a \equiv b \pmod{n}$ then $n|b - a$ so $b - a = np$, for some p.

In this case if $a = nq + r$, with $0 \leq r < n$, then $b = np + a$

so $b = n(p + q) + r$ and (5.1) holds.

In fact, if

$$a = nq + r \text{ and } b = np + r, \text{ where } 0 \leq r < n \qquad (5.1)$$

then

$$b - a = n(p - q),$$

so $n|b - a$: that is $a \equiv b \pmod{n}$.

On the other hand if $a \equiv b \pmod{n}$ then $n|b - a$ so $b - a = np$, for some p.

In this case if $a = nq + r$, with $0 \leq r < n$, then $b = np + a$

so $b = n(p + q) + r$ and (5.1) holds.

Example 5.5

Congruence modulo 2 gives rise to the Odd and Even number system.

Example 5.6

Congruence modulo 3 gives rise to the Red, White and Blue number system.

Example 5.5

Congruence modulo 2 gives rise to the Odd and Even number system.

Example 5.6

Congruence modulo 3 gives rise to the Red, White and Blue number system.

Example 5.7

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.

Example 5.7

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.

Example 5.7

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.

Example 5.7

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.

Example 5.7

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 5.8

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.

Modular arithmetic is consistent

Lemma 5.8

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.

Modular arithmetic is consistent

Lemma 5.8

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.

Modular arithmetic is consistent

Lemma 5.8

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.

Modular arithmetic is consistent

Lemma 5.8

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 5.9

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 1.20.3.

Thus a is congruent to only one integer in the list. □

Lemma 5.9

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 1.20.3.

Thus a is congruent to only one integer in the list. □

Lemma 5.9

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 1.20.3.

Thus a is congruent to only one integer in the list. □

Lemma 5.9

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 1.20.3.

Thus a is congruent to only one integer in the list. □

Lemma 5.9

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 1.20.3.

Thus a is congruent to only one integer in the list. □

Lemma 5.9

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 1.20.3.

Thus a is congruent to only one integer in the list. $\square$

Example 5.10

In modular arithmetic we can always avoid computation with large numbers.

For example working modulo 10 we have

$$74598987903520453 24 \equiv 4 \pmod{10}$$

and

$$9874558754423 \equiv 3 \pmod{10}.$$

Therefore

$$74598987903520453 24 \cdot 9874558754423 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod{10}.$$

Example 5.10

In modular arithmetic we can always avoid computation with large numbers.

For example working modulo 10 we have

$$74598987903520453 24 \equiv 4 \pmod{10}$$

and

$$9874558754423 \equiv 3 \pmod{10}.$$

Therefore

$$74598987903520453 24 \cdot 9874558754423 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod{10}.$$

Example 5.10

In modular arithmetic we can always avoid computation with large numbers.

For example working modulo 10 we have

$$74598987903520453 24 \equiv 4 \pmod{10}$$

and

$$9874558754423 \equiv 3 \pmod{10}.$$

Therefore

$$74598987903520453 24 \cdot 9874558754423 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod{10}.$$

Example 5.10

In modular arithmetic we can always avoid computation with large numbers.

For example working modulo 10 we have

$$74598987903520453 24 \equiv 4 \pmod{10}$$

and

$$9874558754423 \equiv 3 \pmod{10}.$$

Therefore

$$74598987903520453 24 \cdot 9874558754423 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod{10}.$$

Similarly, working modulo 7 we have

$$4543362 \equiv 5 \pmod 7.$$

Therefore

$$4543362^2 \equiv 5^2 \equiv 25 \equiv 4 \pmod 7$$

and

$$4543362^3 = 4543362 \cdot 4543362^2 \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod 7.$$

Similarly, working modulo 7 we have

$$4543362 \equiv 5 \pmod 7.$$

Therefore

$$4543362^2 \equiv 5^2 \equiv 25 \equiv 4 \pmod 7$$

and

$$4543362^3 = 4543362 \cdot 4543362^2 \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod 7.$$

Similarly, working modulo 7 we have

$$4543362 \equiv 5 \pmod 7.$$

Therefore

$$4543362^2 \equiv 5^2 \equiv 25 \equiv 4 \pmod 7$$

and

$$4543362^3 = 4543362 \cdot 4543362^2 \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod 7.$$

Modular exponentiation

In coding and cryptography it's often necessary to compute powers of numbers modulo n; that is $x^m \pmod n$, where x, m and n may be integers with hundreds of digits.

$m = 10^{100}$ is a 1 followed by 100 zeroes (a googol).

Now if $x = 10$ then x^m is a 1 followed by 10^{100} zeros (and is called a googolplex).

It's estimated that there are around 10^{80} elementary particles in the universe:

so if x and m have over 100 digits then no computer, in the lifetime of the known universe, can possibly compute $x^m \pmod n$ by first computing x^m and then reducing modulo n.

Modular exponentiation

In coding and cryptography it's often necessary to compute powers of numbers modulo n; that is $x^m \pmod n$, where x, m and n may be integers with hundreds of digits.

$m = 10^{100}$ is a 1 followed by 100 zeroes (a googol).

Now if $x = 10$ then x^m is a 1 followed by 10^{100} zeros (and is called a googolplex).

It's estimated that there are around 10^{80} elementary particles in the universe:

so if x and m have over 100 digits then no computer, in the lifetime of the known universe, can possibly compute $x^m \pmod n$ by first computing x^m and then reducing modulo n.

Modular exponentiation

In coding and cryptography it's often necessary to compute powers of numbers modulo n; that is $x^m \pmod n$, where x, m and n may be integers with hundreds of digits.

$m = 10^{100}$ is a 1 followed by 100 zeroes (a googol).

Now if $x = 10$ then x^m is a 1 followed by 10^{100} zeros (and is called a googolplex).

It's estimated that there are around 10^{80} elementary particles in the universe:

so if x and m have over 100 digits then no computer, in the lifetime of the known universe, can possibly compute $x^m \pmod n$ by first computing x^m and then reducing modulo n.

Modular exponentiation

In coding and cryptography it's often necessary to compute powers of numbers modulo n; that is $x^m \pmod n$, where x, m and n may be integers with hundreds of digits.

$m = 10^{100}$ is a 1 followed by 100 zeroes (a googol).

Now if $x = 10$ then x^m is a 1 followed by 10^{100} zeros (and is called a googolplex).

It's estimated that there are around 10^{80} elementary particles in the universe:

so if x and m have over 100 digits then no computer, in the lifetime of the known universe, can possibly compute $x^m \pmod n$ by first computing x^m and then reducing modulo n.

Modular exponentiation

In coding and cryptography it's often necessary to compute powers of numbers modulo n; that is $x^m \pmod n$, where x, m and n may be integers with hundreds of digits.

$m = 10^{100}$ is a 1 followed by 100 zeroes (a googol).

Now if $x = 10$ then x^m is a 1 followed by 10^{100} zeros (and is called a googolplex).

It's estimated that there are around 10^{80} elementary particles in the universe:

so if x and m have over 100 digits then no computer, in the lifetime of the known universe, can possibly compute $x^m \pmod n$ by first computing x^m and then reducing modulo n.

Modular exponentiation using Maple

However, using the Maple command "`x&^m mod n;`" with

$$x = 584872422111233465340456456429056847639$$
$$246235844999349393999453003030030303020$$
$$27343242342376894734234234$$
$$m = 8958577747646664309968834761323540685 64$$
$$353545785698694543332456457643234523452$$
$$34443342327347823764563 45$$
$$n = 8878465667858868989969584635216457869 03$$
$$466534564564532899045672585898984567562$$
$$211104039772073403403003322342 34;$$

we obtain

$$x^m \pmod n = 8878465667858868989969584635216457869034$$
$$665345645645328990456725858989845675622 1$$
$$1104039772073403403003322342 34$$

Modular exponentiation using Maple

However, using the Maple command "`x&^m mod n;`" with

$$x = 584872422111233465340456456429056847639$$
$$246235844999349393999453003030030303020$$
$$27343242342376894734234234$$
$$m = 8958577747646664309968834761323540685 64$$
$$353545785698694543332456457643234523452$$
$$34443342327347823764563 45$$
$$n = 8878465667858868989969584635216457869 03$$
$$466534564564532899045672585898456756 2$$
$$211104039772073403403003322342 34;$$

we obtain

$$x^m \pmod n = 8878465667858868989969584635216457869034$$
$$66534564564532899045672585898456756221$$
$$11040397720734034030033223423 4$$

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$7^2 \equiv 49 \pmod{257}$$

It turns out that these powers of 7 can be combined to give 7^{329}.

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$7^2 \equiv 49 \pmod{257}$$
$$7^4 \equiv 49^2 \equiv 2401 \equiv 88 \pmod{257}$$

It turns out that these powers of 7 can be combined to give 7^{329}.

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$7^2 \equiv 49 \pmod{257}$$
$$7^4 \equiv 49^2 \equiv 2401 \equiv 88 \pmod{257}$$
$$7^8 \equiv 88^2 \equiv 7744 \equiv 34 \pmod{257}$$

It turns out that these powers of 7 can be combined to give 7^{329}.

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$7^2 \equiv 49 \pmod{257}$$
$$7^4 \equiv 49^2 \equiv 2401 \equiv 88 \pmod{257}$$
$$7^8 \equiv 88^2 \equiv 7744 \equiv 34 \pmod{257}$$
$$7^{16} \equiv 34^2 \equiv 1156 \equiv 128 \pmod{257}$$

It turns out that these powers of 7 can be combined to give 7^{329}.

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$7^2 \equiv 49 \pmod{257}$$
$$7^4 \equiv 49^2 \equiv 2401 \equiv 88 \pmod{257}$$
$$7^8 \equiv 88^2 \equiv 7744 \equiv 34 \pmod{257}$$
$$7^{16} \equiv 34^2 \equiv 1156 \equiv 128 \pmod{257}$$
$$7^{32} \equiv 128^2 \equiv 16384 \equiv 193 \pmod{257}$$

It turns out that these powers of 7 can be combined to give 7^{329}.

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$7^2 \equiv 49 \pmod{257}$$
$$7^4 \equiv 49^2 \equiv 2401 \equiv 88 \pmod{257}$$
$$7^8 \equiv 88^2 \equiv 7744 \equiv 34 \pmod{257}$$
$$7^{16} \equiv 34^2 \equiv 1156 \equiv 128 \pmod{257}$$
$$7^{32} \equiv 128^2 \equiv 16384 \equiv 193 \pmod{257}$$
$$7^{64} \equiv 193^2 \equiv 37249 \equiv 241 \pmod{257}$$

It turns out that these powers of 7 can be combined to give 7^{329}.

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$
\begin{aligned}
7^2 &\equiv 49 \pmod{257} \\
7^4 &\equiv 49^2 \equiv 2401 \equiv 88 \pmod{257} \\
7^8 &\equiv 88^2 \equiv 7744 \equiv 34 \pmod{257} \\
7^{16} &\equiv 34^2 \equiv 1156 \equiv 128 \pmod{257} \\
7^{32} &\equiv 128^2 \equiv 16384 \equiv 193 \pmod{257} \\
7^{64} &\equiv 193^2 \equiv 37249 \equiv 241 \pmod{257} \\
7^{128} &\equiv 241^2 \equiv 58081 \equiv 256 \pmod{257}.
\end{aligned}
$$

It turns out that these powers of 7 can be combined to give 7^{329}.

To see how this can be done consider the following computation of $7^{183} \pmod{257}$.

$$
\begin{aligned}
7^2 &\equiv 49 \pmod{257} \\
7^4 &\equiv 49^2 \equiv 2401 \equiv 88 \pmod{257} \\
7^8 &\equiv 88^2 \equiv 7744 \equiv 34 \pmod{257} \\
7^{16} &\equiv 34^2 \equiv 1156 \equiv 128 \pmod{257} \\
7^{32} &\equiv 128^2 \equiv 16384 \equiv 193 \pmod{257} \\
7^{64} &\equiv 193^2 \equiv 37249 \equiv 241 \pmod{257} \\
7^{128} &\equiv 241^2 \equiv 58081 \equiv 256 \pmod{257}.
\end{aligned}
$$

It turns out that these powers of 7 can be combined to give 7^{329}.

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.

In fact we can write 183 as a sum of powers of 2:

$$183 = 128 + 55$$

(This is essentially an algorithm for finding the binary expansion of 183.)

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.
In fact we can write 183 as a sum of powers of 2:

$$183 = 128 + 55$$

(This is essentially an algorithm for finding the binary expansion of 183.)

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.
In fact we can write 183 as a sum of powers of 2:

$$\begin{aligned} 183 &= 128 + 55 \\ &= 128 + 32 + 23 \end{aligned}$$

(This is essentially an algorithm for finding the binary expansion of 183.)

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.
In fact we can write 183 as a sum of powers of 2:

$$\begin{aligned} 183 &= 128 + 55 \\ &= 128 + 32 + 23 \\ &= 128 + 32 + 16 + 7 \end{aligned}$$

(This is essentially an algorithm for finding the binary expansion of 183.)

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.
In fact we can write 183 as a sum of powers of 2:

$$\begin{aligned} 183 &= 128 + 55 \\ &= 128 + 32 + 23 \\ &= 128 + 32 + 16 + 7 \\ &= 128 + 32 + 16 + 4 + 3 \end{aligned}$$

(This is essentially an algorithm for finding the binary expansion of 183.)

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.
In fact we can write 183 as a sum of powers of 2:

$$\begin{aligned} 183 &= 128 + 55 \\ &= 128 + 32 + 23 \\ &= 128 + 32 + 16 + 7 \\ &= 128 + 32 + 16 + 4 + 3 \\ &= 128 + 32 + 16 + 4 + 2 + 1 \end{aligned}$$

(This is essentially an algorithm for finding the binary expansion of 183.)

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.
In fact we can write 183 as a sum of powers of 2:

$$\begin{aligned} 183 &= 128 + 55 \\ &= 128 + 32 + 23 \\ &= 128 + 32 + 16 + 7 \\ &= 128 + 32 + 16 + 4 + 3 \\ &= 128 + 32 + 16 + 4 + 2 + 1 \\ &= 2^7 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0. \end{aligned}$$

(This is essentially an algorithm for finding the binary expansion of 183.)

This follows from the observation that $128 = 2^7$ is the largest power of 2 which is less than (or equal to) 183.
In fact we can write 183 as a sum of powers of 2:

$$\begin{aligned} 183 &= 128 + 55 \\ &= 128 + 32 + 23 \\ &= 128 + 32 + 16 + 7 \\ &= 128 + 32 + 16 + 4 + 3 \\ &= 128 + 32 + 16 + 4 + 2 + 1 \\ &= 2^7 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0. \end{aligned}$$

(This is essentially an algorithm for finding the binary expansion of 183.)

Therefore $183 = 128 + 32 + 16 + 4 + 2 + 1$ and

$$7^{183} \equiv 7^{128+32+16+4+2+1} \pmod{257}$$

All these computations are possible on a standard calculator but 7^{183} itself has over 150 digits.

Therefore $183 = 128 + 32 + 16 + 4 + 2 + 1$ and

$$\begin{aligned} 7^{183} &\equiv 7^{128+32+16+4+2+1} \pmod{257} \\ &\equiv 7^{128}7^{32}7^{16}7^{4}7^{2}7 \pmod{257} \end{aligned}$$

All these computations are possible on a standard calculator but 7^{183} itself has over 150 digits.

Therefore $183 = 128 + 32 + 16 + 4 + 2 + 1$ and

$$\begin{aligned} 7^{183} &\equiv 7^{128+32+16+4+2+1} \pmod{257} \\ &\equiv 7^{128}7^{32}7^{16}7^{4}7^{2}7 \pmod{257} \\ &\equiv 256 \cdot 193 \cdot 128 \cdot 88 \cdot 49 \cdot 7 \pmod{257} \end{aligned}$$

All these computations are possible on a standard calculator but 7^{183} itself has over 150 digits.

Therefore $183 = 128 + 32 + 16 + 4 + 2 + 1$ and

$$\begin{aligned} 7^{183} &\equiv 7^{128+32+16+4+2+1} \pmod{257} \\ &\equiv 7^{128}7^{32}7^{16}7^{4}7^{2}7 \pmod{257} \\ &\equiv 256 \cdot 193 \cdot 128 \cdot 88 \cdot 49 \cdot 7 \pmod{257} \\ &\equiv 190890377216 \pmod{257} \end{aligned}$$

All these computations are possible on a standard calculator but 7^{183} itself has over 150 digits.

Therefore $183 = 128 + 32 + 16 + 4 + 2 + 1$ and

$$\begin{aligned}
7^{183} &\equiv 7^{128+32+16+4+2+1} \pmod{257} \\
&\equiv 7^{128}7^{32}7^{16}7^{4}7^{2}7 \pmod{257} \\
&\equiv 256 \cdot 193 \cdot 128 \cdot 88 \cdot 49 \cdot 7 \pmod{257} \\
&\equiv 190890377216 \pmod{257} \\
&\equiv 175 \pmod{257}.
\end{aligned}$$

All these computations are possible on a standard calculator but 7^{183} itself has over 150 digits.

Therefore $183 = 128 + 32 + 16 + 4 + 2 + 1$ and

$$\begin{aligned} 7^{183} &\equiv 7^{128+32+16+4+2+1} \pmod{257} \\ &\equiv 7^{128}7^{32}7^{16}7^{4}7^{2}7 \pmod{257} \\ &\equiv 256 \cdot 193 \cdot 128 \cdot 88 \cdot 49 \cdot 7 \pmod{257} \\ &\equiv 190890377216 \pmod{257} \\ &\equiv 175 \pmod{257}. \end{aligned}$$

All these computations are possible on a standard calculator but 7^{183} itself has over 150 digits.

Computation of $x^m \pmod n$ by repeated squaring

1. Find the largest power of 2 less than or equal m: say $2^k \leq m < 2^{k+1}$.
2. Compute $x^2 \pmod n$, ..., $x^{2^k} \pmod n$, reducing modulo n each time.
3. Express m as a sum of powers of 2.
4. Compute $x^m \pmod n$ using the values $x^{2^i} \pmod n$.

Computation of $x^m \pmod{n}$ by repeated squaring

1. Find the largest power of 2 less than or equal m: say $2^k \leq m < 2^{k+1}$.
2. Compute $x^2 \pmod{n}$, ..., $x^{2^k} \pmod{n}$, reducing modulo n each time.
3. Express m as a sum of powers of 2.
4. Compute $x^m \pmod{n}$ using the values $x^{2^i} \pmod{n}$.

Computation of $x^m \pmod n$ by repeated squaring

1. Find the largest power of 2 less than or equal m: say $2^k \leq m < 2^{k+1}$.
2. Compute $x^2 \pmod n$, ..., $x^{2^k} \pmod n$, reducing modulo n each time.
3. Express m as a sum of powers of 2.
4. Compute $x^m \pmod n$ using the values $x^{2^i} \pmod n$.

Computation of $x^m \pmod n$ by repeated squaring

1. Find the largest power of 2 less than or equal m: say $2^k \leq m < 2^{k+1}$.
2. Compute $x^2 \pmod n$, ..., $x^{2^k} \pmod n$, reducing modulo n each time.
3. Express m as a sum of powers of 2.
4. Compute $x^m \pmod n$ using the values $x^{2^i} \pmod n$.

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$ we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$ we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

Example 5.11

Find the value of $11^{231} \pmod{391}$ (giving an answer between 0 and 390) .

Solution.

1. The largest power of 2 which is no greater than 231 is $2^7 = 128$.
2. Repeatedly squaring 11 and reducing modulo 391 we obtain ....
3. Writing $231 = 128 + 103 = 128 + 64 + 39 = 128 + 64 + 32 + 7 = 128 + 64 + 32 + 4 + 2 + 1$we have $11^{231} = 11^{128+64+32+4+2+1}$.
4. Combining the above ....

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

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9. \quad (5.2)$$

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

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9. \quad (5.2)$$

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

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9. \quad (5.2)$$

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

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9. \quad (5.2)$$

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

$$a_m a_{m-1} \cdots a_1 a_0 \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \pmod 9. \quad (5.2)$$

Casting out nines again

Suppose we cast out nines (Procedure 5.1) 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 (5.2), the result is an integer congruent to m modulo 9.

In Step 2 we add the digits and again, from (5.2), the result is an integer congruent to m modulo 9.

Casting out nines again

Suppose we cast out nines (Procedure 5.1) 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 (5.2), the result is an integer congruent to m modulo 9.

In Step 2 we add the digits and again, from (5.2), the result is an integer congruent to m modulo 9.

Casting out nines again

Suppose we cast out nines (Procedure 5.1) 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 (5.2), the result is an integer congruent to m modulo 9.

In Step 2 we add the digits and again, from (5.2), the result is an integer congruent to m modulo 9.

Casting out nines again

Suppose we cast out nines (Procedure 5.1) 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 (5.2), the result is an integer congruent to m modulo 9.

In Step 2 we add the digits and again, from (5.2), 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 $r \equiv m \pmod 9$.

As $9|m-r$, 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 of m by 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 $r \equiv m \pmod 9$.

As $9|m-r$, 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 of m by 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 $r \equiv m \pmod 9$.

As $9|m-r$, 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 of m by 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 $r \equiv m \pmod 9$.

As $9|m-r$, 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 of m by 9.

Divisibility by 9

The following lemma follows from (5.2).

Lemma 5.12

An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Example 5.13

Are either of 215763401 or 215743401 divisible by 9?

Divisibility by 9

The following lemma follows from (5.2).

Lemma 5.12

An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Example 5.13

Are either of 215763401 or 215743401 divisible by 9?

Divisibility by 9

The following lemma follows from (5.2).

Lemma 5.12

An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

Example 5.13

Are either of 215763401 or 215743401 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

$$939756564890843577455656873867 5 =$$

Divisibility by 4

Now $10^2 \equiv 0 \pmod 4$. Thus, for example,

$$1932526 = (19325 \times 100) + 26 \equiv 26 \pmod 4$$

and

$$939756564890843577455656873867 5 =$$

Divisibility by 4

Now $10^2 \equiv 0 \pmod 4$. Thus, for example,

$$1932526 = (19325 \times 100) + 26 \equiv 26 \pmod 4$$

and

$$939756564890843577455656873867 5 =$$
$$(939756564890843577455655687386 \times 100) + 75 \equiv 75 \pmod 4.$$

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

$$4 \mid a_m \cdots a_1 a_0 \Leftrightarrow 4 \mid a_1 a_0.$$

Example 5.14

Does 4 divide 937475900345 or 80345003732?

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

$$4 \mid a_m \cdots a_1 a_0 \Leftrightarrow 4 \mid a_1 a_0.$$

Example 5.14

Does 4 divide 937475900345 or 80345003732?

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

$$4 \mid a_m \cdots a_1 a_0 \Leftrightarrow 4 \mid a_1 a_0.$$

Example 5.14

Does 4 divide 937475900345 or 80345003732?

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

$$4 \mid a_m \cdots a_1 a_0 \Leftrightarrow 4 \mid a_1 a_0.$$

Example 5.14

Does 4 divide 937475900345 or 803450003732?

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

$$4 \mid a_m \cdots a_1 a_0 \Leftrightarrow 4 \mid a_1 a_0.$$

Example 5.14

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 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 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 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 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 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 5.15

Try to find the inverse of 2 modulo 6.

Example 5.16

Do either 3 or 7 have inverses modulo 10?

Example 5.17

Which numbers have inverses modulo 8?

Inverses modulo n

Example 5.15

Try to find the inverse of 2 modulo 6.

Example 5.16

Do either 3 or 7 have inverses modulo 10?

Example 5.17

Which numbers have inverses modulo 8?

Inverses modulo n

Example 5.15

Try to find the inverse of 2 modulo 6.

Example 5.16

Do either 3 or 7 have inverses modulo 10?

Example 5.17

Which numbers have inverses modulo 8?

Lemma 5.18

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 $\mathbb{Z}$.

Lemma 5.18

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 $\mathbb{Z}$.

Lemma 5.18

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 $\mathbb{Z}$.

Lemma 5.18

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 $\mathbb{Z}$.

Lemma 5.18

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 $\mathbb{Z}$.

Lemma 5.18

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 $\mathbb{Z}$.

Lemma 5.18

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 5.19

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.

Example 5.19

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 5.20

Find all integers x such that

$$6x \equiv 4 \pmod{8}. \tag{5.3}$$

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.

Solving Congruences

Example 5.20

Find all integers x such that

$$6x \equiv 4 \pmod{8}. \tag{5.3}$$

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.

Solving Congruences

Example 5.20

Find all integers x such that

$$6x \equiv 4 \pmod{8}. \tag{5.3}$$

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.

Solving Congruences

Example 5.20

Find all integers x such that

$$6x \equiv 4 \pmod{8}. \tag{5.3}$$

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.

Exhaustive search

x	0	1	2	3	4	5	6	7
$6x \pmod 8$								

From the table we see that the only solutions are $x = 2$ and $x = 6$.

Cancellation does not always work when solving congruences.

Exhaustive search

x	0	1	2	3	4	5	6	7
$6x \pmod 8$								

From the table we see that the only solutions are $x = 2$ and $x = 6$.

Cancellation does not always work when solving congruences.

Exhaustive search

x	0	1	2	3	4	5	6	7
$6x \pmod 8$								

From the table we see that the only solutions are $x = 2$ and $x = 6$.

Cancellation does not always work when solving congruences.

A method of solution

$$ax \equiv b \pmod{n} \tag{5.4}$$

x is a solution to (5.4) 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 2.5 this has a solution if and only if $\gcd(a,n)|b$.

Therefore, if $d = \gcd(a,n)$ then the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d|b$.

A method of solution

$$ax \equiv b \pmod{n} \tag{5.4}$$

x is a solution to (5.4) 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 2.5 this has a solution if and only if $\gcd(a,n)|b$.

Therefore, if $d = \gcd(a,n)$ then the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d|b$.

A method of solution

$$ax \equiv b \pmod{n} \tag{5.4}$$

x is a solution to (5.4) 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 2.5 this has a solution if and only if $\gcd(a,n)|b$.

Therefore, if $d = \gcd(a,n)$ then the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d|b$.

A method of solution

$$ax \equiv b \pmod{n} \tag{5.4}$$

x is a solution to (5.4) 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 2.5 this has a solution if and only if $\gcd(a,n)|b$.

Therefore, if $d = \gcd(a,n)$ then the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d|b$.

A method of solution

$$ax \equiv b \pmod{n} \tag{5.4}$$

x is a solution to (5.4) 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 2.5 this has a solution if and only if $\gcd(a,n)|b$.

Therefore, if $d = \gcd(a,n)$ then the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d|b$.

A method of solution

$$ax \equiv b \pmod{n} \tag{5.4}$$

x is a solution to (5.4) 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 2.5 this has a solution if and only if $\gcd(a,n)|b$.

Therefore, if $d=\gcd(a,n)$ then the congruence $ax \equiv b \pmod{n}$ has solutions if and only if $d|b$.

Finding all solutions to $ax \equiv b \pmod{n}$

If $d = \gcd(a,n) | b$ then we can use the Euclidean algorithm to find a particular solution to the equation

$$ax - ny = b. \qquad (*)$$

If $d|b$ and $x = u$, $y = v$ is a solution to the equation $(*)$

then the general solution is

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$.

So if $x = u$ is a particular solution to (5.4)
then the general solutions is

$$x = u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Finding all solutions to $ax \equiv b \pmod{n}$

If $d = \gcd(a,n) | b$ then we can use the Euclidean algorithm to find a particular solution to the equation

$$ax - ny = b. \qquad (*)$$

If $d|b$ and $x = u$, $y = v$ is a solution to the equation $(*)$

then the general solution is

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$.

So if $x = u$ is a particular solution to (5.4) then the general solutions is

$$x = u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Finding all solutions to $ax \equiv b \pmod{n}$

If $d = \gcd(a,n) | b$ then we can use the Euclidean algorithm to find a particular solution to the equation

$$ax - ny = b. \qquad (*)$$

If $d|b$ and $x = u$, $y = v$ is a solution to the equation $(*)$

then the general solution is

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$.

So if $x = u$ is a particular solution to (5.4) then the general solutions is

$$x = u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Finding all solutions to $ax \equiv b \pmod{n}$

If $d = \gcd(a,n) | b$ then we can use the Euclidean algorithm to find a particular solution to the equation

$$ax - ny = b. \qquad (*)$$

If $d|b$ and $x = u$, $y = v$ is a solution to the equation $(*)$

then the general solution is

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$.

So if $x = u$ is a particular solution to (5.4) then the general solutions is

$$x = u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Finding all solutions to $ax \equiv b \pmod{n}$

If $d = \gcd(a,n) | b$ then we can use the Euclidean algorithm to find a particular solution to the equation

$$ax - ny = b. \qquad (*)$$

If $d|b$ and $x = u$, $y = v$ is a solution to the equation $(*)$

then the general solution is

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$.

So if $x = u$ is a particular solution to (5.4) then the general solutions is

$$x = u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Finding all solutions to $ax \equiv b \pmod{n}$

If $d = \gcd(a,n) | b$ then we can use the Euclidean algorithm to find a particular solution to the equation

$$ax - ny = b. \qquad (*)$$

If $d|b$ and $x = u$, $y = v$ is a solution to the equation $(*)$

then the general solution is

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$.

So if $x = u$ is a particular solution to (5.4)
then the general solutions is

$$x = u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Finding all solutions to $ax \equiv b \pmod{n}$

If $d = \gcd(a,n) | b$ then we can use the Euclidean algorithm to find a particular solution to the equation

$$ax - ny = b. \qquad (*)$$

If $d|b$ and $x = u$, $y = v$ is a solution to the equation $(*)$

then the general solution is

$$x = u - (n/d)t$$

and

$$y = v - (a/d)t,$$

for $t \in \mathbb{Z}$.

So if $x = u$ is a particular solution to (5.4)
then the general solutions is

$$x = u - (n/d)t,$$

where t runs through the integers $\mathbb{Z}$.

Applying the method to congruence (5.3) above:

How many of the solutions to congruence (5.4) which we have found are congruent?

If $d|b$ and $x = u$ is one solution to the congruence (5.4)

then the list of solutions to (5.4) consists of the integers of the form

$$u - (n/d)t,$$

for $t \in \mathbb{Z}$.

Applying the method to congruence (5.3) above:

How many of the solutions to congruence (5.4) which we have found are congruent?

If $d|b$ and $x = u$ is one solution to the congruence (5.4)

then the list of solutions to (5.4) consists of the integers of the form

$$u - (n/d)t,$$

for $t \in \mathbb{Z}$.

Applying the method to congruence (5.3) above:

How many of the solutions to congruence (5.4) which we have found are congruent?

If $d|b$ and $x = u$ is one solution to the congruence (5.4)

then the list of solutions to (5.4) consists of the integers of the form

$$u - (n/d)t,$$

for $t \in \mathbb{Z}$.

Applying the method to congruence (5.3) above:

How many of the solutions to congruence (5.4) which we have found are congruent?

If $d|b$ and $x = u$ is one solution to the congruence (5.4)

then the list of solutions to (5.4) consists of the integers of the form

$$u - (n/d)t,$$

for $t \in \mathbb{Z}$.

Summary

Theorem 5.21

Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$.

Then the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

If $d \mid b$ then both the following hold.

(i) *There are exactly d pairwise incongruent solutions. (That is, solutions no two of which are congruent to each other.)*

(ii) *If x_0 is one solution then the complete list of (pairwise incongruent) solutions is*

$$x_0, x_0 + (n/d), x_0 + (2n/d), \cdots, x_0 + ([d-1]n/d).$$

That is, the solutions are precisely $x_0 + (tn/d)$, for $0 \leq t \leq d - 1$.

Summary

Theorem 5.21

Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$.

Then the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

If $d \mid b$ then both the following hold.

(i) *There are exactly d pairwise incongruent solutions. (That is, solutions no two of which are congruent to each other.)*

(ii) *If x_0 is one solution then the complete list of (pairwise incongruent) solutions is*

$$x_0, x_0 + (n/d), x_0 + (2n/d), \cdots, x_0 + ([d-1]n/d).$$

That is, the solutions are precisely $x_0 + (tn/d)$, for $0 \leq t \leq d - 1$.

Summary

Theorem 5.21

Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$.

Then the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

If $d \mid b$ then both the following hold.

(i) *There are exactly d pairwise incongruent solutions. (That is, solutions no two of which are congruent to each other.)*

(ii) *If x_0 is one solution then the complete list of (pairwise incongruent) solutions is*

$$x_0, x_0 + (n/d), x_0 + (2n/d), \cdots, x_0 + ([d-1]n/d).$$

That is, the solutions are precisely $x_0 + (tn/d)$, for $0 \leq t \leq d - 1$.

Summary

Theorem 5.21

Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$.

Then the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

If $d \mid b$ then both the following hold.

(i) *There are exactly d pairwise incongruent solutions. (That is, solutions no two of which are congruent to each other.)*

(ii) *If x_0 is one solution then the complete list of (pairwise incongruent) solutions is*

$$x_0, x_0 + (n/d), x_0 + (2n/d), \cdots, x_0 + ([d-1]n/d).$$

That is, the solutions are precisely $x_0 + (tn/d)$, for $0 \leq t \leq d - 1$.

Summary

Theorem 5.21

Let a, b and n be integers with $n > 0$ and let $d = \gcd(a, n)$.

Then the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

If $d \mid b$ then both the following hold.

(i) *There are exactly d pairwise incongruent solutions. (That is, solutions no two of which are congruent to each other.)*

(ii) *If x_0 is one solution then the complete list of (pairwise incongruent) solutions is*

$$x_0, x_0 + (n/d), x_0 + (2n/d), \cdots, x_0 + ([d-1]n/d).$$

That is, the solutions are precisely $x_0 + (tn/d)$, for $0 \leq t \leq d - 1$.

Example 5.22

Find all solutions to the congruence

$$2x \equiv 3 \pmod{6}.$$

Example 5.23

Find all solutions to the congruence $6x \equiv 9 \pmod{15}$.

Example 5.22

Find all solutions to the congruence

$$2x \equiv 3 \pmod{6}.$$

Example 5.23

Find all solutions to the congruence $6x \equiv 9 \pmod{15}$.

Cancellation again

Example 5.24

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.

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/.

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/.

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/.

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/.

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.

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.

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.

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.

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.

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 5.25

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

$$13, 26, 32, 4, 28, 36, 12, 4, 28, 36, 12.$$

Example 5.25

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

$$13, 26, 32, 4, 28, 36, 12, 4, 28, 36, 12.$$

Example 5.25

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

$$13, 26, 32, 4, 28, 36, 12, 4, 28, 36, 12.$$

Example 5.25

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.

Theorem 5.26

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.

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 5.26

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.

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 5.26

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.

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 5.26

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.

Of course such sequences are not random (by definition) and we have a formula for the terms.

Theorem 5.26

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 5.8 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.