A Level Further Mathematics for OCR A
Additional Pure Student Book (AS/A Level)
John Sykes
Contents

Introduction

How to use this resource

1 Sequences and series
   Section 1: Recurrence relations, properties of sequences, Fibonacci and related numbers
   Section 2: Solving recurrence relations
   Mixed practice 1

2 Number theory
   Section 1: Number bases
   Section 2: Divisibility tests
   Section 3: Modular (or finite) arithmetic
   Section 4: Prime numbers
   Mixed practice 2

3 Groups
   Section 1: Binary operations
   Section 2: Definition of a group
   Section 3: Subgroups, cyclic groups, isomorphism and structure of groups
   Mixed practice 3

Cross-topic review exercise 1

4 Further vectors
   Section 1: Vector product
   Mixed practice 4

5 Surfaces and partial differentiation
   Section 1: Three-dimensional (3-D) surfaces
   Section 2: Partial differentiation
   Section 3: Stationary points
   Section 4: Tangent planes
   Mixed practice 5

6 Further calculus
   Section 1: Integration by reduction
   Section 2: Arc lengths and surface areas
   Mixed practice 6

Cross-topic review exercise 2

Practice paper

Formulae
1 Sequences and series

In this chapter you will learn how to:

- work with general sequences
- use induction to prove results relating to sequences and series
- describe behaviour of sequences
- use the limits of sequences
- work with Fibonacci and Lucas numbers
- solve first-order recurrence relations
- solve second-order recurrence relations.

Before you start...

You should be able to use the following formulae for geometric progressions:

- \( n \text{th term of a G. P.} = a \times r^{n-1} \)
- \( S_n = \frac{a(1 - r^n)}{1 - r} \)
- \( S_{\infty} = \frac{a}{1 - r} \)

1. Given that a sequence has terms 3, 12, 48, 192 find:
   - a the tenth term
   - b the sum of the first 5 terms.

2. Given that a sequence has terms \( \frac{4}{3}, \frac{8}{9}, \ldots \) find
   - a the 6th term
   - b the sum of the first 10 terms
   - c the sum to infinity.

3. Prove by induction that the sum of the first \( n \) integers is \( \frac{1}{2}n(n + 1) \).
Section 1: Recurrence relations, properties of sequences, Fibonacci and related numbers

**Key point 1.1**

A **sequence** is a list of terms.

A **series** is the sum of the terms.

The terms of a sequence may be defined as:

- **recurrence relation**, e.g. \( u_{n+1} = u_n + 3, \) \( u_1 = 2 \).
- **position-to-term formula**, e.g. \( u_n = 2n + 3 \).

**Induction** may be used to prove results relating to both sequences and series.

**Behaviour of sequences:**

- **Periodic**: terms of the sequence are repeated, e.g. 1, 3, 2, 1, 3, 2, 1, 3, 2, ...
- **Oscillating**: periodic with two terms, e.g. 1, 2, 1, 2, 1, 2, ...
- **Convergent**: the terms of the sequence get closer to some limiting value;
  the sum of the terms of the sequence has a finite value.
- **Divergent**: not convergent and the sum of the sequence is not finite.
- **Monotonic**: a sequence is strictly monotonic increasing if each term is larger than or the same as the previous one, i.e. \( u_{n+1} \geq u_n \), and monotonic decreasing if each term is less than the previous one, i.e. \( u_{n+1} < u_n \).

**Particular sequences**

- **Fibonacci numbers**: \( u_{n+2} = u_{n+1} + u_n, \) \( u_1 = 1, u_2 = 1 \).
  The ratio of each term to the previous one converges to \( \phi \).
  \[ \phi = \frac{1 + \sqrt{5}}{2}. \]
  \( \phi \) is the **Golden ratio**.
- **Lucas numbers**: \( u_{n+2} = u_{n+1} + u_n, \) \( u_1 = 1, u_2 = 3 \).
a Write down the first five terms of the sequence defined by \( u_{n+1} = u_n + 3 \), \( u_1 = 5 \).

b Find the position-to-term rule for the sequence 10, 16, 22, 28, … which has \( n \)th term \( t_n \).

c Describe the relationship between \( u_n \) and \( t_n \).

d Describe the behaviour of these sequences.

\[
a \quad u_1 = 5, u_2 = u_1 + 3 = 8, u_3 = u_2 + 3 = 11, \ldots
\]

Sequence is: 5, 8, 11, 14, …

\[
b \quad 10, 16, 22, 28, \ldots \text{ has first difference } 6
\]

\[. \quad t_n = 6n + 4
\]

\[↑ \quad \text{First difference}
\]

\[
c \quad t_n = 2u_n
\]

d Both sequences are monotonic increasing.

WORKED EXAMPLE 1.2

A sequence is defined by \( u_{n+2} = 3u_{n+1} - 2u_n \) with \( u_1 = 1 \) and \( u_2 = 3 \).

Prove by induction that \( u_n = 2^n - 1 \) for all positive integers \( n \).

When \( n = 1 \) \( \quad \text{LHS} = u_1 = 1 \),

\( \quad \text{RHS} = 2^1 - 1 = 1 \). Hence it is true for \( n = 1 \).

When \( n = 2 \) \( \quad \text{LHS} = u_2 = 3 \),

\( \quad \text{RHS} = 2^2 - 1 = 3 \). Hence it is true for \( n = 3 \).

Assume true for \( n = k \), i.e. \( u_k = 2^k - 1 \) and true for \( n = k + 1 \),

\( \quad \text{i.e. } u_{k+1} = 2^{k+1} - 1 \).

For \( n = k + 2 \):

\[\text{This is the standard method for induction:}\]

check true for initial conditions

assume true for \( n = k \) and \( n = k + 1 \)

show true for \( n = k + 2 \)
\[ u_{k+2} = 3u_{k+1} - 2u_k = 3(2^{k+1} - 1) - 2(2^k - 1) \]
\[ = 3 \times 2^{k+1} - 2 \times 2^k - 1 \]
\[ = 3 \times 2 \times 2^k - 2 \times 2^k - 1 \]
\[ = 4 \times 2^k - 1 = 2^2 \times 2^k - 1 \]
\[ = 2^{k+2} - 1 \]

Hence it is true for \( n = k + 1 \) and so it is true for all positive integers \( n \).

hence true for all positive integers.

Rewind

The method of induction was covered in Pure Core Student Book 1, Chapter 6.

WORKED EXAMPLE 1.3

Consider the sequences \( u_n = \frac{1}{2^{n-1}} \) and \( t_n = \frac{1}{n} \).

a Write down the first five terms of each sequence.

b State the value to which each sequence converges.

c Find the sum of the first five terms and the sum to infinity of each sequence.

d Describe each sequence.

\[ a_1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16} \text{ and } t_1, t_2, t_3, t_4, t_5 \]

b They both converge to 0.

As \( n \to \infty \), \( \frac{1}{n} \to 0 \)

Substituting \( n = 1, 2, 3, \ldots \)

\[ r = \frac{1}{2} \]

\[ s_5 = \frac{a(1 - r^n)}{1 - r} = \frac{1 \times \left( 1 - \left( \frac{1}{2} \right)^5 \right)}{1 - \left( \frac{1}{2} \right)} = \frac{31}{16} \]
and \( S_\infty = \frac{a}{1-r} = \frac{1}{1 - \left(\frac{1}{2}\right)} = 2. \)

\( t_n \) is not geometric:

\[
t_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} = \frac{137}{60}
\]

and the sum to infinity \( = \infty \)

\textbf{d} \text{ } \( u_n \) is monotonic decreasing and convergent.

\( t_n \) is monotonic decreasing and divergent and it is called the harmonic series.

**Tip**

Do not confuse \( u_n \) with \( n. \) \( u_n \) is the value of the term, \( n \) is the position of the term.
1. Find the recurrence relation for each of these sequences.
   a. 6, 9, 12, 15, 18, ...
   b. 22, 18, 14, 10, 6, ...
   c. 3, 9, 21, 45, 93, ...
   d. 18, 10, 6, 4, 3, ...

2. For each of these sequences state the position-to-term rule.
   a. 2, 7, 12, 17, 22, ...
   b. 1, 4, 16, 64, 256, ...
   c. 4, 7, 12, 19, 28, ...
   d. \[\frac{1}{3}, \frac{3}{5}, \frac{5}{7}, \frac{7}{9}, \frac{9}{11}, \ldots\]

3. For each of the following recurrence relations, write down the first five terms of the sequence and find a position-to-term formula.
   a. \[u_{n+1} = 3u_n, \quad u_1 = 1\]
   b. \[u_{n+1} = 2u_n, \quad u_1 = 3\]
   c. \[u_{n+1} = u_n + 2, \quad u_1 = 1\]
   d. \[u_{n+1} = 4u_n - 3, \quad u_1 = 2\]

4. For each of the following position-to-term formulae, write down the first five terms of the sequence and find a recurrence relation.
   a. \[t_n = 3n - 1\]
   b. \[t_n = 5n + 2\]
   c. \[t_n = 2^{n+1} - 1\]
   d. \[t_n = 2 \times 3^n - 1\]

5. The Fibonacci sequence is defined by \[u_{n+2} = u_{n+1} + u_n, \quad u_1 = 1, \quad u_2 = 1\].
   a. Find the first eight terms of the sequence.
   b. Find the first seven terms of the sequence obtained by taking the differences between consecutive terms of the Fibonacci sequence.
   c. Write down the first seven terms of the sequence obtained by dividing each term of the Fibonacci sequence by its previous term.
   d. A rectangle has area 1 square unit. Its length is \(x\) and its width is \(x - 1\).
   d. Form a quadratic equation in \(x\) and solve it to find the value of \(x\).
6. Find out the name of this number. Evaluate the first six terms, i.e. \( u_1 \) to \( u_6 \), of
\[
 u_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right)
\]

7. The Lucas sequence is defined by \( u_{n+2} = u_{n+1} + u_n \), \( u_1 = 1 \), \( u_2 = 3 \).
   a. Find the first six numbers of the sequence.

   The \( n \)th Lucas numbers is denoted by \( L_n \) and the \( n \)th Fibonacci number is denoted by \( F_n \).
   b. Verify that:
      i. \( L_n = F_{n-1} + F_{n+1} \)
      ii. \( L_n = 2F_n + F_{n-1} \)
      iii. \( F_{2n} = L_nF_n \)

8. The terms of a sequence are given by \( u_n = 5 + (-1)^n \times 3 \).
   a. Calculate the values of the terms \( u_1 \) to \( u_6 \).
   b. Describe the behaviour of the series.
   
   Repeat the question for:
   c. \( u_n = 5 + (-3)^n \times 3 \)
   d. \( u_n = 5 + \left( -\frac{1}{3} \right)^n \times 3 \)

9. Describe the sequence given by \( u_n = 2\sin(90n^\circ) \).

10. A sequence of terms is given by \( u_{n+1} = u_n^2 - 6 \).
   a. If \( u_1 = 2 \), find \( u_{50} \) and describe the sequence.
   b. Find another value of \( u_1 \) that leads to a fixed point sequence.
   c. Determine the behaviour of the sequence if:
      i. \( u_1 = 4 \)
      ii. \( u_1 = \sqrt{6} \)

11. a. The sequence \( u_1, u_2, u_3, \ldots \) is 9, 12, 15, 18, 21, …
    
    Find the position-to-term rule for this sequence.
b The sequence \( t_1, t_2, t_3, \ldots \) is 4, 7, 10, 13, 16…

Find the recurrence relation for this sequence.

c Hence find \( t_{100} \).

d Describe the sequence given by \( u_n - t_n \) for all positive integers \( n \).

The sequence \( u_1, u_2, u_3, \ldots \) is defined by \( u_0 = 0, u_1 = 1 \) and \( u_n = 2u_{n-1} + u_{n-2} \).

a Evaluate \( u_2, u_3 \) and \( u_4 \) and verify that \( u_5 = 29 \).

The sequence \( t_1, t_2, t_3, \ldots \) is defined by \( t_0 = 2, t_1 = 2 \) and \( t_n = 2t_{n-1} + t_{n-2} \).

b Evaluate \( t_2, t_3 \) and \( t_4 \) and verify that \( t_5 = 82 \).

The sequence \( v_1, v_2, v_3, \ldots \) is defined by \( v_n = \frac{t_n}{2u_n} \).

c Find \( v_1, v_2, v_3 \) and \( v_4 \), expressing your answers as fractions, and verify that \( v_5 = \frac{41}{29} \).

d By writing your answers to question part c as decimals, suggest the value to which this sequence of terms is converging.

(The sequence \( u_1, u_2, u_3, \ldots \) gives the Pell numbers. The sequence \( t_1, t_2, t_3, \ldots \) gives the Pell–Lucas numbers.)

A sequence is defined by \( u_{n+1} = 4u_n \), with \( u_1 = 1 \).

Prove by induction that \( u_n = 4^{n-1} \) for all positive integers \( n \).

Verify that your proof is valid for the first five terms of each sequence.

A sequence is defined by \( u_{n+1} = 5u_n - 4 \), with \( u_1 = 2 \).

Prove by induction that \( u_n = 5^{n-1} + 1 \) for all positive integers \( n \).

Verify that your proof is valid for the first five terms of each sequence.

A sequence is defined by \( u_{n+1} = 3u_n + 1 \), with \( u_1 = 1 \).

Prove by induction that \( u_n = \frac{1}{2} (3^n - 1) \) for all positive integers \( n \).

Verify that your proof is valid for the first five terms of each sequence.

a Write down the first five terms of \( u_{n+1} = 2u_n + 3n \), with \( u_1 = 2 \).

b Write down the first five terms of \( u_n = 4 \times 2^n - 3n - 3 \).

c Prove by induction that the sequence defined by \( u_{n+1} = 2u_n + 3n \), with \( u_1 = 2 \) has \( u_n = 4 \times 2^n - 3n - 3 \).
The sequence \( u_1, u_2, u_3, \ldots \) is defined by \( u_1 = 2 \) and \( u_{n+1} = 2u_n - 1 \).

Prove by induction that \( u_n = 2^{n-1} + 1 \).

The sequence \( u_1, u_2, u_3, \ldots \) is defined by \( u_1 = 1 \) and \( u_{n+1} = u_n + 2n + 1 \).

a) Show that \( u_4 = 16 \).

b) Hence suggest an expression for \( u_n \).

c) Use induction to prove that your answer to part (b) is correct.

The sequence \( u_1, u_2, u_3, \ldots \) is defined by \( u_1 = 3 \) and \( u_{n+1} = 3u_n - 2 \).

a) Find \( u_2 \) and \( u_3 \) and verify that \( \frac{1}{2}(u_4 - 1) = 27 \).

b) Hence suggest an expression for \( u_n \).

c) Use induction to prove that your answer to part (b) is correct.

The sequence \( u_1, u_2, u_3, \ldots \) is defined by \( u_1 = 2 \) and \( u_{n+1} = \frac{u_n}{u_n + 1} \) for \( n \geq 1 \).

a) Find \( u_2 \) and \( u_3 \) and show that \( u_4 = \frac{2}{7} \).

b) Hence suggest an expression for \( u_n \).

c) Use induction to prove that your answer to part (b) is correct.
Explore

The image at the start is mostly obscured! It would be better to put an image of the full Mandelbrot set WITH this explore and refer to it directly.
So, the Explore would begin:
This is an image of the Mandelbrot set, which is a geometric fractal, that is, a set of points in the complex plane that have different colours according to an algorithm. Investigate how fractals can be used to describe and simulate naturally occurring objects and phenomena.

Section 2: Solving recurrence relations

First-order recurrence relations
Key point 1.2

A **linear recurrence relation** is one in which each term of a sequence is a linear function of a previous term or terms, e.g. \( u_{n+1} = 2u_n + 3 \).

**Homogeneous**: a first-order recurrence relation is homogeneous if it is of the form \( u_{n+1} = ku_n \).

**Non-homogeneous**: a first-order recurrence relation is non-homogeneous if it is of the form \( u_{n+1} = ku_n + f(n) \). (\( f(n) \) will be polynomial or of the form \( a \times b^n \).)

**Closed form solution**: a solution in position-to-term form, i.e. \( u_n \), is written in terms of \( n \) and not referring to previous terms.

**Recurrence system**: a system consists of the recurrence relation (e.g. \( u_{n+1} = 2u_n + 3 \)), an initial condition (e.g. \( u_1 = 4 \)) and a range of the variable \( n \).

**Method**

The solution is made up of two parts: the **complementary function** \( c(n) \) and the **particular solution** \( p(n) \).

Consider the first-order recurrence relation \( u_{n+1} = ku_n + f(n) \).

Start with the **reduced equation** \( u_{n+1} = ku_n \) and replace \( u_n \) by \( r^n \) (where \( r \) is a non-zero constant). This gives the **auxiliary** (or characteristic) equation. Solving this gives a value for \( r \).

The complementary function is then \( c_n = A \times r^n \).

Next find the particular solution \( p(n) \) by replacing \( f(n) \) by a general function of the same form:

<table>
<thead>
<tr>
<th>( f(n) )</th>
<th>let ( p(n) ) be</th>
</tr>
</thead>
<tbody>
<tr>
<td>number, e.g. 3</td>
<td>( a )</td>
</tr>
<tr>
<td>linear, e.g. 2( n ) + 3</td>
<td>( an + b )</td>
</tr>
<tr>
<td>quadratic, e.g. ( n^2 ) + 2( n ) + 3</td>
<td>( an^2 + bn + c )</td>
</tr>
<tr>
<td>power, e.g. 2 ( \times 3^n )</td>
<td>( a \times 3^n )</td>
</tr>
</tbody>
</table>

where the constants \( a, b \) and \( c \) are found by substitution into the full equation.

Note: the **failure case** is when \( f(n) \) is of the same form as the complementary function. In this situation, multiply \( p(n) \) by \( n \).
Finally, the general (closed form) solution is \( u_n = c_n + p_n \).

The final solution is found by applying the boundary condition to determine \( A \).

(The method is comparable with one used for solving first-order differential equations.)

**Rewind**

You learned how to solve first-order differential equations in A Level Mathematics Student Book 2, Chapter 13.

WORKED EXAMPLE 1.4

Solve the recurrence relation \( u_{n+1} = 2u_n \) with \( u_1 = 1 \).

Reduced equation: \( u_{n+1} = 2u_n \)  
No \( f(n) \) term.

Auxiliary equation: \( r^{n+1} = 2r^n \)  
\( \Rightarrow r = 2 \)

Complementary function: \( c_n = A \times 2^n \)  
There is no \( f(n) \) term.

The general solution is \( u_n = A \times 2^n \).

Final solution:  
substituting \( u_1 = 1 \)  
\( \Rightarrow A = \frac{1}{2} \)

\( \therefore u_n = \frac{1}{2} \times 2^n = 2^{n-1} \)

WORKED EXAMPLE 1.5

Solve the recurrence relation \( u_{n+1} = 2u_n + 5 \) with \( u_0 = 1 \).

Complementary function: \( c_n = A \times 2^n \)  
Same as Worked example 1.4.

Particular solution: Let \( p_n = a \)  
Substitute \( p_n = u_n = a \) in the full equation.

\( \therefore a = 2a + 5 \)  
\( \Rightarrow a = -5 \)

so \( p_n = -5 \)

Since \( p_n = a \).
**General solution:** \( u_n = A \times 2^n - 5 \)

**Final solution:** substituting \( u_0 = 1 \)

\[ \therefore 1 = A - 5 \Rightarrow A = 6 \]

\[ \therefore u_n = 6 \times 2^n - 5 \]

**Check:**

\( u_{n+1} = 2u_n + 5 \) with \( u_0 = 1 \)

\[ \Rightarrow 1, 7, 19, 43, 91, \ldots \]

\( u_n = 6 \times 2^n - 5 \)

\[ \Rightarrow 1, 7, 19, 43, 91, \ldots \]

It is wise to check the answers.

---

**WORKED EXAMPLE 1.6**

Solve the recurrence relation \( u_{n+1} = 2u_n + 3n \), with \( u_0 = 1 \).

**Complementary function:** \( c_n = A \times 2^n \)

Same as Worked example 1.4.

**Particular solution:** let \( p_n = an + b \),

\[ \therefore a(n + 1) + b = 2(an + b) + 3n \]

Coefficients of \( n \): \( a = 2a + 3 \Rightarrow a = -3 \)

Numbers: \( a + b = 2b \Rightarrow b = -3 \)

**General solution:** \( u_n = c_n + p_n = A \times 2^n - 3n - 3 \)

**Final solution:** substituting \( u_0 = 1 \)

\[ \therefore 1 = A - 0 - 3 \Rightarrow A = 4 \]

\[ \therefore u_n = 4 \times 2^n - 3n - 3 \]

**Check:**

\( u_{n+1} = 2u_n + 3n \) with \( u_0 = 1 \)

\[ \Rightarrow 1, 7, 20, 49, \ldots \]

\( u_n = 4 \times 2^n - 3n - 3 \)

\[ \Rightarrow 1, 7, 20, 49, \ldots \]

It is wise to check the answers.
Tip

When finding $c_n$ you substitute $u_n = r^n$, $u_{n+1} = r^{n+1}$…

When finding $p_n$ you replace, for example, $u_n$ with $an + b$ and $u_{n+1}$ with $a(n+1) + b$…

Do not confuse these and put $u_n = an + b$ and $u_{n+1} = a(n+1) + b$ when finding $c_n$.

WORKED EXAMPLE 1.7

Solve the recurrence relation $u_{n+1} = 2u_n + 3^n$, with $u_0 = 1$.

Complementary function: $c_n = A \times 2^n$

Particular solution: let $u_n = a \times 3^n$

$\therefore a \times 3^{n+1} = 2a \times 3^n + 3^n$
$\therefore 3a \times 3^n = (2a + 1) \times 3^n$
$\therefore 3a = 2a + 1$
$\therefore a = 1$ so $p_n = 3^n$

General solution: $u_n = A \times 2^n + 3^n$

Final solution: substituting $u_0 = 1$

$\therefore 1 = A + 1 \Rightarrow A = 0$
$\therefore u_n = 3^n$

Check:
$u_{n+1} = 2u_n + 3^n$ with $u_0 = 1$
$\Rightarrow 1, 3, 9, 27, 81, …$
$u_n = 3^n$
$\Rightarrow 1, 3, 9, 27, 81, …$

It is wise to check the answers.

Failure case

WORKED EXAMPLE 1.8

Solve the recurrence relation $u_{n+1} = 2u_n + 3 \times 2^n$, with $u_0 = 1$. 
Complementary function: \( c_n = A \times 2^n \)

Particular solution:

let \( u_n = a \times n \times 2^n \)

\[
\Rightarrow 2a(n + 1) \times 2^{n+1} = 2an \times 2^n + 3 \times 2^n
\]

\[
\Rightarrow 2a(n + 1) = 2an + 3
\]

\[
\Rightarrow 2a = 3 \quad \text{and} \quad p_n = \frac{3}{2} n \times 2^n
\]

General solution: \( u_n = A \times 2^n + \frac{3}{2} n \times 2^n \)

\[
\Rightarrow u_n = \left( A + \frac{3}{2} n \right) \times 2^n
\]

Final solution: substituting \( u_0 = 1 \)

\[
\Rightarrow 1 = A \Rightarrow A = 1
\]

\[
\Rightarrow u_n = \left( 1 + \frac{3}{2} n \right) \times 2^n
\]

or \( u_n = (2 + 3n) \times 2^{n-1} \)

Check:

\( u_{n+1} = 2u_n + 3 \times 2^n \) with \( u_0 = 1 \)

\[
\Rightarrow 1, 5, 16, 44, 112, \ldots
\]

\[
\Rightarrow u_n = (2 + 3n) \times 2^{n-1}
\]

\[
\Rightarrow 1, 5, 16, 44, 112, \ldots
\]

It is common to miss noticing a failure case: in which case, \( a \) cannot be found (you obtain the equation \( 1 = 1 \)).

This tells you to reflect on your solution and recognise whether or not it is the failure case.

See worked example 1.4.

Putting \( u_n = a \times 2^n \) gives the same form as \( c_n \) (i.e. failure case) so substitute \( p_n = u_n = a \times n \times 2^n \) in the full equation.

Note: if \( u_n = a \times n \times 2^n \), then \( u_{n+1} = a \times (n + 1) \times 2^{n+1} \).

Solve.

Using \( u_n = c_n + p_n \).

Apply boundary conditions.

It is wise to check the answers.

Second-order recurrence relations
Key point 1.3

A **second-order recurrence relation** is one in which each term of a sequence is a linear function of two previous term or terms, e.g. \( u_{n+2} = u_{n+1} + 2u_n + 3 \).

**Homogeneous**: a second-order recurrence relation is homogeneous if it is of the form 
\[ u_{n+2} = k_1u_{n+1} + k_2u_n \]
where \( k_1 \) and \( k_2 \) are constants.

**Non-homogeneous**: a second-order recurrence relation is non-homogeneous if it is of the form 
\[ u_{n+2} = k_1u_{n+1} + k_2u_n + f(n) \]  
(\( f(n) \) will be polynomial or of the form \( a \times b^n \).)

**Method**

As with first-order recurrence relations, the solution is given by the sum of the complementary function \( c(n) \) and the particular solution \( p(n) \), i.e. \( u_n = c_n + p_n \).

Consider the second-order recurrence relation 
\[ u_{n+2} = k_1u_{n+1} + k_2u_n + f(n) \]

Start with the reduced equation 
\[ u_{n+2} = k_1u_{n+1} + k_2u_n \]
and replace \( u_n \) by \( r^n \). This gives the auxiliary (or characteristic) equation. Solving this gives values \( r_1 \) and \( r_2 \).

To find the complementary function:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complementary Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>real and distinct roots ( r_1 ) and ( r_2 )</td>
<td>( c_n = Ar_1^n + Br_2^n )</td>
</tr>
<tr>
<td>repeated real roots (i.e. ( r_1 = r_2 ))</td>
<td>( c_n = (A + Bn)r_1^n )</td>
</tr>
<tr>
<td>complex roots ( z_1 ) and ( z_2 )</td>
<td>( c_n = Az_1^n + Bz_2^n )</td>
</tr>
</tbody>
</table>

Next find the particular solution \( p(n) \) by replacing \( f(n) \) as for solving first-order relations.

Again, for the failure case, multiply \( p(n) \) by \( n \).

Finally, the general (closed form) solution is 
\[ u_n = c_n + p_n \]

The final solution is found by applying the boundary conditions to determine \( A \) and \( B \).

The solution is **stable** if it converges to a fixed value (which is usually zero) and this happens if and only if \( |r_1| < 1 \) and \( |r_2| < 1 \).

[The method is comparable with one used for solving second-order differential equations.]
Rewind

You will have solved second-order differential equations in Pure Core Student Book 2, Chapter 11.

WORKED EXAMPLE 1.9

Solve the second-order recurrence relation $u_{n+2} = 5u_{n+1} - 6u_n$, with $u_1 = 1$ and $u_2 = 5$.

Reduced equation:

$u_{n+2} - 5u_{n+1} + 6u_n = 0$

Auxiliary equation:

$r^{n+2} - 5r^{n+1} + 6r^n = 0$

$r^2 - 5r + 6 = 0$

$(r - 2)(r - 3) = 0$

$\Rightarrow r = 2$ or $r = 3$

Complementary function:

$c_n = A \times 2^n + B \times 3^n$

The general solution is

$u_n = A \times 2^n + B \times 3^n$

Final solution: substituting

$u_1 = 1 \Rightarrow 1 = 2A + 3B$ (i)

$u_2 = 5 \Rightarrow 5 = 4A + 9B$ ... (ii)

(ii) − 3(i) $\Rightarrow 2 = -2A$

$\therefore A = -1$ and $B = 1$

Hence $u_n = 3^n - 2^n$

Check:

$u_{n+2} = 5u_{n+1} - 6u_n$, with $u_1 = 1$ and $u_2 = 5$

$\Rightarrow 1, 5, 19, 65, 211, ...$

$u_n = 3^n - 2^n$

$\Rightarrow 1, 5, 19, 65, 211, ...$

Check the answers.
WORKED EXAMPLE 1.10

Solve the second-order recurrence relation \( u_{n+2} = 5u_{n+1} - 6u_n + 2n + 1 \) with \( u_1 = 4 \) and \( u_2 = 3 \).

Reduced equation: \( u_{n+2} - 5u_{n+1} + 6u_n = 0 \)

So the complementary function is \( c_n = A \times 2^n + B \times 3^n \).

Particular solution: let \( u_n = an + b \)

\[ \begin{align*}
   a(n + 2) + b &= 5(a(n + 1) + b) - 6(an + b) + 2n + 1 \\
   \text{coefficients of } n & : a = 5a - 6a + 2 \Rightarrow a = 1 \\
   \text{numbers: } 2a + b &= 5a + 5b - 6b + 1 \Rightarrow b = 2 \\
   \text{Hence: } p_n &= n + 2
\end{align*} \]

The general solution is \( u_n = A \times 2^n + B \times 3^n + n + 2 \).

Final solution: substituting

\[ \begin{align*}
   u_1 &= 4 \Rightarrow 4 = 2A + 3B + 3 \ldots (i) \\
   u_2 &= 3 \Rightarrow 3 = 4A + 9B + 4 \ldots (ii) \\
   3(i) - (ii) & \Rightarrow 9 = 2A + 5 \\
   \text{Hence: } u_n &= 2 \times 2^n - 3^n + n + 2 \\
   \text{or } u_n &= 2^{n+1} - 3^n + n + 2 \\
\end{align*} \]

Check:

\[ \begin{align*}
   u_{n+2} &= 5u_{n+1} - 6u_n + 2n + 1, \text{ with } u_1 = 4 \text{ and } u_2 = 3 \\
   \Rightarrow 4, 3, -6, -43, -172, \ldots
\end{align*} \]

\[ \begin{align*}
   u_n &= 2^{n+1} - 3^n + n + 2 \\
   \Rightarrow 4, 3, -6, -43, -172, \ldots
\end{align*} \]

WORKED EXAMPLE 1.11

Solve the second-order recurrence relation \( u_{n+2} = 8u_{n+1} - 16u_n + 3^n \) with \( u_1 = 6 \) and \( u_2 = 25 \).

Reduced equation is found by putting \( f(n) = 0 \).

Same as Worked example 1.9.

Substitute \( p_n = u_n = an + b \) in the full equation. Note: if \( u_n = an + b \), then \( u_{n+1} = a(n + 1) + b \).

Apply boundary conditions.

Using \( u_n = c_n + p_n \).

Check the answers.
Reduced equation: \( u_{n+2} - 8u_{n+1} + 16u_n = 0 \)

Auxiliary equation: \( r^2 - 8r + 16 = (r - 4)^2 = 0 \)
\[ \therefore r = 4 \text{ (equal roots)} \]

The complementary function is:
\[ c_n = (A + Bn) \times 4^n \]

Particular solution: let \( u_n = a \times 3^n \)
\[ a \times 3^{n+2} = 8a \times 3^{n+1} - 16a \times 3^n + 3^n \]
\[ 9a = 24a - 16a + 1 \]
\[ a = 1 \text{ Hence: } p_n = 3^n \]

The general solution is \( u_n = (A + Bn) \times 4^n + 3^n \).

Final solution: substituting
\[ u_1 = 6 \Rightarrow 6 = 4A + 4B + 3 \text{ (i)} \]
\[ u_2 = 25 \Rightarrow 25 = 16A + 32B + 9 \ldots \text{ (ii)} \]
\[ 8(i) - (ii) \Rightarrow 23 = 16A + 15 \]
\[ \therefore A = \frac{1}{2} \text{ and } B = \frac{1}{4} \]

Hence
\[ u_n = \left( \frac{1}{2} + \frac{1}{4}n \right)4^n + 3^n \]
\[ = (2 + n)4^{n-1} + 3^n \]

Check:
\[ u_n + 2 = 8u_{n+1} - 16u_n + 3^n \text{, with } u_1 = 6 \text{ and } u_2 = 33 \]
\[ \Rightarrow 6, 25, 107, 465, 2035, \ldots \]
\[ u_n = (2 + n)4^{n-1} + 3^n \]
\[ \Rightarrow 6, 25, 107, 465, 2035, \ldots \]

\[ \text{Check the answers.} \]

WORKED EXAMPLE 1.12

Solve the second-order recurrence relation \( u_{n+2} = 4u_{n+1} - 13u_n + 20 \) with \( u_1 = 3 - i \) and \( u_2 = 5 - i \).

Reduced equation: \( u_{n+2} - 4u_{n+1} + 13u_n = 0 \) \[ \text{Put } f(n) = 0. \]

Replace \( u_n \) by \( r^n \) and simplify.

Using \( c_n = (A + Bn)r_n \).

Substitute \( p_n = u_n = a \times 3^n \) in the full equation.

Note: if \( u_n = a \times 3^n \), then:
\[ u_{n+1} = a \times 3^{n+1} = a \times 3^n \times 3. \]

Solve.

Using \( u_n = c_n + p_n \).

Apply boundary conditions.

Check:
\[ u_n + 2 = 8u_{n+1} - 16u_n + 3^n, \text{ with } u_1 = 6 \text{ and } u_2 = 33 \]
\[ \Rightarrow 6, 25, 107, 465, 2035, \ldots \]
\[ u_n = (2 + n)4^{n-1} + 3^n \]
\[ \Rightarrow 6, 25, 107, 465, 2035, \ldots \]

Check the answers.
Auxiliary equation becomes: \( r^2 - 4r + 13 = 0 \)

\[
4 \pm \sqrt{16 - 4 \times 13} \over 2 = 2 \pm 3i
\]

The complementary function is: \( c_n = A(2 + 3i)^n + B(2 - 3i)^n \)

Particular solution: let \( u_n = a \)

\[
a = 4a - 13a + 20 \quad \therefore \quad a = 2
\]

Hence: \( p_n = 2 \)

The general solution is \( u_n = A(2 + 3i)^n + B(2 - 3i)^n + 2 \).

Final solution: substituting

\[
\begin{align*}
  u_1 &= 3 - i \Rightarrow 3 - i = A(2 + 3i) + 4(2 - 3i) + 2 \ldots \text{(i)} \\
  u_2 &= 5 - i \Rightarrow 5 - i = A(-5 + 12i) + 4(-5 - 12i) + 2 \ldots \text{(ii)} \\
  \text{(i)} \times (-5 + 12i) - \text{(ii)} \times (2 + 3i) &\Rightarrow -2 + 10i = 78i B \\
  \therefore \quad B &= \frac{1}{39}(5 + i) \text{ and } A = \frac{1}{39}(-2 - 10i)
\end{align*}
\]

Hence \( u_n = \frac{1}{39}(-2 - 10i)(2 + 3i)^n + \frac{1}{39}(5 + i)(2 - 3i)^n + 2 \)

Check:

Substituting \( n = 1 \) gives \( 3 - i \).

Substituting \( n = 2 \) gives \( 5 - i \).

WORKED EXAMPLE 1.13

Solve the second-order recurrence relation \( u_{n+2} = u_{n+1} + 2u_n + 18 \times 2^n \), with \( u_1 = 4 \) and \( u_2 = 8 \).

Reduced equation: \( u_n + 2 - u_{n+1} - 2u_n = 0 \)

Auxiliary equation: \( r^2 - r - 2 = 0 \)

\[
(r + 1)(r - 2) = 0
\]

\( \Rightarrow r = -1 \text{ or } r = 2 \)

Complementary function: \( c_n = A(-1)^n + B \times 2^n \)

Particular solution: failure case so let \( u_n = an \times 2^n \)

\[
a(n + 2) \times 2^{n+2} = a(n + 1) \times 2^{n+1} + 2an \times 2^n + 2^n
\]

Replace \( u_n \) by \( r^n \) and simplify.

Using \( c_n = Az_1^n + Bz_2^n \)

Substitute \( p_n = u_n = a \).

Solve.

Using \( u_n = c_n + p_n \).

Apply boundary conditions.

Put \( f(n) = 0 \).

Replace \( u_n \) by \( r^n \) and simplify.

Using \( c_n = Ar_1^n + Br_2^n \).
4a(n + 2) = 2a(n + 1) + 2an + 18

6a = 18

Hence: $p_n = 3n \times 2^n$

The general solution is

$u_n = A \times (-1)^n + B \times 2^n + 3n \times 2^n$

Final solution: substituting

$u_1 = 4 \Rightarrow 4 = -A + 2B + 6 \text{ (i)}$

$u_2 = 8 \Rightarrow 8 = A + 4B + 24 \ldots \text{ (ii)}$

(i) + (ii) $\Rightarrow 12 = 6B + 30$

$\therefore B = -3$ and $A = -4$

Hence $u_n = -4 \times (-1)^n - 3 \times 2^n + 3n \times 2^n$

or $u_n = -4 \times (-1)^n + 3(n-1) \times 2^n$

Check:

$u_{n+2} = u_{n+1} + 2u_n + 18 \times 2^n$ with $u_1 = 4$ and $u_2 = 8$

$\Rightarrow \ 4, 8, 52, 140, 388, \ldots$

$u_n = -4 \times (-1)^n + 3(n-1) \times 2^n$

$\Rightarrow \ 4, 8, 52, 140, 388, \ldots$

Putting $u_n = a \times 2^n$ gives the same form as $c_n$ (i.e. failure case) so put

$p_n = u_n = a \times n \times 2^n$ in the full equation.

Note: if $u_n = a \times n \times 2^n$, then

$u_{n+1} = a \times (n + 1) \times 2^{n+1}$. Solve.

Using $u_n = c_n + p_n$.

Apply boundary conditions.

Check the answers.

EXERCISE 1B
1 Solve the following first-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+1} = u_n + 5, u_1 = 2 \)

b \( u_{n+1} = u_n + 4, u_1 = -5 \)

c \( u_{n+1} = u_n - 3, u_1 = 4 \)

d \( u_{n+1} = 6 - u_n, u_1 = 3 \)

2 Solve the following first-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+1} = 2u_n - 3, u_1 = 4 \)

b \( u_{n+1} = 3u_n + 2, u_1 = 3 \)

c \( u_{n+1} = 5u_n + 1, u_1 = 1 \)

d \( u_{n+1} = 9 - 3u_n, u_1 = 1 \)

3 Solve the following first-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+1} = u_n + 2n + 5, u_1 = 2 \)

b \( u_{n+1} = 2u_n + n + 4, u_1 = 1 \)

c \( u_{n+1} = 5u_n + 2n - 4, u_1 = 3 \)

d \( u_{n+1} = 6 + 9n - 2u_n, u_1 = 1 \)

4 Solve the following first-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+1} = u_n + n^2 + n + 1, u_1 = 3 \)

b \( u_{n+1} = u_n + 2n^2 + 3n + 4, u_1 = 2 \)

c \( u_{n+1} = 2u_n + n^2 + 2n + 1, u_1 = 1 \)

d \( u_{n+1} = 6 + 5n - 3n^2 + 3u_n, u_1 = 0 \)

5 Solve the following first-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+1} = u_n + 3^n, \text{ with } u_1 = 2 \)

b \( u_{n+1} = 3u_n + 2^n, \text{ with } u_1 = 1 \)

c \( u_{n+1} = 2u_n - (-1)^n, u_1 = 0 \)

d \( u_{n+1} = 3u_n - (-2)^n, u_1 = -1 \)
Solve the following first-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+1} = 2u_n + 2^n \), with \( u_1 = 3 \)

b \( u_{n+1} = 4u_n + 3 \times 4^n \), with \( u_1 = 1 \)

c \( u_{n+1} = \left(\frac{1}{2}\right)^n + \frac{1}{2}u_n, u_1 = 1 \)

d \( u_{n+1} = \frac{1}{3}n + \frac{1}{3}u_n, u_1 = 0 \)

In 2017 the population of the United Kingdom is taken to be 66 million people. The annual growth rate is 0.6\%. In addition, it is expected that the net immigration will be 150000 people per year.

Set up a recurrence system to model the population and solve it to estimate the number of people in \( n \) years' time. Show that the population of the United Kingdom in 2022 will be 68.8 million people.

The population of red squirrels in a large wood is found to be decreasing by a constant rate of 10\% each year. To overcome this, a conservancy group introduce 6 squirrels a year. At the moment, there are believed to be 48 squirrels.

a Using the first model, set up a recurrence relation and solve it to find the population in four years' time. What would this model predict for the population growth over time?

b In a second model, the recurrence relation is \( p_{n+1} = \text{INT}[0.9 \times p_n] + 6 \), where \( \text{INT}[x] \) is the integer value of \( x \) (i.e. the whole number part). Use this model to determine the population in four years' time. What would this second model predict for the population growth over time?

The Tower of Hanoi is a problem involving three rods and a number of disks of different sizes. Only one disk is moved at a time and it is placed on the top of any disks of a larger size on any other rod. The purpose is to reconstruct the pile of disks on another rod.

Obtain a recurrence system for \( n \) disks and find a general solution. Show that for three disks the puzzle can be solved in seven moves.

Solve the following second-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+2} = 4u_{n+1} - 3u_n, u_1 = 1, u_2 = 7 \)

b \( u_{n+2} = u_{n+1} + 6u_n, u_1 = 8, u_2 = 14 \)

c \( u_{n+2} = 6u_{n+1} - 8u_n, u_1 = 2, u_2 = 20 \)

d \( u_{n+2} = 8u_{n+1} - 15u_n, u_1 = 10, u_2 = 60 \)
Solve the following second-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a  \( u_{n+2} = 6u_{n+1} - 9u_n, u_1 = 1, u_2 = 4 \)

b  \( u_{n+2} = 10u_{n+1} - 25u_n, u_1 = 2, u_2 = 5 \)

c  \( u_{n+2} = u_{n+1} - 0.25u_n, u_1 = 1, u_2 = 2 \)

d  \( 9u_{n+2} = 12u_{n+1} - 4u_n, u_1 = 3, u_2 = 6 \)

Solve the following second-order recurrence equations. Check your solutions by calculating the first two terms of the solution.

a  \( u_{n+2} = 2u_{n+1} - 2u_n, u_1 = 5 - i, u_2 = -2i \)

b  \( u_{n+2} = 8u_{n+1} - 41u_n, u_1 = 24, u_2 = -54 \)

c  \( u_{n+2} = 6u_{n+1} - 13u_n, u_1 = 15 + 6i, u_2 = 25 + 36i \)

d  \( u_{n+2} = 10u_{n+1} - 29u_n, u_1 = 35 + 2i, u_2 = 147 + 20i \)

Solve the following second-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a  \( u_{n+2} = 7u_{n+1} - 12u_n + 18, u_1 = 2, u_2 = 4 \)

b  \( u_{n+2} = u_{n+1} + 6u_n + 12, u_1 = 1, u_2 = 2 \)

c  \( u_{n+2} = 9u_{n+1} - 20u_n - 24, u_1 = 0, u_2 = 3 \)

d  \( u_{n+2} = u_{n+1} + 20u_n - 40, u_1 = 26, u_2 = 86 \)

Solve the following second-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a  \( u_{n+2} = u_{n+1} + 6u_n + 6n - 7, u_1 = 1, u_2 = 2 \)

b  \( u_{n+2} = 2u_{n+1} + 3u_n + 4n + 12, u_1 = -1, u_2 = 16 \)

c  \( u_{n+2} = 4u_{n+1} - 4u_n + 2n + 6, u_1 = 2, u_2 = 10 \)

d  \( u_{n+2} = 6u_{n+1} - 10u_n + 25n - 10, u_0 = 8, u_1 = 21 + 6i \)

Solve the following second-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a  \( u_{n+2} = u_{n+1} + 6u_n + 12n^2 - 10n + 1, u_1 = 3, u_2 = -2 \)

b  \( u_{n+2} = 2u_{n+1} + 15u_n - 16n^2 - 64n + 50, u_1 = 9, u_2 = 68 \)

c  \( u_{n+2} + 2u_{n+1} + u_n = 4n^2 + 16n + 18, u_1 = -1, u_2 = 17 \)

d  \( u_{n+2} + 2u_{n+1} + 2u_n = 10n^2 + 11n + 33, u_0 = 7, u_1 = 4 \)
Solve the following second-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+2} = u_{n+1} + 6u_n + 12 \times 4^n, u_0 = 2, u_1 = 3 \)

b \( u_{n+2} = 4u_{n+1} + 5u_n + 27 \times 2^n, u_1 = -5, u_2 = 17 \)

c \( 2u_{n+2} = 5u_{n+1} - 2u_n - 5 \times 3^n, u_1 = 5, u_2 = 4 \)

d \( u_{n+2} = 10u_{n+1} - 25u_n - 2 \times 6^n, u_1 = 23, u_2 = 203 \)

Solve the following second-order recurrence equations. Check your solutions by writing down the first five terms of the original relation and of its solution.

a \( u_{n+2} = u_{n+1} + 6u_n + 5 \times 3^n, u_0 = 2, u_1 = 2 \)

b \( u_{n+2} = 8u_{n+1} - 12u_n + 24 \times 2^n, u_1 = 12, u_2 = 60 \)

c \( u_{n+2} = 2u_{n+1} + 3u_n + 12 \times 3^n, u_1 = 10, u_2 = 35 \)

d \( u_{n+2} = 4u_{n+1} - 4u_n + 4 \times 2^n, u_1 = 1, u_2 = 2 \)

Show that the solution of the Fibonacci recurrence system \( u_{n+2} = u_{n+1} + u_n \) with \( u_1 = 1 \) and \( u_2 = 1 \) is Binet’s formula:

\[
\frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right)
\]

Obtain a similar solution for the Lucas recurrence system \( L_{n+2} = L_{n+1} + L_n \) with \( L_1 = 1 \) and \( L_2 = 3 \) and verify that your answer gives \( L_4 = 7 \).

Show that the recurrence system \( u_{n+2} = u_{n+1} + u_n \) with \( u_1 = 1 \) and \( u_2 = 2 \) has solution:

\( u_n = 2^n - 1 \)

Prove by induction that the result is correct.

The number 1331 is a palindrome as it is the same when read forwards or backwards. Similarly, we can find all the integer sums for a particular number and determine the number of palindromes. For example, 3 can be written as 3 or 1 + 1 + 1, that is, in two palindromic ways. Similarly 5 can be written as 5, 1 + 3 + 1, 1 + 1 + 1 + 1 + 1, that is, in three palindromic ways.

Find the number of palindromic ways in which each of the numbers 1 to 6 can be written and write down a recurrence relation satisfying the results.

Show that the solution is:

\[
\left( \frac{1}{2} + \frac{1}{2\sqrt{2}} \right) \left( \sqrt{2} \right)^n + \left( \frac{1}{2} - \frac{1}{2\sqrt{2}} \right) \left( -\sqrt{2} \right)^n
\]
Checklist of learning and understanding

Sequences:

- Recurrence relations are term to term rules of the form \( u_{n+1} = 2u_n + 3, \ u_1 = 4 \).
- Position-to-term rules take the form \( u_n = 2n + 3 \).

Behaviour of sequences:

- Periodic is where terms of the sequence are repeated.
- Oscillating is periodic with two terms.
- Convergent is where the terms of the sequence get closer to some limiting value.
- Divergent is when the sequence is not convergent and the sum of the sequence is not finite.
- A series is monotonically increasing (or decreasing) when each term is larger (or smaller) than the previous one.

Fibonacci and Lucas numbers:

- The Fibonacci recurrence relation is \( u_{n+2} = u_{n+1} + u_n, u_1 = 1, u_2 = 1 \).
- The Fibonacci sequence is \( 1, 1, 2, 3, 5, 8, \ldots \).
- The ratio of each term to its previous one converges to the Golden Ratio \( \varphi \).
- The Golden ratio \( \varphi = \frac{1 + \sqrt{5}}{2} \).
- The Lucas numbers are generated from the recurrence relation \( u_{n+2} = u_{n+1} + u_n, u_1 = 1, u_2 = 3 \).
- The Lucas sequence is \( 1, 3, 4, 7, 11, 18, \ldots \).

First order recurrence relations:

- A first order linear relation is one in which each term of the sequence is a linear function of a previous term such as \( u_{n+1} = ku_n + f(n) \).
- A first order recurrence relation is homogeneous if it is of the form \( u_{n+1} = ku_n \).
- Solutions are made up of complementary function \( c(n) \) and a particular solution \( p(n) \).
- To find \( c(n) \) replace \( u_n \) by \( r^n \) in the reduced equation \( u_{n+1} = ku_n \) then put \( c_n = A \times r^n \).
- To find \( p(n) \) replace \( f(n) \) by a function of the same form.
- The general solution is \( c(n) + p(n) \).
- Apply the boundary conditions to find any constants.

Second order recurrence relations:
A second order linear relation is one in which each term of the sequence is a linear function of two previous terms, e.g. \(u_{n+2} = k_1 u_{n+1} + k_2 u_n + f(n)\).

A second order recurrence relation is homogeneous if it is of the form

\[u_{n+2} = k_1 u_{n+1} + k_2 u_n.\]

Solutions are made up of complementary function \(c(n)\) and a particular solution \(p(n)\).

To find \(c(n)\) replace \(u_n\) by \(r^n\) in the reduced equation \(u_{n+1} = ku_n\) to give the auxiliary (or characteristic) equation.

If the auxiliary equation has real roots then \(c(n) = Ar_1^n + Br_2^n\).

If the auxiliary equation has equal roots then \(c(n) = (A + Bn)r^n\).

If the auxiliary equation has complex roots \(z_1\) and \(z_2\) then \(c(n) = c_n = Az_1^n + Bz_2^n\).

To find \(p(n)\) replace \(f(n)\) by a function of the same form.

The general solution is \(c(n) + p(n)\).

Apply the boundary conditions to find any constants.

**Mixed practice 1**

1. A sequence \( \{u_n\} \) is defined by \(u_{n+1} = 5u_n\) with \(u_1 = 1\).
   
   a. Given that \(u_n = 5^{n-1}\), show that \(u_1 = 1\).
   
   b. Using \(u_k = 5^{k-1}\), show that \(u_{k+1} = 5 \times 5^{k-1}\).
   
   c. Prove by induction that \(u_n = 5^{n-1}\) for all positive integers \(n\).
   
   d. Verify that your proof is valid for the first three terms of each sequence.

2. The sequence \( \{u_n\} \) is defined by \(u_{n+1} = 3u_n + 2\) with \(u_1 = 3\).
   
   a. If \(u_k = 4 \times 3^{k-1} - 1\), verify that \(u_1 = 3\) and show that \(u_{k+1} = 4 \times 3^k - 1\).
   
   b. Prove by induction that \(u_k = 4 \times 3^{k-1} - 1\).
   
   c. Show that \(u_6\) is divisible by 5.

3. A sequence has recurrence relation \(u_{n+1} = 2u_n + n + 5\), \(u_1 = 3\).
   
   a. By putting \(u_n = an + b\), show that the particular solution is \(p_n = -n - 6\).
   
   b. Solve the recurrence relation to show that \(u_n = 5 \times 2^n - n - 6\).
c Explain why the terms of the sequence \( \{u_n\} \) are odd when \( n \) is odd and even when \( n \) is even.

4 a Solve the recurrence relation \( u_{n+1} = 5u_n + 5^n \), with \( u_1 = 3 \).

b Prove your answer is correct by induction.

5 The population of fish in a pond is decreasing by 40% each year through fishing. Each year the pond is re-stocked by having an extra \( n \) fish added. The initial population \( P_0 \) of fish is 5000.

a Write down an equation to model the population \( P_t \) of fish in \( t \) years’ time in terms of \( P_{t-1} \).

b Solve this equation to find the population \( P_t \) in terms of \( t \) and \( n \).

c Find the value of \( n \) to maintain a constant number of fish at the start of each year.

d If \( n = 3000 \) find the number of fish there will be at the end of the tenth year.

6 A second order recurrence equation is

\[ u_{n+2} = 6u_{n+1} - 8u_n + 6n + 4, \quad u_1 = 1, \quad u_2 = 2 \]

a By writing \( u_n \) as \( r^n \) show that the complementary function is \( c_n = A \times 2^n + B \times 4^n \).

b Show that the particular solution is \( p_n = 2n + 4 \).

c Hence find the solution of the recurrence relation.

7 Solve the second order recurrence equations

\[ u_{n+2} = 10u_{n+1} - 25u_n + 18 \times 2^n, \quad u_1 = 2, \quad u_2 = 3 \]

8 Solve the second order recurrence equations

\[ u_{n+2} = 2u_{n+1} - 10u_n + 27, \quad u_0 = 4, \quad u_1 = 4 + 9i \]

9 Find, in terms of the constant \( k \), the general solution of:

\[ u_{n+2} = ku_{n+1} + u_n \]

It is given that \( u_0 = 1, \quad u_1 = 1 \).

Solve the recurrence equation for:

a \( k = 1 \), showing your answer is in terms of the golden ratio \( \frac{1 + \sqrt{5}}{2} \)

b \( k = 2 \), showing your answer is in terms of the silver ratio \( 1 + \sqrt{2} \)

10 In a tactical game the number of points a player scores in a session is 5 times the previous score minus six times the score before that plus 4 times the number of the
In this chapter you will learn how to:

- understand and be able to work with number bases
- use divisibility tests
- use the division algorithm
- understand and use finite (modular) arithmetic
- solve linear congruences
- solve simultaneous linear congruences
- calculate quadratic residues and solve equations using them
- understand prime numbers
- use Euclid’s lemma
- use Fermat’s little theorem

**Session.**

Show that, after \( n \) sessions, the score \( u_n \) is given by:

\[
u_n = 5u_{n-1} - 6u_{n-2} + 4n\]

After the first session the player has 21 points. After the second he has 41 points.

Solve the recurrence relation and find the number of sessions played for the score to exceed 1000.

11 Solve \( u_{n+3} = 9u_{n+2} - 26u_{n+1} + 24u_n + 12n + 2 \) given that \( u_0 = 0, u_1 = 2 \) and \( u_2 = 6 \).

Show that your solution and the recurrence relation both give \( u_4 = -58 \).

12 In chaos theory, the quadratic recurrence relation \( z = z^2 + c \) is used.

Depending on the long-term behaviour of \( c \) and the starting value of \( z \) the position of the coordinates of \( z \) in the complex plain is coloured by a specific colour. This leads to such diagrams as those named after Julia or Mandelbrot.

An attractor is a number to which the iteration converges.

a  Put \( c = -0.5 \) and investigate what happens when (i) \( x > 1 \), (ii) \( 0 < x \leq 1 \).

b  Repeat (i) with \( c = -1 \).

c  Repeat (i) with \( c = -1.3 \).

d  Repeat (i) with \( c = -1.5 \).
Before you start…

<table>
<thead>
<tr>
<th>GCSE</th>
<th>You should be able to divide by single and double digit numbers. Division to include long division:</th>
</tr>
</thead>
</table>
|      | 1. Without a calculator:  
|      | a. Divide 11571 by 7.  
|      | b. Divide 90893 by 11. |

<table>
<thead>
<tr>
<th>GCSE</th>
<th>You should be able to carry out long multiplication.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Without a calculator multiply 5132 by 17.</td>
</tr>
</tbody>
</table>

| GCSE | You should be able to find prime factors of a number.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3. Express 24 as a product of its prime factors.</td>
</tr>
</tbody>
</table>

| A Level Mathematics Student Book 1, Chapter 9 | You should know the binomial expansion.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4. Find the binomial expansion of ((1 - 2x)^5).</td>
</tr>
</tbody>
</table>
integer $n$ is:

$$(a + b)^p$$

$$= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{r}a^{p-r}b^r + \ldots + b^p$$

Section 1: Number bases

Key point 2.1

Decimal numbers are numbers to the base 10.
The decimal number $2013 = 2 \times 10^3 + 0 \times 10^2 + 1 \times 10 + 3 \times 1$.
For a base $n$, $2013_n = 2 \times n^3 + 0 \times n^2 + 1 \times n + 3 \times 1$.
Further, $2013.584_n = 2 \times n^3 + 0 \times n^2 + 1 \times n + 3 \times 1 + 5 \times n^{-1} + 8 \times n^{-2} + 4 \times n^{-3}$.

We shall consider numbers with bases from 2 to 16.
In numbers up to base 16, we use $A \equiv 10$, $B \equiv 11$, $C \equiv 12$, $D \equiv 13$, $E \equiv 14$, $F \equiv 15$.

Decimal numbers have digits 0 to 9.
Binary numbers have digits 0 and 1.
Hexadecimal numbers have digits 0 to F.
Numbers to base $n$ have digits 0 to $n-1$.
Base 2 is called binary and base 16 is hexadecimal (both used in computing).

WORKED EXAMPLE 2.1

Convert the hexadecimal number $31E$ to a decimal number.

$$31E_{16} = 3 \times 16^2 + 1 \times 16 + 14 \times 1 = 798$$

$E$ is in the units column, 1 is in the $16s$ column and 3 is in the $16^2$ column.

WORKED EXAMPLE 2.2
Convert the decimal $45$ to binary (base $2$).

**Method 1:** consider powers of $2$, i.e.

$1, 2, 4, 8, 16, 32.$

So $45 = 1 \times 32 + 0 \times 16 + 1 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1$

i.e. $45 \equiv 101101_2$

**Method 2:** repeatedly divide by $2$

So $45 \div 2 = 22 \ \text{r} \ 1$

$22 \div 2 = 11 \ \text{r} \ 0$

$11 \div 2 = 5 \ \text{r} \ 1$

$5 \div 2 = 2 \ \text{r} \ 1$

$2 \div 2 = 1 \ \text{r} \ 0$

$1 \div 2 = 0 \ \text{r} \ 1$

Reading the sequence from the bottom to the top gives $45 \equiv 101101_2$.

Check:

e.g.

$101101_2 = 1 \times 32 + 1 \times 8 + 1 \times 4 + 1 \times 1 = 45_{10}$

which is correct.

**Tip**

It is a common error to write the number in the reverse order.

**WORKED EXAMPLE 2.3**

Convert $275_8$ to base $5$.

First convert $275_8$ to decimal

$= 2 \times 8^2 + 7 \times 8 + 5 \times 1 = 189$

Now convert $189$ to base $5$

Use the powers of $8$.

Use Method 2 as in Worked example 2.2.
189 ÷ 5 = 37 r 4
37 ÷ 5 = 7 r 2
7 ÷ 5 = 1 r 2
1 ÷ 5 = 0 r 1
∴ 2758 ≡ 12245

WORKED EXAMPLE 2.4

Find $1101_2 + 1011_2$, giving your answer in base 2.

WORKED EXAMPLE 2.5

Find $132_6 \times 215_6$, giving your answer in base 6.

Tip

Always convert the numbers to the base being used. In Worked example 2.5 it is a common error to write $5 \times 2 = 10$ rather than $5 \times 2 = 14_6$.

WORKED EXAMPLE 2.6

Calculate $14232_5 \div 31_5$.

Check your answer by converting the numbers to decimals.
Working in base 5.

\[
\begin{array}{c}
411 \\
31 \overline{23241} \\
224 \\
34 \\
31 \\
31 \\
\end{array}
\]

Or

Convert to base 10:

\[23241_5 \equiv 2 \times 625 + 3 \times 125 + 2 \times 25 + 4 \times 5 + 1 = 1696\]

and \[31_5 = 3 \times 5 + 1 = 16\]

do the division then convert back to base 5:

\[1696 \div 16 = 106 \equiv 411_5\]
1 Convert the following numbers to decimal numbers:
   a $314_5$
   b $10110_2$
   c $7A_{16}$
   d $374_8$
   e $32231_4$
   f $B2A3_{12}$

2 Write the following numbers as binary numbers (base 2):
   a 9
   b 15
   c 43
   d 150
   e 54
   f 21.5

3 Change the following numbers to base 5:
   a 19
   b 34
   c 100
   d 156
   e 500
   f 54.04

4 Convert the following numbers to hexadecimal numbers (base 16):
   a 25
   b 31
   c 356
   d 255
   e 10000
   f 20.75

5 Find the following numbers as numbers in base 7:
6 Convert the numbers to the base given:
   a 135_6 to base 8
   b 19B_{16} to base 12
   c 538_9 to base 4
   d CAB_{13} to base 11
   e 153_6 to base 3
   f 518_9 to base 5

7 Do the following calculations in the base given. You may wish to check your answers by
   converting to decimal numbers and back again.
   a 10101_2 + 1101_2
   b 325_6 + 143_6
   c 265_8 + 375_8
   d 9A_{16} + B6_{16}

8 Carry out the following calculations in the base given. You may wish to check your answers
   by converting to decimal numbers and back again.
   a 2112_3 - 1211_3
   b 5312_7 - 666_7
   c 3131_5 - 1313_5
   d B6_{13} - 1A_{13}

9 Evaluate the following products, giving your answers to the same base as that in the
   question. You may wish to check your answers by converting to decimal numbers and back
   again.
   a 11011_2 \times 110_2
   b 312_4 \times 23_4
c  \(729_{11} \times 85_{11}\)

d  \(444_5 \times 44_5\)

10. Do the following divisions writing your answers in the given base. You may wish to check your answers by converting to decimal numbers and back again.

a  \(110001_2 \div 111_2\)

b  \(345_7 \div 21_7\)

c  \(3200_4 \div 13_4\)

d  \(1B38_{16} \div 1A_{16}\)

11. Carry out the following calculations:

a  \(1101_2 + 312_4\) giving your answers in base 8

b  \(324_6 + 222_3\) giving your answers in base 9

c  \(8A_{12} + 67_8\) giving your answers in base 4

d  \(342_5 + 243_6\) giving your answers in base 7.

12. Carry out the following calculations:

a  \(512_6 - 210_3\) giving your answers in base 9

b  \(241_9 - 345_6\) giving your answers in base 3

c  \(8B_{12} - 63_8\) giving your answers in base 4

d  \(241_{10} - 241_5\) giving your answers in base 8.

13. Carry out the following calculations:

a  \(111_2 \times 222_3\) giving your answers in base 4

b  \(AA_{11} \times 31_7\) giving your answers in base 9

c  \(416_3 \times 34_5\) giving your answers in base 3

d  \(412_7 \times 24_9\) giving your answers in base 8.

14. Carry out the following calculations:

a  \(B8_{12} \div 13_4\) giving your answers in base 8

b  \(214_9 \div 31_8\) giving your answers in base 6

c  \(286_9 \div 11_{14}\) giving your answers in base 5

d  \(279_{11} \div 105_6\) giving your answers in base 2.
To convert binary numbers to hexadecimal, break up the string into groups of four digits (starting from the right). Convert each group of four digits to a hexadecimal. Concatenate the hexadecimal digits to give the answer.

a Convert $11010101_2$ to hexadecimal.

b Convert $11110101110111_2$ to hexadecimal.

c Convert $753_{16}$ to binary.

d Convert $AC9_{16}$ to binary.

Apply the same idea developed in question 15 to these problems:

a Convert $101111010_2$ to octal

b Convert $11110011101_2$ to octal

c Convert $657_8$ to binary

d Convert $7075_8$ to binary.

In base $n$, a number, when converted to decimal, is divisible by $n$ if it ends in zero. Show that this is correct by:

a dividing $1220_3$ by 3

b dividing $5310_6$ by 6

c dividing $8160_9$ by 9

d dividing $3A40_{16}$ by 16

In base $n$, if a number is divisible by a factor of $n$, the number ends in a digit that is also divisible by that factor. Show that this is correct by:

a dividing $1534_6$ by 2

b dividing $2154_8$ by 2

c dividing $2756_9$ by 3

d dividing $1B6_{12}$ by 6

In base $n$, a number is divisible by 2 if the last digit is divisible by 2 only if $n$ is divisible by 2.

a Show this result is true when $7156_8$ is divided by 2.

b Show this result is false when $7156_9$ is divided by 2.

In base $n$, if the sum of the digits is divisible by a factor of $n - 1$, then the number itself is also divisible by that factor.
Section 2: Divisibility tests

Show that this is correct by:

a  dividing 2121 by 3

b  dividing 3414 by 3

c  dividing 2734 by 4

d  dividing 1854 by 3
Key point 2.2

**Notation**: $b \mid a$ means that $b$ divides exactly into $a$, i.e. $b$ is a factor of $a$ or $a$ is a multiple of $b$.

**Standard tests for divisibility:**

<table>
<thead>
<tr>
<th>Divides by</th>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>last digit divisible by 2</td>
<td>$1528 \div 2 = 764$</td>
</tr>
<tr>
<td>3</td>
<td>sum of digits divisible by 3</td>
<td>$2946 \div 3 = 982$</td>
</tr>
<tr>
<td>4</td>
<td>last 2 digits divisible by 4</td>
<td>$3124 \div 4 = 781$</td>
</tr>
<tr>
<td>5</td>
<td>last digit 5 or 0</td>
<td>$1325 \div 5 = 265$</td>
</tr>
<tr>
<td>8</td>
<td>last 3 digits divisible by 8</td>
<td>$5128 \div 8 = 641$</td>
</tr>
<tr>
<td>9</td>
<td>sum of digits divisible by 9</td>
<td>$1872 \div 9 = 208$</td>
</tr>
<tr>
<td>11</td>
<td>the value found by subtracting and adding consecutive digits is 0 or divisible by 11</td>
<td>$714032 \div 11 = 64911$</td>
</tr>
</tbody>
</table>

**Divisibility by any primes number $p$ (up to 50):**

Find $n$ where $n = \frac{(kp + 1)}{10}$ and $k$ is the smallest digit that makes $\frac{(kp + 1)}{10}$ an integer.

Remove the last digit to make two numbers.

Multiply this last digit by $n$ and subtract the result to the first number formed when the original number was split.

If the result is divisible by $p$ then the original number is divisible by $p$.

If the new number is too large repeat the process.

**Divisibility of composite numbers**: a number is divisible by a composite number if it is divisible by all the factors of the composite number.
The division algorithm (the fundamental theorem of Euclid): If $a$ is divided by $b$ where $0 < b < a$ then $a = bq + r$ where $q$ is the quotient and $r$ is the residue. If $r = 0$ then $b \mid a$.

WORKED EXAMPLE 2.7

Without performing the division, show that $538949224$ is divisible by $88$.

$88$ is a composite number: i.e.
$88 = 8 \times 11$

$8 \mid 224 \quad \therefore \quad 8 \mid 538949224$

$5 - 3 + 8 - 9 + 4 - 9 + 2 - 2 + 4 = 0$

$\therefore \quad 11 \mid 538949224$

Hence $88 \mid 538949224$

WORKED EXAMPLE 2.8

Find the quotient and residue when $27$ is divided by $4$.

By the division algorithm: $27 = 4 \times 6 + 3$

$\therefore \quad q = \text{quotient} = 6, \quad r = \text{residue} = 3$

WORKED EXAMPLE 2.9

Use a suitable algorithm to determine whether $59925$ is divisible by $17$.

$p = 17$

Find integer $n = \frac{(kp + 1)}{10}$ for smallest $k$.

If $10 \mid (17k + 1)$ then smallest
$k = 7 \Rightarrow n = 12$

Remove the last digit to make two numbers.

Multiply last digit by $n$.

Split $59925$ into $5992$ and $5$.

Add the result to the first part of the split number and if the result is divisible by $p$ then the original number is divisible by $p$.

$5 \times 12 = 60$
5992 + 60 = 6052

Repeat
605 + 2 \times 12 = 629
62 + 9 \times 12 = 170 = 17 \times 10

Hence 17 \mid 59925

**Tip**

It is a common error to use the value of $k$ rather than the value of $n$ when using the algorithm.

If the algorithm fails, go back and check that you have used the correct value of $n$.

**WORKED EXAMPLE 2.10**

By putting $n = 4q + r$, where $n$ is any odd integer, prove that the square of $n$ takes the form $8k + 1$, where $k$ is an integer.

By the division algorithm, let the integer $n$ be given by $n = 4q + r$.

Since $n$ is odd then $r = 1$ or $r = 3$.

When $r = 1$:

\[n^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k + 1\]

When $r = 3$:

\[n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1 = 8k + 1\]

Hence, the square of any odd integer is of the form $8k + 1$.

**Euclid’s algorithm**

To find the highest common factor of $a$ and $b$ ($a > b$).
Write $a = bq_1 + r_1$, and if $r_1 = 0$, then $b \mid a$ and $\text{hcf}(a, b) = b$.

If $r_1 \neq 0$ divide $b$ by $r_1$ such that $b = r_1q_2 + r_2$. If $r_2 = 0$, then $b \mid a$ and $\text{hcf}(a, b) = r_1$.

If $r_2 \neq 0$ divide $b$ by $r_2$ such that $r_1 = r_2q_3 + r_3$. If $r_3 = 0$, then $b \mid a$ and $\text{hcf}(a, b) = r_2$.

Repeat until the residue is zero, i.e. when $r_{n-1} = r_nq_n + 0$, giving $\text{hcf}(a, b) = r_n$

**WORKED EXAMPLE 2.11**

Find the $\text{hcf}$ of:

**a** 1260 and 308

1260 = 308 × 4 + 28
and 308 = 28 × 11 + 0
so $\text{hcf}$ of 1260 and 308 is 28

**b** 7735 and 231

7735 = 231 × 33 + 112
and 231 = 112 × 2 + 7
112 = 7 × 16 + 0
so $\text{hcf}$ of 7735 and 231 is 7

**EXERCISE 2B**

a 1260 and 308

b 7735 and 231

1260 = 308 × 4 + 28
and 308 = 28 × 11 + 0
so $\text{hcf}$ of 1260 and 308 is 28

7735 = 231 × 33 + 112
and 231 = 112 × 2 + 7
112 = 7 × 16 + 0
so $\text{hcf}$ of 7735 and 231 is 7
1. Without performing the division, determine whether:
   a) 2136 is divisible by 4
   b) 4215 is divisible by 4
   c) 54128 is divisible by 8
   d) 31764 is divisible by 9
   e) 7284916375 is divisible by 11.

2. Show that $15 \mid 24630$.

3. Without performing the division, determine whether:
   a) 27545024 and 33440778 are both divisible by 8 and/or 9
   b) 17841106 and 13880328 are both divisible by 9 and/or 11
   c) 55581768 and 66593934 are both divisible by 9 and/or 11
   d) 667667 and 289731 are both divisible by 3 and/or 11.

4. Show that $11 \mid 34601919$.

5. Using the algorithm described in Key Point 2.2 to determine whether:
   a) 1956955 is divisible by 17
   b) 189200 is divisible by 43
   c) 3141259 is divisible by 19
   d) 456617 is divisible by 37.

6. Without doing the division, show that 11 is not a factor of 2018.

Find the residue when 2018 is divided by 11.

7. Given that 165 divides into $51a20b5$, find $a$ and $b$.

8. Show that $(x + 3) \mid (x^4 - 4x^2 + 14x - 3)$.

9. Use the division algorithm to find the quotient and the remainder when:
   a) $x^2 + 3x - 4$ is divided by $x - 2$
   b) $n^3 - 3n^2 + 2n + 4$ is divided by $n^2 + 2n - 3$.

10. Find the residue when $1495 \times 1594 + 500$ is divided by 13.

11. Find the remainders when $2, 2^2, 2^3, 2^4, 2^5, 2^6$ and $2^7$ are divided by 7.
Hence find the residue when $2^{50}$ is divided by 7.

Find the residue when $5^{1000}$ is divided by 11.

Find the smallest number that has a residue of 3 when divided by 5 and a residue of 4 when divided by 6 or 7.

Use Euclid’s algorithm to find the highest common factor of:

- a 2275 and 42
- b 2041 and 117
- c 4860 and 1476
- d 4389 and 299

By putting $n = 5q + r$, where $n$ is an integer, prove that every square number is of the form $5k$, $5k + 1$ or $5k + 4$, where $k$ is an integer.

Given that $n$ is an integer and by putting $n = 3q + r$ prove that $n(n^2 + 2)$ is an integer when it is divided by 3.

Given that $n$ is an integer and by putting $n = 9q + r$ show that $n^3 = 9k + r^3$.

Hence prove that every cube number is of the form $9k$ or $9k + 1$, where $k$ is an integer.

By putting $n = 5q + r$ show that $n^4 = 5k + r^4$.

Hence prove $n^4$ is of the form $5k$ or $5k + 1$, where $k$ is an integer.

Show that $n^3$ has the form $7k$ or $7k + 1$, where $k$ is an integer.

Show that $3 | n(7n^2 + 5)$.

---

Section 3: Modular (or finite) arithmetic
Key point 2.3

From the division algorithm, \( a = nq + r \), from which:

\[ a \equiv r \pmod{n} \]

i.e. \( r \) is the residue when a number \( a \) is divided by a number \( n \).

\[ \text{e.g. } 15 \equiv 3 \pmod{12} \]

[This is sometimes referred to as clock arithmetic, e.g. 15:00 hours is the same as 3 p.m.]

Rules

If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then:

\[ a + c \equiv b + d \pmod{n} \]
\[ a - c \equiv b - d \pmod{n} \]
\[ ac \equiv bd \pmod{n} \]
\[ a^n \equiv b^n \pmod{n} \]

If \( f(x) \) is a polynomial in \( x \) with integer coefficients, then \( f(a) \equiv f(b) \pmod{n} \)

If \( a \equiv b \pmod{m} \) and \( a \equiv b \pmod{n} \), where \( m \) and \( n \) have no common factors, then:

\[ a \equiv b \pmod{mn} \]

Solving linear congruences

A **linear congruence** is an equation of the form \( ax \equiv b \pmod{n} \).

It has a solution if, and only if, \( d \mid b \) where \( d \) is the highest common factor of \( a \) and \( n \).

In this case, there are exactly \( d \) mutually **incongruent solutions** given by:

\[ x_1 + \frac{n}{d} \times r \]

where \( x_1 \) is a solution found by inspection and \( r = 0, 1, 2, \ldots d - 1 \).

Note: if \( n \) is prime, then \( ax \equiv b \pmod{n} \) will have a solution (since \( \text{hcf}(a, n) = 1 \)).

**WORKED EXAMPLE 2.12**

a Show that \( 5x \equiv 2 \pmod{15} \) has no solution.

b Solve the linear congruence \( 5x + 107 \equiv 12 \pmod{15} \).

\[ \text{a } \text{hcf}(5, 15) = 5 \]
\[ 2 \text{ is not a multiple of } 5, \text{ so no solution} \]

\[ \text{b } 5x + 107 \equiv 12 \pmod{15} \]
\[ 5x + 2 \equiv 12 \pmod{15} \]
\[ 5x \equiv 10 \pmod{15} \]
\[ d = \text{hcf}(5, 15) = 5 \]

For \( ax \equiv b \pmod{n} \) a solution requires \( d \mid b \) where \( d = \text{hcf}(a, n) \)

Simplify by changing 107 to base 15, i.e. \( 107 \equiv 2 \pmod{15} \)

\[ 5 \text{ is the number of incongruent solutions.} \]
Using \( x_1 + \frac{n}{d} \times r \).

Note: since \( \text{mod } 15 \), all solutions lie between 0 and 14.

**A** Solving simultaneous linear congruences

**WORKED EXAMPLE 2.13**

Solve the simultaneous linear congruences

\[ x \equiv 3 \pmod{5} \quad \text{...(i)} \]

\[ x \equiv 4 \pmod{7} \quad \text{...(ii)} \]

\[ a \text{ is } x \equiv 3 \pmod{5} \Rightarrow x = 3 + 5k \]

Where \( k \) is an integer.

\[ \text{Write } x \equiv 3 + 5k \pmod{7} \]

\[ \therefore 3 + 5k \equiv 4 \pmod{7} \]

\[ \Rightarrow 5k \equiv 1 \pmod{7} \]

\[ \Rightarrow k \equiv 3 \pmod{7} \]

\[ \text{Rewriting this gives } k = 3 + 7m \ (m \text{ is an integer}) \]

\[ \text{Substituting in (i)} \]

\[ x = 3 + 5(3 + 7m) = 18 + 35m \]

\[ \text{Hence the solution to the simultaneous equations is:} \]

\[ x \equiv 18 \pmod{35} \]

To check the answer note that:

\[ 18 \equiv 3 \pmod{5} \text{ and } 18 \equiv 4 \pmod{7} \]
In the above example we could have started with \( x \equiv 4 \pmod{7} \Rightarrow x = 4 + 7k \) and then written this in modulo 5 and proceeded in the same way.

**Tip**

Most errors occur when solving the linear congruences, e.g. \( 5k \equiv 1 \pmod{7} \) should give \( k \equiv 3 \pmod{7} \). Always check this answer before completing the problem.

**WORKED EXAMPLE 2.14**

Solve the simultaneous linear congruences:

\[
x \equiv 4 \pmod{6} \quad \text{...(i)}
\]

\[
x \equiv 2 \pmod{5} \quad \text{...(ii)}
\]

\[
x \equiv 2 \pmod{4} \quad \text{...(iii)}
\]

(i) is \( x \equiv 4 \pmod{6} \Rightarrow x = 4 + 6k \ldots(*) \)

Where \( k \) is an integer.

Write

\[
x = 4 + 6k \equiv 2 \pmod{5}
\]

\[
\therefore 6k \equiv -2 \equiv 3 \pmod{5}
\]

\[
\therefore k \equiv 3 \pmod{5}
\]

Hence \( k = 3 + 5m \) (\( m \) is an integer) and substituting in (*)

\[
x = 4 + 6(3 + 5m) = 22 + 30m
\]

Hence the solution to (i) and (ii) is:

\[
x \equiv 22 \pmod{30} \ldots(iv)
\]

Now solve the simultaneous equations (iii) and (iv):

(iii) \( \Rightarrow x \equiv 2 \pmod{4} \therefore x = 2 + 4k \)

and \( x = 2 + 4k \equiv 22 \pmod{30} \)

\[
4k \equiv 20 \pmod{30}
\]

\[
\therefore 2k \equiv 10 \pmod{15}
\]

\[
\therefore k \equiv 5 \pmod{15}
\]

Note – change of modulo since

\[
4k \equiv 20 \pmod{30} \Rightarrow 4k = 20 + 30t
\]

\[
\div 2 \Rightarrow 2k = 10 + 15t
\]

\[
\therefore 2k \equiv 10 \pmod{15}
\]
Hence $k = 5 + 30m$ ($m$ is an integer) and substituting in (iii):

$$x = 2 + 4(5 + 15m) = 22 + 60m$$

Hence the solution to all three equations is:

$$x = 22 \pmod{60}$$

To check the answer note that:

$$22 \equiv 4 \pmod{6}, 22 \equiv 2 \pmod{5} \text{ and } 22 \equiv 2 \pmod{4}$$

**Tip**

Always check that your answer to the solution of the first two congruences satisfies both of them before moving on to complete the problem.

**Condition for a solution of two linear congruences**

- Each congruence must be solvable.
- If $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, then the condition for an integer solution to exist is $d \mid (a - b)$, where $d = \text{hcf}(m, n)$.

**WORKED EXAMPLE 2.15**

Explain why $3x \equiv 8 \pmod{12}$ and $5x = 7 \pmod{16}$ have no solutions.

1. $d = \text{hcf}(12, 16) = 4$
2. $a - b = 8 - 7 = 1$
3. 1 is not a multiple of 4
4. No solution.

**Tip**

Remember that you are checking that $d \mid (a - b)$ and **not** $d \mid a$ and $d \mid b$.

**Condition for a solution of three linear congruences**

- Each congruence must be solvable.
If the moduli are coprime (they have no common factors), then there will be a unique solution.

Check whether each pair of congruences has a solution (as above).

**WORKED EXAMPLE 2.16**

Explain whether the following have solutions:

a) \( x \equiv 1 \pmod{2} \), \( x \equiv 2 \pmod{3} \) and \( x \equiv 3 \pmod{5} \)

b) \( x \equiv 5 \pmod{12} \), \( x \equiv 11 \pmod{13} \) and \( x \equiv 12 \pmod{14} \)

a) Yes

b) Consider \( x \equiv 5 \pmod{12} \) and \( x \equiv 12 \pmod{14} \)

\[ d = \text{hcf}(12, 14) = 2 \]

\[ a - b = 12 - 5 = 7 \]

7 is not a multiple of 2.

No solution.

**Quadratic residues**

If the congruence \( x^2 \equiv q \pmod{n} \) has a solution, then \( q \) is called the quadratic residue \( \pmod{n} \).

If the congruence has no solution, then \( q \) is a quadratic non-residue.

**WORKED EXAMPLE 2.17**

Find all the quadratic residues for modulo 12.

Write a table with all possible values for modulo 12.

<table>
<thead>
<tr>
<th>( x )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x^2 \pmod{12} )</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Quadratic residues modulo 12 are: 0, 1, 4, 9

This means that \( x^2 \equiv q \pmod{12} \) has solutions only for these quadratic residues.
Tip

It is easy to make an error in converting to the given modulo.
Always check the symmetry of the values in the table.
If you use the symmetry of the table always check your values are correct – it is common error to take symmetry about the wrong ‘middle’ number.

WORKED EXAMPLE 2.18

Solve the congruence $x^2 \equiv 7 \pmod{9}$.

Write a table with all possible values for modulo 9.

<table>
<thead>
<tr>
<th>$x$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^2 \pmod{12}$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

From the table: $x \equiv 4 \pmod{9}$ or $x \equiv 5 \pmod{9}$

Possible values are 4, 13, 22, … or 5, 14, 23, …

WORKED EXAMPLE 2.19

Prove that the congruence $x^2 \equiv 6 \pmod{8}$ has no solutions.

Write a table with all possible values for modulo 8.

<table>
<thead>
<tr>
<th>$x$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^2 \pmod{12}$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

From the table there are no solutions satisfying $x^2 \equiv 6 \pmod{8}$

Only $x^2 \equiv 0$, 1 or 4(mod 8) have solutions.
Tip

If you exclude the trivial value 0 from the tables in the examples above, you will notice that the pattern of numbers is symmetrical.
Write the numbers in the given modulo.

a. \(23 \mod 5\)

b. \(71 \mod 8\)

c. \(43 \mod 3\)

d. \(38 \mod 6\)

Write 46 in modulo 4 and 53 in modulo 4 hence find \(46 + 53 \mod 4\).

Write 76 in modulo 7 and 44 in modulo 7 hence find \(76 - 44 \mod 7\).

Write 187 in modulo 8 and 118 in modulo 8 hence find \(187 - 118 \mod 8\).

Write 31 in modulo 5 and 64 in modulo 5 hence find \(31 \times 64 \mod 5\).

Write 65 in modulo 9 and 34 in modulo 9 hence find \(65 \times 34 \mod 9\).

If \(22 \equiv 2 \mod 5\) find the value of \(22^{10} \mod 5\).

Find the value of \(380^4 \mod 3\).

Find the highest common factor of 6 and 15. Hence solve the linear congruence:
\(6x \equiv 3 \mod 15\).

Find the highest common factor of 10 and 25. Hence solve the linear congruence:
\(10x \equiv 15 \mod 25\).

Solve the following linear congruences:

a. \(9x \equiv 21 \mod 30\)

b. \(9x \equiv 6 \mod 12\)

c. \(12x + 403 \equiv 11 \mod 16\)

d. \(15x + 347 \equiv 12 \mod 20\)

Solve the following simultaneous linear congruences:

a. \(x \equiv 5 \mod 6\), \(x \equiv 2 \mod 9\)

b. \(x \equiv 4 \mod 7\), \(x \equiv 3 \mod 11\)

c. \(x \equiv 11 \mod 12\), \(x \equiv 5 \mod 18\)

d. \(x \equiv 3 \mod 11\), \(x \equiv 9 \mod 13\)

Explain why the following have no integer solutions:

a. \(3x \equiv 2 \mod 12\)

b. \(10x + 111 \equiv 9 \mod 15\)

c. \(x \equiv 3 \mod 12\) and \(x \equiv 4 \mod 18\)
14 Solve the following simultaneous linear congruences:

a \( x \equiv 9 \pmod{12}, \ x \equiv 5 \pmod{8}, \ x \equiv 3 \pmod{18} \)

b \( x \equiv 2 \pmod{3}, \ x \equiv 5 \pmod{6}, \ x \equiv 7 \pmod{8} \)

c \( x \equiv 3 \pmod{5}, \ x \equiv 4 \pmod{6}, \ x \equiv 4 \pmod{8} \)

d \( x \equiv 5 \pmod{8}, \ x \equiv 3 \pmod{7}, \ x \equiv 1 \pmod{9} \)

15 Find the quadratic residues for:

a modulo 6

b modulo 11

c modulo 15

d modulo 20

16 Show that 3 is a quadratic residue of 23 and is a non-residue of 31.

17 Solve the following congruences:

a \( x^2 \equiv 4 \pmod{9} \)

b \( x^2 \equiv 6 \pmod{10} \)

c \( x^2 \equiv 11 \pmod{14} \)

d \( x^2 \equiv 7 \pmod{18} \)

If \( x^2 \equiv q \pmod{n} \), where \( n > 2 \), has one solution \( x \equiv x_0 \pmod{n} \), state another solution in terms of \( n \) and \( x_0 \).

18 Prove that the following have no solutions:

a \( x^2 \equiv 5 \pmod{9} \)

b \( x^2 \equiv 3 \pmod{7} \)

c \( x^2 \equiv 2 \pmod{16} \)

d \( x^2 \equiv 3 \pmod{19} \)

19 List all the quadratic residues and all the quadratic non-residues for

a modulo 5

b modulo 7

c modulo 11

d modulo 13

State the number of quadratic residues and non-residues for modulo \( p \) where \( p \) is prime.
If \( p \) is an odd prime number and \( q \) and \( p \) have no common factors, then Euler proved that \( q \) is a quadratic residue of \( p \) if and only if \( q^{(p-1)/2} \equiv \pm 1 \pmod{p} \).

Demonstrate that this result is correct for all the quadratic residues of modulo 11.

You will be able to prove this result when you have studied the next section.

Section 4: Prime numbers

Key point 2.4

**Prime**: an integer \( p \) \((p \neq 1)\) is prime if it has no divisors except 1 and itself.

**Composite**: a composite number has at least one divisor other than 1 and itself.

**Highest common factor**: the hcf (also called the greatest common divisor gcd) is the highest factor of two or more numbers.

**Coprime**: two or more integers are coprime (or relatively prime) if 1 is there only common factor.

**Fundamental theorem of arithmetic** (also known as the unique prime factorisation theorem) states that every integer greater than 1 is either prime or the product of primes in exactly one way (apart from arrangements).

Useful results for integers \( a, b \) and \( c \):

- If \( a \) and \( b \) are coprime and \( a \mid c \) and \( b \mid c \), then \( ab \mid c \).
- If \( a \mid b \) and \( c \mid d \), then \( ac \mid bd \).
- If \( a \mid b \) and \( b \mid c \), then \( a \mid c \).
- If \( a \mid b \) and \( a \mid c \), then \( a \mid (bx + cy) \), where \( x \) and \( y \) are integers.

**Bezout's identity**: the highest common factor of \( b \) and \( c \) is \( bx + cy \). Note: if this hcf is 1 , then \( b \) and \( c \) are coprime.

WORKED EXAMPLE 2.20

Use Bezout's identity to show that 8 is the highest common factor of 40 and 56.

\[ 8 = 3 \times 40 - 2 \times 56 \]

Hence 8 is the hcf(40, 56)

List multiples of each number:

- 40, 80, 120, 160, ...
- 56, 112, 168, 224, ...

Spot the linear combination.

Euclid's algorithm to find the hcf(56, 40):
56 = 40 \times 1 + 16 \\
40 = 16 \times 2 + 8 \\
16 = 8 \times 2 + 0 \\

Writing it backwards:
8 = 40 - 2 \times 16 = 40 - 2(56 - 1 \times 40) \\
8 = 8 = 3 \times 40 - 2 \times 56 \\

WORKED EXAMPLE 2.21

Use Bezout's identity to show that:

a) \( n \) and \( n + 1 \) are coprime

b) \( \frac{5n + 7}{3n + 4} \) is irreducible

c) \( \frac{24n + 5}{18n + 3} \) is reducible

a) Let \( d \) be the highest common factor of \( n \) and \( n + 1 \).

If \( d \mid n \) and \( d \mid (n + 1) \), then
\[
d \mid (1 \times (n + 1) - 1 \times n) \\
\therefore d \mid 1 \\
i.e. highest common factor of \( n \) and \( n + 1 \) is 1.

Hence \( n \) and \( n + 1 \) are coprime.

b) Let \( d \) be the highest common factor of \( 5n + 7 \) and \( 3n + 4 \).

If \( d \mid (5n + 7) \) and \( d \mid (3n + 4) \), then
\[
d \mid (3 \times (5n + 7) - 5 \times (3n + 4)) \\
\therefore d \mid 1 \\
i.e. highest common factor of \( 5n + 7 \) and \( 3n + 4 \) is 1.

Hence \( \frac{5n + 7}{3n + 4} \) is irreducible.

c) Let \( d \) be the highest common factor of \( 24n + 5 \) and \( 18n + 3 \).

Irreducible = cannot cancel down.

Since if \( d \mid a \) and \( d \mid b \) then \( d \mid (ax + by) \) and put \( x = 3 \) and \( y = -5 \) to eliminate \( n \).

Numerator and denominator have no common factors (other than 1) so the fraction cannot cancel down.
Reducible = can cancel down.

Since if \(d \mid a\) and \(d \mid b\), then \(d \mid (ax + by)\)
and put \(x = 3\) and \(y = −4\) to eliminate \(n\).

Hence \(\frac{5n + 7}{3n + 4}\) is reducible.

Numerator and denominator have common factor 5 so the fraction can cancel down.

Euclid’s lemma

Generally, if a prime number \(p\) divides into the composite number \(a_1 \times a_2 \times a_3 \ldots \times a_n\) then \(p\) must divide into one of \(a_1\) to \(a_n\).

Further, if \(a \mid bc\), where \(a\) and \(b\) are coprime, i.e. \(\text{hcf}(a, b) = 1\), then \(a \mid c\).

WORKED EXAMPLE 2.22

Use a step-by-step algorithm to show that 23 is a factor of 30107.

7 is also a factor of 30107.

Explain why 23 is also a factor of 4301.

\[
\begin{align*}
3010 + 7 \times 7 & = 3059 \\
305 + 7 \times 9 & = 368 \\
36 + 7 \times 8 & = 92 = 23 \times 4 \quad \therefore 23 \mid 30107 \\
7 \times 4301 & = 30107 \\
\text{since } 23 \mid 30107 \text{ then } 23 \mid (7 \times 4301) \\
23 \text{ and } 7 \text{ are coprime, and hence } \\
23 \mid 4301.
\end{align*}
\]

Euler’s lemma

Fermat’s little theorem:

- If \(p\) is prime and \(\text{hcf}(a, p) = 1\), then \(a^{p-1} \equiv 1 \pmod{p}\).
- If \(p\) is prime, then \(a^p \equiv a \pmod{p}\).

Note that if \(p\) is prime, then this result is true. It does not follow that if this result is true that \(p\) is prime.

WORKED EXAMPLE 2.23

\[
\begin{align*}
N & = \frac{(23 \times 3 + 1)}{10} = 7 \\
\text{and } a^{x-1} & \equiv 1 \pmod{x} \text{ then } x \text{ is called a pseudo-prime.}
\end{align*}
\]
Show that $3^6 \equiv 1 \pmod{7}$ and hence find the value of $3^7 \pmod{7}$.

Putting $a = 3$ and $p = 7$ (prime) gives $3^6 = 3^{7-1} \equiv 1 \pmod{7}$. Using Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$.

Note that 3 and 7 are coprime.

$3^7 = 3 \times 3^6 = 3 \times 3^{7-1} \equiv 3 \times 1 \equiv 3 \pmod{7}$

**Tip**

It is a common error to use $a^p \equiv 1 \pmod{p}$.

Remember Fermat's little theorem states that $a^p \equiv a \pmod{p}$ or $a^{p-1} \equiv 1 \pmod{p}$.

**The order of a modulo**

$p$ is the smallest possible integer $n$ such that $a^n \equiv 1 \pmod{p}$.

Comparing with Fermat's little theorem, which states that $a^{p-1} \equiv 1 \pmod{p}$, note that $p - 1$ is not necessarily the least value of $n$.

Note also that $n \mid (p - 1)$.

**WORKED EXAMPLE 2.24**

Use Fermat's little theorem to find a value of $n$ for which $3^n \equiv 1 \pmod{13}$.

Find any other values of $n \pmod{13}$ satisfying $3^n \equiv 1 \pmod{13}$.

$3^{13-1} = 3^{12} \equiv 1 \pmod{13}$

Fermat's little theorem: $a^{p-1} \equiv 1 \pmod{p}$

Test other values of $n$.

$3^1 \equiv 3 \pmod{13}, 3^2 \equiv 9 \pmod{13}, 3^3 \equiv 1 \pmod{13}$

$n = 3$ satisfies $3^n \equiv 1 \pmod{13}$

Smallest value of $n$ is 3.

The order of modulo 13 is 3.

**The binomial theorem**

$(a + b)^p \equiv a^p + b^p \pmod{p}$, where $p$ is prime

Proof: This is obtained by:
\[(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{r}a^{p-r}b^r + \cdots + b^p\]

The \(r\)th term has coefficient: \(\binom{p}{r} = \frac{p!}{r!(p-r)!} = p \times \frac{(p-1)!}{r!(p-r)!}\)

Since \(p\) is prime, this expression (which is an integer) is a multiple of \(p\). So \(\binom{p}{r} \equiv 0\) (mod \(p\))

Hence: \((a + b)^p \equiv a^p + b^p\) (mod \(p\))

WORKED EXAMPLE 2.25

Solve \((\sqrt{x} + 2)^6 \equiv 4\) (mod 7)

\[(\sqrt{x} + 2)^6 \equiv x^3 + 2^6 \equiv 4\) (mod 7)

But \(2^6 \equiv 1\) (mod 7)

\(\therefore x^3 \equiv 3\) (mod 7)

Make a table:

<table>
<thead>
<tr>
<th>(x)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x^3) (mod 7)</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

Hence \(x \equiv 3\) or 4 (mod 7)

EXERCISE 2D
Use a suitable algorithm, showing each step, to show that 11 is a factor of 19019.

Hence write the composite number 19019 in terms of its prime factors.

It is given that \( x = n^2 + 3n + 2 \) and \( y = n^3 + 5n^2 + 7n + 2 \).

Show that, for integer values of \( n \) greater than 1, \( x \) and \( y \) are each composite numbers.

Factorise \( n^5 + 1 \) and hence explain why \( 100001_n \) is a composite number for all integers \( n \geq 2 \).

Find a counter-example to show that the statement ‘\( 101^n \) is prime’ is false.

Use a step-by-step algorithm to show that 17 is a factor of 32045.

State another factor of 32045.

Explain why 17 is also a factor of 6409.

If \( 7 \mid (3x + 2) \), prove that \( 7 \mid (15x^2 - 11x - 14) \).

Find \( x \) and \( y \) given that \( 6 = 78x + 30y \).

Hence state the highest common factor of 30 and 78.

By writing down multiples of 77 and 132, show that 11 is the highest common factor of 77 and 132.

Use the fact that if \( a \mid b \) and \( a \mid c \), then \( a \mid (bx + cy) \), where \( x \) and \( y \) are integers, to show that:

a 3 is the highest common factor of 24 and 45
b 7 is the highest common factor of 35 and 42
c 13 is the highest common factor of 39 and 65
d 1 is the highest common factor of 7 and 11

Given that \( n \) is an integer, use the theorem that if \( d \mid a \) and \( d \mid b \), then \( d \mid (ax + by) \) to:

a prove that \( \frac{45n + 2}{20n + 1} \) is irreducible
b prove that \( \frac{12n + 3}{21n + 4} \) is reducible
c determine whether \( \frac{105n + 9}{70n + 5} \) has any integer values.

Use Euclid’s algorithm and then write it backwards to show that:

a 28 is the highest common factor of 420 and 308
b 11 is the highest common factor of 2255 and 286
c 23 is the highest common factor of 2737 and 138
11 Evaluate the following using Fermat’s little theorem:
   a \(2^{12} \pmod{13}\)
   b \(9^{16} \pmod{17}\)
   c \(2^{48} \pmod{17}\)
   d \(2^{12} \pmod{13}\)

12 Evaluate the following using Fermat’s little theorem.
   a \(2^{11} \pmod{11}\).
   b \(3^{19} \pmod{7}\).
   c \(3^{50} \pmod{5}\).
   d \(17^{40} \pmod{19}\).

13 Evaluate \(2^{340} \pmod{341}\) and state whether this means that 341 is a prime number.

   Show that 11 and 13 are factors of 341.

14 Solve the following using Fermat’s little theorem:
   a \(x^7 \equiv 2 \pmod{7}\)
   b \(x^{22} \equiv 3 \pmod{11}\)
   c \(3x^9 \equiv 4 \pmod{5}\)
   d \(x^{34} \equiv 16 \pmod{17}\)

15 Find the order \(n\) of the following numbers, each with order \(p\).
   a \(4 \pmod{7}\)
   b \(3 \pmod{11}\)
   c \(5 \pmod{19}\)
   d \(4 \pmod{23}\)

   For each question show that \(n | (p - 1)\).

16 Prove that \((m + n)^p \equiv m^p + n^p \pmod{p}\) and write down the congruence for:
   \((1 + n)^p \pmod{p}\).

   Find the values of \(2^p\), \(3^p\) and \(4^p\) and hence make a conjecture for the value of \(a^p\).

   Prove your conjecture by induction and hence obtain a proof of Fermat’s little theorem.

17 If today is Monday what day will it be in 10^{100} days’ time?
18 Solve \((4\sqrt[4]{x} + 3)^{16} \equiv 14\) (mod 17).

19 It is given that \(N = 12a + b\) and \(M = a - 4b\), where \(a\) and \(b\) are integers.

Prove that \(7 \mid N\) if, and only if, \(7 \mid M\).

**Tip**

If, and only if, means that the relation applies both ways,
i.e. check that if \(7 \mid M\), then \(7 \mid N\) and then check that if \(7 \mid N\), then \(7 \mid M\).

20 By considering \((2^m)^n\) and \((2^n)^m\), or otherwise, show that \(2^m - 1\) and \(2^n + 1\) are coprime, where \(m\) and \(n\) are positive integers, and \(m\) is odd.
Checklist of learning and understanding

Number bases:

- Columns are powers of the base, e.g.
  \[ a_n = a \times n^4 + b \times n^3 + c \times n^2 + d \times n + e. \]

Divisibility tests:

- To divide by 2, the last digit is divisible by 2.
- To divide by 3, the sum of the digits is divisible by 3.
- To divide by 4, the last 2 digits are divisible by 4.
- To divide by 5, the last digit is 5 or 0.
- To divide by 8, the last 3 digits are divisible by 8.
- To divide by 9, the sum of the digits is divisible by 9.
- To divide by 11, the value found by subtracting and adding consecutive digits is 0 or divisible by ±11.

Division algorithm:

- If \( a \) is divided by \( b \), where \( 0 < b < a \), then \( a = bq + r \), where \( q \) is the quotient and \( r \) is the residue. If \( r = 0 \), then \( b \mid a \).

Finite (modular arithmetic):

- If \( a = nq + r \) then \( a \equiv r \pmod{n} \).

Linear congruences:

- A linear congruence is an equation of the form \( ax \equiv b \pmod{n} \).
- Linear congruences have a solution if, and only if, \( d \mid b \), where \( d \) is the highest common factor of \( a \) and \( n \). The solutions are \( x_1 = \frac{n}{d} \times r \).
- If \( n \) is prime, then \( ax \equiv b \pmod{n} \) will have a solution (since \( \text{hcf}(a, n) = 1 \)).

Quadratic congruences:

- If the congruence \( x^2 \equiv q \pmod{n} \) has a solution, then \( q \) is the quadratic residue \( \pmod{n} \).

Prime numbers:

- An integer \( p (p \neq 1) \) is prime if it has no divisors except 1 and itself.
- A composite number has at least one divisor other than 1 and itself.
- Two or more integers are coprime (or relatively prime) if 1 is their only common factor.
The fundamental theorem of arithmetic states that every integer greater than 1 is either prime or the product of primes in exactly one way (apart from arrangements).

Bezout’s identity:
- If \( d \mid a \) and \( d \mid b \), then \( d \mid (ax + by) \), where \( x \) and \( y \) are integers.

Euclid’s lemma:
- If a prime number \( p \) divides into the composite number \( a_1 \times a_2 \times a_3 \times \ldots \times a_n \), then \( p \) must divide into one of \( a_1 \) to \( a_n \).

Fermat’s little theorem:
- If \( p \) is prime and \( \gcd(a, p) = 1 \), then \( a^{p-1} \equiv 1 \pmod{p} \).
- If \( p \) is prime, then \( a^p \equiv a \pmod{p} \).

The order of \( a \) modulo \( p \):
- This is the smallest possible integer \( n \) such that \( a^n \equiv 1 \pmod{p} \).

Binomial theorem:
- \( (a + b)^p \equiv a^p + b^p \pmod{p} \)

Mixed practice 2

1. Write \( 443^n \) as a quadratic in \( n \).
2. Given that \( 443^n = 323^{n+1} \) show that \( n^2 - 4n - 5 = 0 \) and hence find the value of \( n \) where \( n > 0 \).
3. Express the \( 443^n \) as a decimal number.
4. Show that \( 443^n \) is a composite number.
5. Use the standard divisibility tests to show that 248952 is divisible by 3, 8 and 11.
6. By putting \( n = 3q + r \), where \( n \) is an integer, prove that the square of \( n \) takes the form \( 3k \) or \( 3k + 1 \) where \( k \) is an integer.
7. Solve the linear congruence \( 7x + 322 \equiv 9 \pmod{23} \).
8. Solve the system of linear congruences:
   \[ x^2 \equiv 9 \pmod{15} \]
9. Solve the simultaneous linear congruences:
Use a step-by-step algorithm to show that $31 \mid 933317$.

a) Explain why the simultaneous linear congruences:

$$x = 3 \pmod{20} \text{ and } x = 12 \pmod{15}$$

have no integer solutions.

b) Solve the system of linear congruences:

$$x = 3 \pmod{20}, x = 13 \pmod{15} \text{ and } x = 33 \pmod{50}$$

9

a) Use the binomial expansion to prove that $(22)^n \equiv 1 \pmod{7}$.

b) Hence use Fermat’s little theorem to simplify $2^n + 3 \times 22^n \pmod{7}$.

c) Use quadratic residues to find the values of $n$ that make $2^n + 3 \times 22^n \pmod{7}$ a perfect square.

Let $M = 46a + b$ and $N = a - 5b$. Prove that $11 \mid M$ if, and only if, $11 \mid N$.

11

a) i) Use the binomial theorem to show that $33^2 \equiv 1 \pmod{2}$. Show that $33^2 \equiv 4 \pmod{5}$.

Hence show that if $33^2 + 44^2 = n^2$, where $n$ is an integer, that $n$ is odd and $n$ is a multiple of 5.

Use these results to find $n$.

ii) It is given that $35^2 + 45^2 = n^2$. By considering the values of $35^2 + 45^2 \pmod{2}, 3$ and 5 and finding quadratic residues show that $n$ cannot be an integer.

b) i) Use Fermat’s little theorem to show that $133^5 \equiv 3 \pmod{5}$. Find the values, modulo 5, of $110^5, 84^5$ and $27^5$.

ii) Find the values in modulo 2 and 3 of $133^5, 105^5, 84^5$ and $27^5$.

iii) Hence find the integer value $n$ satisfying $133^5 + 105^5 + 84^5 + 27^5 = n^5$.

12

a) Show that $n$ is not a factor of $2^n + 1$ if $n$ is even.

b) Use Fermat’s little theorem to find $2^n + 1 \pmod{p}$, where $p$ is an odd prime.

c) Find the set of values for which $n \mid (2^n + 1)$.

d) Prove your answer to c by induction.