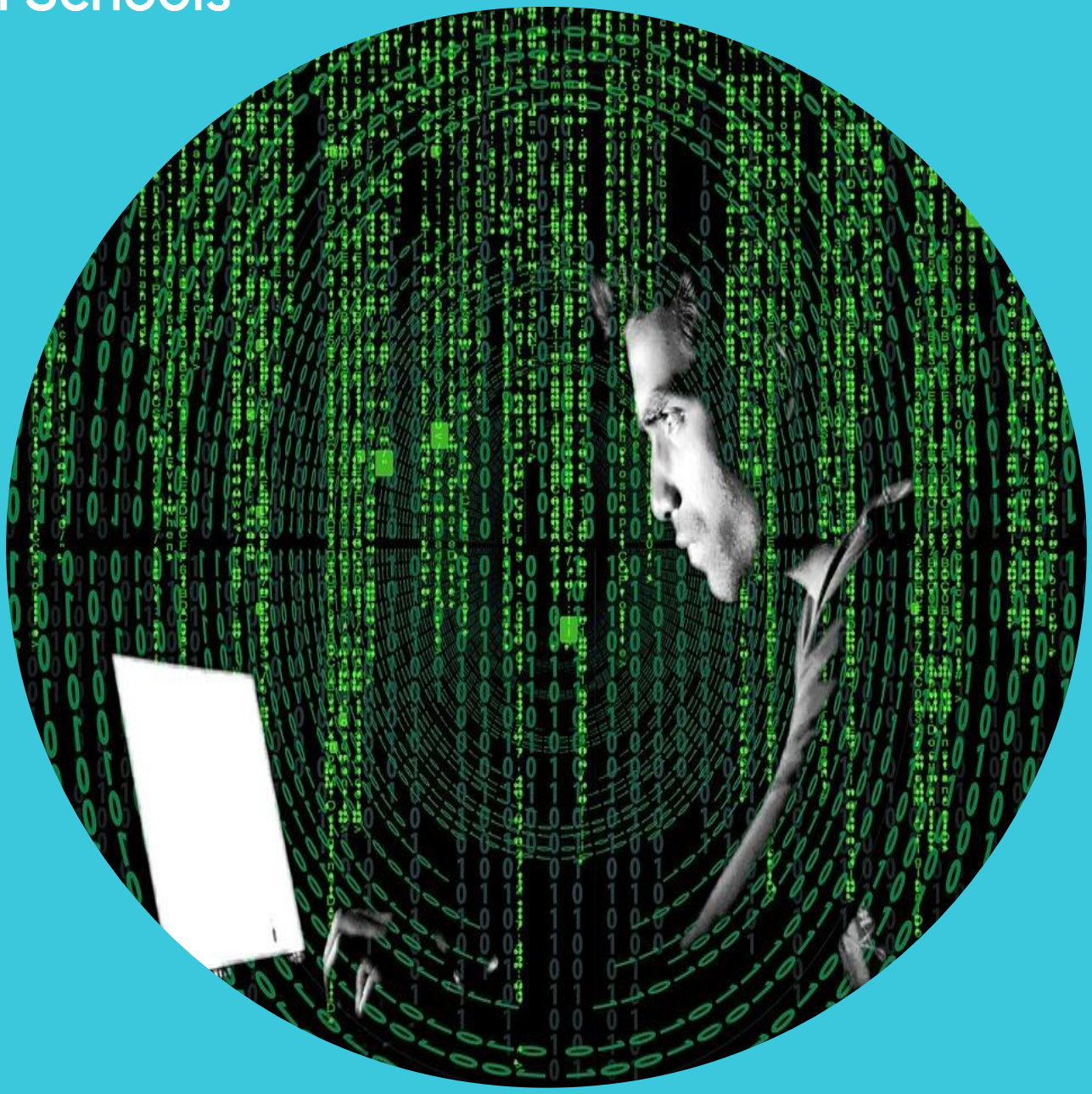
Researchers in Schools



Can good encryption make the difference when we are online?

Pupil Name	
Coursebook Designed by	Dr S Sannella

Timetable and Assignment Submission

Timetable – Tutorials

Tutorial	Date	Time	Location
1	09 – 12 - 2019	12pm	Royal West of England Academy, Queens Rd, Bristol, BS8 1PX
2	15-01-2020	3:20pm	School (OAJW)
3	22-01-2020	3:20pm	School (OAJW)
4	29-01-2020	3:20pm	School (OAJW)
5	05-01-2020	3:20pm	School (OAJW)
6 (Feedback)	26-02-2020	3:20pm	School (OAJW)
7 (Feedback)	15-03-2020	3:20pm	School (OAJW)

Timetable – Homework Assignments

Homework Assignment	Description	Due Date
Tutorial 1	Baseline assignment	13-12-2019
Tutorial 2	Modular arithmetic - Introduction	20-01-2020
Tutorial 3	Modular arithmetic - Powers	27-01-2020
Tutorial 4	Modular arithmetic - Applications	03-02-2020
Tutorial 5	Final assignment	14-02-2020

Assignment Submission – Lateness and Plagiarism

Lateness	
Submission after midnight on 9th August	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	Automatic fail

Contents

Course Rationale **4**

Mark Scheme **5**

Glossary of Keywords **9**

Tutorial 1 **10**

Activity 1 **11**

Activity 2 **11**

Tutorial 2 **14**

Activity 1 **14**

Activity 2 **15**

Activity 3 **15**

Tutorial 3 **18**

Activity 1 **19**

Activity 2 **19**

Activity 3 **19**

Tutorial 4 **21**

Activity 1 **21**

Activity 2 **22**

Activity 3 **22**

Tutorial 5 **24**

Activity 1 **24**

Activity 2 **25**

Activity n **25**

Tutorial 6 **28**

Reflection on feedback **28**

Tutorial 7 **30**

Reflecting on the course **31**

Appendices **32**

Referencing correctly **32**

Course Rationale

Every time we are online, our safety relies on complex methods to protect our sensible personal data (emails, banking, etc.) from unknown third parties. We will explain what cryptography is, why we need it, and how we make use of it in our everyday life. Most of the course consists of introducing modular arithmetic, which can be regarded as the "type" of mathematics mostly involved in cryptography. Although modern cryptography is based on very advanced mathematics, we will still be able to give an introduction of some basic mathematical tools that will allow us to understand some simple procedures of cryptography. Finally, we will discuss how we can make a good use of cryptography in our everyday life, in order to be secure and protect our privacy and our sensible information online.

Photo source: https://pxhere.com/en/photo/545994. License: CC0 1.0Universal (Public Domain Dedication).

We can split this mini-course in three different parts:

- In tutorial 1, we aim to introduce why this topic is important, and what the consequences of a weak level of online security could be.
- Tutorials 2,3 and 4 will be spent studying the basics of modular arithmetic. This is a very powerful and fundamental part of algebra, which is normally studied (more in depth) in the 1st year of University of a Maths degree.
- Tutorials 5 will be spent discussing some simple, actual and concrete precautions that we can put into place in order to navigate safely.

Uni Pathways Mark Scheme 2019 – problem-set assignments

	Skills	1st (70-100)	2:1 (60-69)	2:2 (50-59)	3rd (40-49)	Mark /100
Subject knowledge	Knowledge and understanding	○ All content included and materials used are relevant to the general topic and to the specific question/title ○ Good understanding of all the relevant topics. ○ Technical terms are defined and used accurately throughout ○ Clear justification of how the material and content included is related to the specific issues that are the focus of the assignment	○ Most of the content included is relevant to the general topic and to the specific question/title ○ Good understanding of most the relevant topics ○ Technical terms are used accurately but not always clearly defined. ○ Adequate justification of how the content included is related to the specific issues that are the focus of the assignment	○ Some of the content included is relevant to the general topic and to the specific question/title ○ Good understanding on some of the relevant topics but occasional confusion on others. ○ Scientific terms are used mostly accurately with occasional confusion and often not defined. ○ Some justification on how the content included is related to the specific issues that are the focus of the assignment	○ The content included and materials used are not applied to the question/title in a relevant manner ○ There is confusion in how understanding of the topics is expressed	
Critical thinking	Research and evidence	○ Uses evidence/calculations to support claims/assertions/ideas, consistently clearly and convincingly ○ Data is effectively analysed, and appropriate assumptions/conclusions are reached ○ Includes rich sources of research findings, data, quotations or other sourced material as evidence for the claims/ideas	○ Uses evidence/calculations to support claims/assertions/ideas, mostly clearly and convincingly ○ Data is analysed and the assumptions/conclusions that are reached are mostly appropriate ○ Includes adequate sources of research findings, data, quotations or other sourced material as evidence for the claims/ideas	○ Uses evidence/calculations to support claims/assertions/ideas, at times clearly and convincingly ○ There is an attempt to analyse data is and draw assumptions/conclusions ○ Includes some sources of research findings, data, quotations or other sourced material as evidence for the claims/ ideas	○ Data is presented largely without analysis	
	Developing an argument	○ Argument/proof is <u>exceptionally</u> well-developed and well-justified ○ Uses content from the tutorials in an unfamiliar context and does so accurately and confidently.	○ Argument/proof is <u>clear and well-developed,</u> and position is justified ○ Uses some content from the tutorials in an unfamiliar context, but not always accurately	○ Argument/proof is <u>clear but not well-developed</u> ○ Limited use of content from the tutorials in other contexts	○ Sometimes the argument/proof is not clearly established ○ Limited use of content from the tutorial and often inaccurately	
	Critical evaluation	○ Effectively critiques the problem set and effectively establishes a thorough response to it	○ Some evidence of critiquing the problem set and establishes a reasonable response to it	○ Limited evidence of critiquing the problem set and establishes a response to it that has some coherence	○ The problem is explored in the work but without explanation	
Wr itt	Structure and presentation	○ Ideas are presented in paragraphs and arranged in a logical structure	○ Ideas are presented in paragraphs and arranged in a structure that is	○ Ideas are presented in paragraphs and arranged in a structure	○ Ideas are presented in paragraphs but there is	

		that is appropriate for the assignment o The introduction clearly outlines how the essay/report will deal with the issues o The conclusion summarises all the main points clearly and concisely o All calculations, formulas and methods are clearly structured, clear to follow and correct o Tables and graphs are effectively constructed including appropriate headings, units and scales. o All sources are referenced correctly in an agreed format	mostly appropriate for the assignment o The introduction adequately describes how the essay/report will deal with the issues o The conclusion summarises most of the main points clearly o Calculations, formulas and methods are mostly structured, clear to follow and correct o Most tables and graphs are well constructed o Most sources are referenced correctly in an agreed format	o The introduction mentions how the essay/report will deal with the issues o The conclusion summarises some of the main points clearly o Calculations, formulas and methods are not always structured, clear to follow and correct. o Some tables and graphs are well constructed but contains some errors o Some sources are referenced correctly in the agreed format with occasional errors	a lack of structure in how the work is presented o The work lacks an introduction that establishes the scope of the question o The work lacks a conclusion that summarise the main points raised o Work is not referenced accurately	
	Language and style	o No spelling, grammar or punctuation errors o Writing style consistently clear, tone appropriate and easy to follow o Accurate and consistent use of technical language and vocabulary	o Minimal spelling, grammar or punctuation errors o Writing style mostly clear, tone appropriate and easy to follow o Some attempts of using technical language and vocabulary, but not always accurate	o Some spelling, grammar or punctuation errors o Writing style moderately clear, tone appropriate and easy to follow o Use of simple language and vocabulary effectively but struggles to use technical language	o There are a significant number of spelling, grammar and punctuation errors o Use of simple language and vocabulary effectively but a lack of technical language	

	Overall Mark for written element (average of the 6 marks from the criteria above)/100	
		+
	Problem Set mark/100	
		÷ 2
	Final mark/100	

Baseline Assignment (problem-set): Pupil Feedback Report

Name of Pupil	
Name of School	Oasis Academy John Williams
Name of RIS teacher	Stefano Sannella
Title of Assignment	

How your assignment is graded:

Grade	Marks	What this means
1st	70+	Performing to an excellent standard at A-level
2:1	60-69	Performing to a good standard at A-level
2:2	50-59	Performing to an excellent standard at GCSE
3rd	40-49	Performing to a good standard at GCSE
Working towards a pass	0-39	Performing below a good standard at GCSE
Did not submit	DNS	No assignment received by The Brilliant Club

Lateness	
Any lateness	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	Automatic fail

Marks

OVERALL MARK / 100		FINAL MARK / 100 (including any deductions)	
DEDUCTED MARKS		FINAL GRADE	

If marks have been deducted (e.g. late submission, plagiarism) the teacher should give an explanation in this section:

Mark Breakdown and Feedback

Knowledge and Understanding		Research and Evidence	
	mark		*mark*
Developing an Argument		**Critical Evaluation**	
	mark		*mark*
Structure and Presentation		**Language and Style**	
	mark		*mark*
Problem Set			
Comment			*mark*

Final Assignment (problem-set): Pupil Feedback Report

Name of Pupil	
Name of School	Oasis Academy John Williams
Name of RIS teacher	Stefano Sannella
Title of Assignment	Essay + Exercise set

How your assignment is graded:

Grade	Marks	What this means
1st	70+	Performing to an excellent standard at A-level
2:1	60-69	Performing to a good standard at A-level
2:2	50-59	Performing to an excellent standard at GCSE
3rd	40-49	Performing to a good standard at GCSE
Working towards a pass	0-39	Performing below a good standard at GCSE
Did not submit	DNS	No assignment received by The Brilliant Club

Lateness	
Any lateness	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	Automatic fail

Marks

OVERALL MARK / 100		FINAL MARK / 100 (including any deductions)	
DEDUCTED MARKS		FINAL GRADE	

If marks have been deducted (e.g. late submission, plagiarism) the teacher should give an explanation in this section:

Mark Breakdown and Feedback

Knowledge and Understanding		Research and Evidence	
	mark		*mark*
Developing an Argument		**Critical Evaluation**	
	mark		*mark*
Structure and Presentation		**Language and Style**	
	mark		*mark*
Problem Set			
			mark

Subject Vocabulary

Word	Definition	In a sentence
Encryption	The process of turning a message into a secret code for the purpose of making difficult, for unauthorised people, to comprehend it. Example: "ifmmp" is the message resulting from an (easy) encryption of "hello" by replacing each letter with the following one (so "h" becomes "i", etc). Synonymous: encoding.	The process of replacing words, characters or numbers by using a determinate rule for the purpose of hiding the meaning of a message.
Decryption	The opposite of "encryption". It is the process of taking a pre-encrypted message (like "ifmmp", see above) and returning the original message ("hello"). Synonymous: decoding.	The process of turning an encrypted message into the original message.
Cryptography	The study of methods of encryption.	The study of methods of encryption.
Privacy	A personal area (physical, spacial, information, etc.) that an individual might want to keep protected and confidential.	A personal area (physical, spacial, information, etc.) that an individual might want to keep protected and confidential.
Code	A code is a specific way to encrypt messages; in other words, chosen an encryption method, the code is the system of rules that is actually converting a given message into the encrypted message.	Chosen an encryption method, the code is the system of rules that is actually converting a given message into the encrypted message.
Divisibility	The property of a number of being divisible (by another number).	The property of a number of being divisible (by another number).
Modular Arithmetic	The area of mathematics studying the laws and properties of set of numbers which are grouped by criteria about divisibility.	The area of mathematics studying the laws and properties of set of numbers which are grouped by criteria about divisibility.
To Break (a code)	A successful attempt of a third-party to understand the code of an encryption, and therefore to be able to decipher messages encrypted under such code.	A successful attempt of a third-party to understand the code of an encryption, and therefore to be able to decipher messaged encrypted under such code.
Natural number	A number who is positive and integer (namely 1,2,3,4…).	A number who is positive and integer.
Congruence (modulo n)	An expression in the form a=b (mod n), meaning that a-b is divisible by n.	An expression in the form a=b (mod n).

Tutorial 1 – Online security

Image above: Creator:MaxPixel's contributors. Credit: https://www.maxpixel.net/

What is the Purpose of Tutorial 1?

Mathematics has always been applied to a tremendous number of situations and technologies that are part of our everyday life. Since the end of the previous century, information technology has totally changed how we communicate, how we work, how we buy, how we organise our social life, and the list can continue. Information technology strongly relies on advanced mathematics, more or less in every aspect. The rise of internet has simplified our lives greatly, but at the same time has exposed us to risks that were unknown before then. Cryptography studies all the techniques that allow us to keep our information online protected.

In this tutorial, we aim to:

- Realise the size of the problem about online frauds and theft.
- Understand what cryptography is and why we need it.
- Recall basic notions of arithmetic (prime numbers, divisibility) and introduce the notion of congruence.

Starter:

Last year, a number of people in the UK have got some of their money stolen from online fraudsters and cyber criminals. Can you estimate how many of them?

1) ~10,000

2) ~100,000

3) ~1,000,000

4) ~5,000,000

How many cases have been solved? More or less than 50%? What is the average amount of money that is stolen? More or less than £500?

This started is supposed to rise some awareness about the problem of online frauds.

Activity 1:

Individually, based on what we have discussed in our starter, find out what was the total amount of money that was stolen from people living in the UK.

Activity 2:

In group, let us compute some reduction (mod n). For example:

$10 \equiv$ __ (mod 4)

$19 \equiv$ __ (mod 7)

$11 \equiv$ __ (mod 2),

$59 \equiv$ __ (mod 29).

Homework – Baseline Assessment:

- **Essay (250 words):** *Why is encryption important for our security? Have you haver thought about this issue before? In your answer, you could include what we have discussed in our first tutorial, as well as other information from your personal cultural background and/or your personal reading on the subject.*

- **Exercises:**

  Perform the following reductions and operations modulo n.

  13 (mod 3); 25 (mod 7); 13 (mod 2); 93 (mod 15); 52 (mod 2);

  61 (mod 9); 92 (mod 2); 37 (mod 8); 101 (mod 2); 99 (mod 46).

  What can you notice when you reduce modulo 2?

  Perform the following operations modulo n:

  6 × 8 (mod 7); 6 × 22 (mod 7);

  11+18 (mod 5); 13+28 (mod 5);

  90-17 (mod 13); 90-43 (mod 13);

  31+15 (mod 10); 31+45 (mod 10).

  What do you notice? Hint: Try to check what 8 and 22 have in common, thinking mod 7. Or also, what 18 and 28 have in common, mod 5.

  Try to deduce a general rule explaining this phenomenon, and write it as a formal mathematical statement.

Success criteria:

- *You should demonstrate an understanding about what the course is about, and why we are studying this topic. Knowledge of the data that we have discussed in the tutorial is required.*
- *The small amount of maths that we have explored in the first tutorial should be clear enough to be able to carry out basic operations. When you are required to explain something, this should be done concisely but clearly, and with the correct terminology.*
- *Clear language and style are essential (both in the essay and in the maths task).*

Tutorial 2 – Modular arithmetic, part 1.

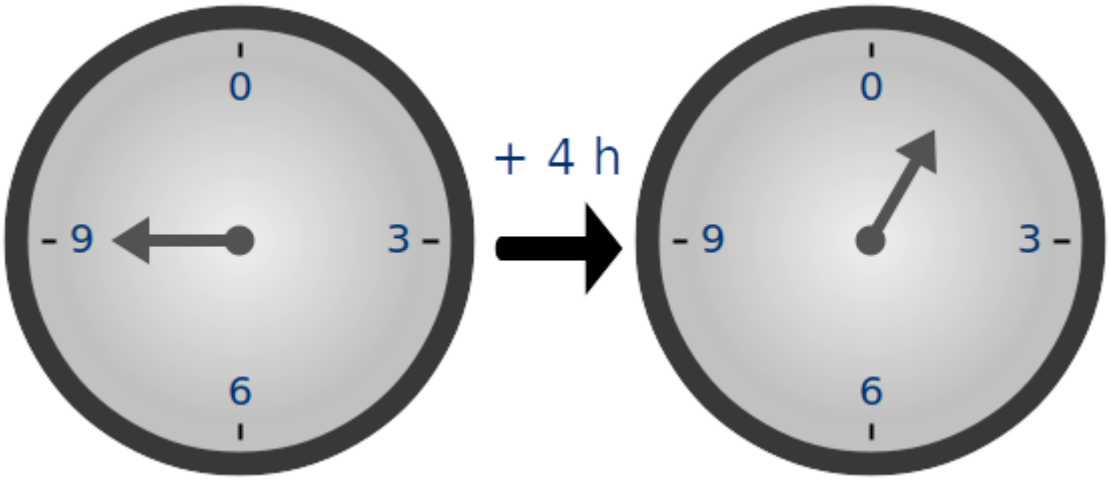


Photo source:
Photo from English Wikipedia. The original uploader was Spindled at English Wikipedia. [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0/)]

What is the Purpose of Tutorial 2?

- Know what modular arithmetic is about, and perform basic operations in that setting.
- Realise that unusual phenomena happen in modular arithmetic.

Starter:

Let us suppose that it is 11am.

- What time will it be in 3 hours?
- We know that it will be 2pm. Do we deduce that 11+3=2?

The correct mathematical answer is yes! Provided that we work in modular arithmetic, in particular "modulo 12".

Activity 1:

In group, let us revise some reduction (mod n). For example:

$13 \equiv$ __ (mod3) $\qquad$ $10 \equiv$ __ (mod 7)

$9 \equiv$ __ (mod 2), $\qquad$ $55 \equiv$ __ (mod 21).

Activity 2: Can we find a null factor law? And inverse law?

Let us practise some operations (mod n). For example:

$2 \times 4 \equiv$ __ (mod 7)

$4 \times 5 \equiv$ __ (mod 10)

$3 \times 5 \equiv$ __ (mod 14),

$8 \times 4 \equiv$ __ (mod 16).

What do we notice?

Activity 3 – Numbers being zero modulo n

Let us suppose that a positive integer number a is 0 modulo n, namely $a \equiv 0 \pmod{n}$. What does it actually mean?

Homework:

1) Create the multiplication tables mod 4, mod 5, mod 6, mod 7.

2) Observe in which case you get 1's, 0's, and try to deduce a more general rule about this phenomenon.

Example: As an example, I provide the multiplication table mod 2 and mod 3.

Mod 2	0	1
0	0	0
1	0	1

Mod 3	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

In the table mod 3, we have $2 \times 2 = 4 \equiv 1 \pmod 3$, therefore 1 is the entry in the right bottom corner (the result of the multiplication of 2 and 2, when computing modulo 3).

Homework instructions:

In order to be able to follow the next tutorials, being able to make computations mod n smoothly is essential. The first purpose of this exercise is to practise this, since you will be required to make many multiplications and reductions mod n in order to write down the full tables. The second purpose is about understanding what happens when we do arithmetic mod n, for example understanding when we get 0 or 1 as a result of a multiplication.

Homework success criteria:

The tables must be correct; although it might be a bit time-consuming, the task is purely computational and no critical thinking is required. After practising for a bit, it will definitely become easier. Most important, when solving 2) you should be able to understand the role that the specific number n (so 4,5,6 or 7) plays. Clarity is essential.

Tutorial 3 – Modular arithmetic, part 2.

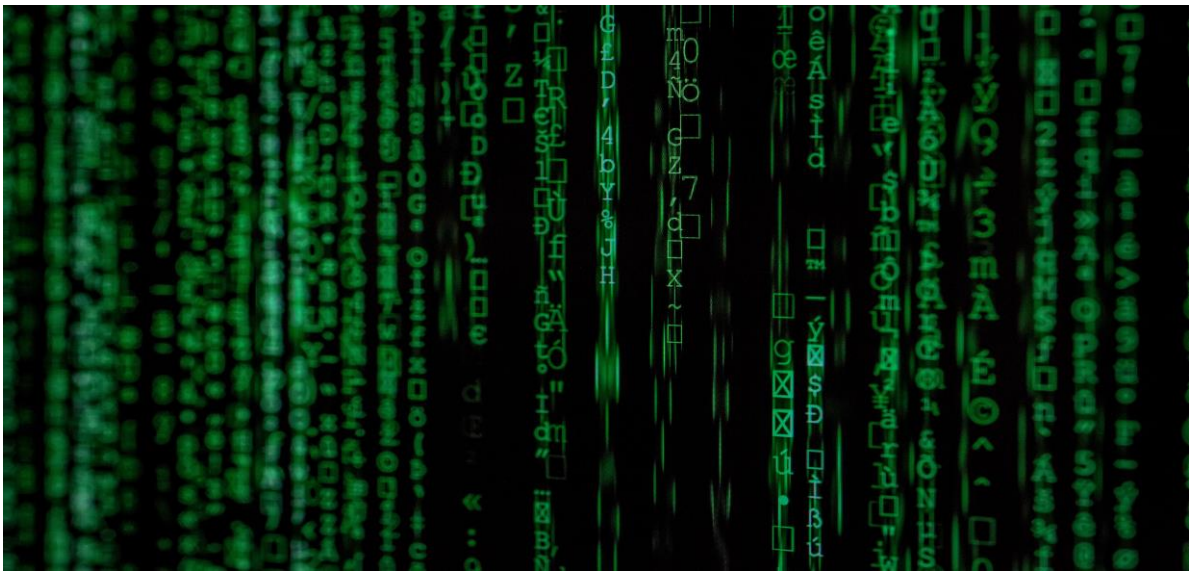


Photo by Markus Spiske on Unsplash.

What is the Purpose of Tutorial

- Practise how we can effectively compute powers mod n.
- State Fermat's little theorem.
- State Euler's theorem.

Starter:

Individually, reduce the following powers modulo n:

$3^3 \equiv$ __ (mod 5)

$2^6 \equiv$ __ (mod 10)

$12^2 \equiv$ __ (mod 11).

$17^9 \equiv$ __ (mod 16).

As you might have realised, 17^9 is very large ($17^9 = 118587876497$), but the positive fact is that we do not have to compute it!

Activity 1:

Apply the methods that we have just discussed and reduce modulo n the following large powers (work with the person next to you, if you want).

$13^4 \equiv$ __ (mod 11)

$15^7 \equiv$ __ (mod 16).

$135^7 \equiv$ __ (mod 4).

$5^5 \equiv$ __ (mod 4).

Activity 2:

1) Reduce:

$2^6 \equiv$ __ (mod 7)

$3^4 \equiv$ __ (mod 5)

$7^2 \equiv$ __ (mod 3)

$2^{10} \equiv$ __ (mod 11)

2) What did you notice? Try to guess what the cause of this phenomenon might be.

Activity 3:

We have defined φ (Euler's function).

1) Compute the value of φ for the following numbers: 3, 5, 6, 10, 14, 17, 20.

φ(3)=

φ(5)=

φ(6)=

φ(10)=

φ(14)=

φ(17)=

2) What happens when you apply φ to a prime number?

Homework:

Euler's theorem is an example of generalisation of another theorem: basically, this means that Euler's theorem implies Fermat little theorem. To make it easier to understand, think about the statement "the angles of every quadrilateral sum up to 360°". This *generalises* the statement "the angles of every parallelogram sum up to 360°", because the statements about quadrilaterals includes parallelograms too (since parallelograms are quadrilateral).

Using what we have learned in Activity 4, can you convince yourself that Euler's Theorem generalises Fermat little theorem?

Homework instructions:

Question 2) from Activity 4 is necessary in order to answer the question. The question is really about the following: when we apply the statement of Euler's Theorem using the assumptions of Fermat little theorem (namely, that n is a prime number), do we get the statement of Fermat little theorem?

Homework success criteria:

The answer is not supposed to be necessarily long, but it should be:

- clear and concise;
- expressed with the due terminology.

Tutorial 4 – Modular arithmetic, part 3.

Image from: https://www.needpix.com/photo/1183690/safety-encryption-ssl-world-protection-lock-security-internet-privacy

What is the Purpose of Tutorial 4?

- Recall some divisibility criteria, for example the case of the number 3
- Show that such criteria, which were only stated at school, can be rigorously proved using modular arithmetic.
- Finding the last digit of a great number given as a power (which seems hard, but is indeed perfectly treatable by using modular arithmetic).

Starter – Divisibility by 3

Let us recall (together) the criterion to determine if a number is divisible by 3.

Activity 1 – Proving why this criterion holds

Let us consider the number 357. We know that this is divisible by 3, because the sum of its digits 3,5 and 7 gives 15, which is divisible by 3. But why does this criterion show that 357 is divisible by 3?

- Let us decompose 357 in its units, tenths and hundreds. We have: 300+50+7, namely **3** × 100+ **5** × 10 + **7**. We want to see if this number is divisible by 3. Therefore, we must evaluate it modulo 3 and see if we get 0 as a result! Let us try it:

$$\mathbf{3} \times 100 + \mathbf{5} \times 10 + \mathbf{7} \equiv ?? \pmod 3$$

But we notice that $10 \equiv 1 \pmod 3$, and also $100 \equiv 1 \pmod 3$. Conclude the exercise.

- Can it be extended to any number? How can we do it?

Activity 2 - Divisibility by 5

We have just recalled the criterion to determine if a number can be divisible by 3, and we have provided a sketch of the proof.

- Can we give a similar argument to explain the criterion to determine if a number is divisible by 5? Discuss this with the person next to you.

Activity 3 – Determine the last digit

Let us consider the number 2057^{88}. We want to find out its last digit (the unit). This number, if expressed in digits, has 294 of them. In particular, this number is:

3 669 591 060 469 381 499 192 806 988 909 154 369 413 412 693 750 215 923 571 897 873 635 129 316 360 056 630 812 969 283 759 351 031 751 098 214 575 910 390 724 266 879 559 314 166 789 232 334 067 617 841 581 936 952 461 820 489 917 547 272 607 298 838 078 091 749 623 429 292 788 356 113 402 704 163 673 608 173 435 497 359 232 205 230 819 815 340 305 399 447 362 923 161 786 298 200 001.

We can see that its last digit is 1! But what if we want to try to work it out **without** the full calculation? Try to solve this exercise by realising that the unit of any number is what you get after reducing modulo 10. After realising that, we need to effectively solve

$$2057^{88} \equiv __ \pmod{10}$$

We can do it either

- By manipulating the power (see Activity 2 in Tutorial 3).
- Using Euler's theorem.

Homework

Let us consider Activity 3. Try to solve the same exercise by using the alternative method (not the one that you have chosen to use initially).

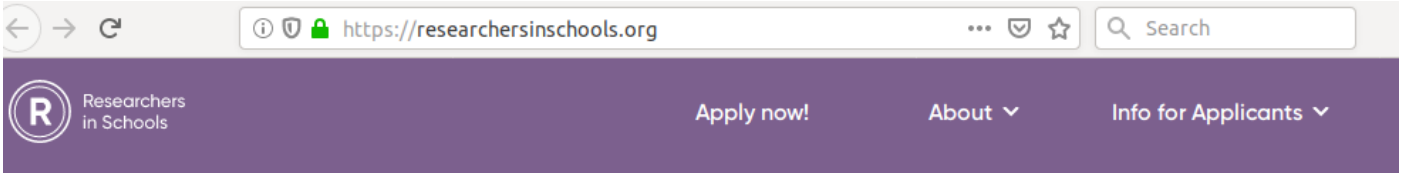
Using the method that you prefer, find the last digit of 7073^{42}. Although this number is larger, this exercise is slightly easier that the one in Activity 3.

Homework success criteria:

- If you use Euler's theorem in your homework, make sure that you structure your answer logically. Start by saying that you are applying Euler's theorem, and proceed finding the value of φ for n. This would make the answer clearer.

- Regardless of the method that you want to use to solve the exercise, ensure that the strategy is clearly written at the beginning, for example "we aim to reduce our number by noticing that 7073 (mod10) is…".

Tutorial 5 – Real world applications



As a last lesson, we will go through the most common security threat that rely on poor encryption.

What is the Purpose of Tutorial 5?

- We will learn how to recognise if an internet connection is secure or not.
- We will describe the type of threats that can be hidden behind a public unsecured Wi-Fi.
- We will briefly discuss what a VPN is, and in which circumstances it might be useful.

Starter:

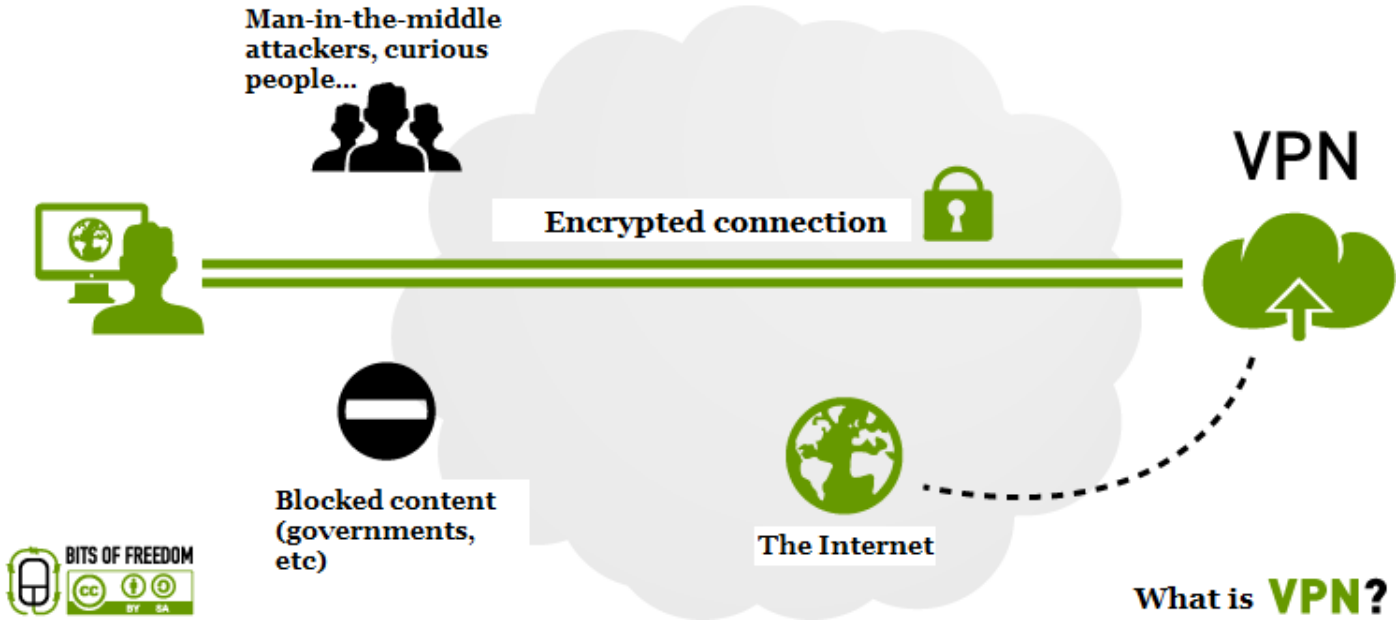
Above, we can see a picture of a part of the RIS website and one of our school website. They are different, but they have one thing in common. What is it? Have you ever noticed it somewhere else?

Activity 1:

For many aspects, sending information over internet is not different from sending information via more "traditional" channels, for example post, phone, etc.

- *Talk to the person next to you, and try to imagine how information that you send over internet can be compromised.*
- *Try to focus on two points: the recipient (and its trustability), and the path that the information are travelling through.*

Activity 2 – VPN, an example of protection



Edited version of a photo from bitsoffreedom.nl (original creator). [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0/)]. Original photo here: https://toolbox.bitsoffreedom.nl/adviezen/vpn/

We have discussed what a Virtual Private Network (VPN) is. Talk to the person next to you and try to think why:

- *Using a VPN can increase your security in some circumstances;*
- *Using a VPN can neutralise a man-in-the-middle attack.*

Activity 3 – General discussion

As in life, the most prudent conduct cannot always preserve us from an online threat, but a good understanding of online security can definitely rule out many of them. What do you think about it?

Final assignment.

Essay

Write a short essay (around 1000 words) about what you have learned in terms of online security, online threats and some simple strategies to overcome them. What are the most common security issues/vulnerabilities that an average person might experience online? How can these affect us? How can we protect ourselves? You can both mention what we have studied in Tutorial 1 and Tutorial 5, as well as including other information from your independent reading on this topic or from your previous knowledge.

Success criteria:

- *This essay is meant to be useful for your everyday life and online security, so I will be happy to see that what we have covered in class has been absorbed.*
- *Apart from the content, as well as your stile and clarity. See "Written communication" in the Marking Scheme.*
- *If you want to mention some example that we have not covered in class, you can try to do your own search; mention the source when you include it in your essay. See "Research and evidence" in the Marking Scheme.*

Exercises

1) In Tutorial 4, we have recalled some divisibility criteria, for example for the number 3. In that footstep, discuss the divisibility criterion for 9, namely:

- When is a number divisible by 9? I suggest you to consider numbers divisible by 9, for example 18, 27, 36… to guess the criterion.
- Use modular arithmetic to explain why this criterion works.

2) More challenging: do as in exercise 1), but with 11 instead of 9. Let us recall the divisibility criterion for 11: a number is divisible by 11 if the *alternating sum of its digit* is zero. This means that if we consider 143, the alternating sum is 1-4+3 (you sum the digits with their sign changing every time). That sum is zero, and indeed 143 is divisible by 11, because $143=11 \times 13$.

3) Find the last digit of the following numbers (given as powers):

1022^{24}, 565^{106}, 1010^{31}.

Success criteria:

This is the most important of the two assignments, as it tests how much maths we have absorbed during the course. I consider the following success criteria:

- *You should demonstrate a fair understanding of basic modular arithmetic and show that you can use it to solve the proposed exercises.*

- *Demonstrate capability to illustrate your work and procedure using the appropriate mathematical language. Your solution must be clearly explained, and every step must be justified without gap (the reader has to be able to follow your procedure smoothly).*

  See "Subject knowledge" and "Written communication" in the Marking Scheme for more details.

Tutorial 6 – Feedback tutorial

What is the Purpose of Tutorial 6?

- To receive feedback on your final assignment
- To respond to the feedback from your Uni Pathways teacher
- To write targets for improvement on your final assignment

Final assignment feedback from your Uni Pathways Teacher

(Remember to look at the mark scheme to help you understand what you have done well so far, and how you can do even better in your final assignment)

Here are three things that my Uni Pathways Teacher thought I did well in my draft assignment
•   •   •

Here are three things that my Uni Pathways Teacher thinks that I could do to get a higher mark in my final assignment
•   •   •

Tasks from my Uni Pathways Teacher to do during the feedback tutorial to help me improve
•   •   •
My response:

Actions I will take to improve my final assignment after this tutorial…
•   •   •

Hand in date for my final assignment:	

Tutorial 7 – Final tutorial

What is the Purpose of Tutorial 7?

- To receive feedback and a grade on your final assignment.
- To reflect on the programme including what you enjoyed and what was challenging.
- To ask any questions you may have about university.

Final assignment feedback from my Uni Pathways Teacher

Final mark:	University style grade:
Feedback: Here are three things that my Uni Pathways teacher thought I did well in my final assignment • • •	

Here are three things that my Uni Pathways teacher thinks I should remember for when I am doing this kind of study in the future
• • •

University

What questions do you still have about University after taking part in Uni Pathways?
•   •   •

Reflecting on Uni Pathways

What did you most enjoy about Uni Pathways?
•   •   •

What did you find challenging about the programme?	How did you overcome these challenges?
• • •	• • •

Appendix 1 – Referencing correctly

When you get to university, you will need to include references in the assignments that you write, so we would like you to start getting into the habit of referencing in your Brilliant Club assignment. This is really important, because it will help you to avoid plagiarism. Plagiarism is when you take someone else's work or ideas and pass them off as your own. Whether plagiarism is deliberate or accidental, the consequences can be severe. In order to avoid losing marks in your final assignment, or even failing, you must be careful to reference your sources correctly.

What is a reference?

A reference is just a note in your assignment which says if you have referred to or been influenced by another source such as book, website or article. For example, if you use the internet to research a particular subject, and you want to include a specific piece of information from this website, you will need to reference it.

Why should I reference?

Referencing is important in your work for the following reasons:

- It gives credit to the authors of any sources you have referred to or been influenced by.
- It supports the arguments you make in your assignments.
- It demonstrates the variety of sources you have used.
- It helps to prevent you losing marks, or failing, due to plagiarism.

When should I use a reference?

You should use a reference when you:

- Quote directly from another source.
- Summarise or rephrase another piece of work.
- Include a specific statistic or fact from a source.

How do I reference?

There are a number of different ways of referencing, and these often vary depending on what subject you are studying. The most important to thing is to be consistent. This means that you need to stick to the same system throughout your whole assignment. Here is a basic system of referencing that you can use, which consists of the following two parts:

1. **A marker in your assignment**: After you have used a reference in your assignment (you have read something and included it in your work as a quote, or re-written it your own words) you should mark this is in your text with a number, e.g. [1]. The next time you use a reference you should use the next number, e.g. [2].
2. **Bibliography**: This is just a list of the references you have used in your assignment. In the bibliography, you list your references by the numbers you have used, and include as much information as you have about the reference. The list below gives what should be included for different sources.

    a. **Websites** – Author (if possible), title of the web page, website address, [date you accessed it, in square brackets].

    E.g. Dan Snow, 'How did so many soldiers survive the trenches?', http://www.bbc.co.uk/guides/z3kgjxs#zg2dtfr [11 July 2014].

    b. **Books** – Author, date published, title of book (in italics), pages where the information came from.

    E.g. S. Dubner and S. Levitt, (2006) *Freakonomics*, 7-9.

    c. **Articles** – Author, 'title of the article' (with quotation marks), *where the article comes from* (newspaper, journal etc.), date of the article.

    E.g. Maev Kennedy, 'The lights to go out across the UK to mark First World War's centenary', Guardian, 10 July 2014.

Notes

Notes

UNI PATHWAYS

UNI PATHWAYS

researchersinschools.org