Fermat and Beyond

Cathal Sweeney, Jennifer Blanker , Conrad Dixon , Laura O'Reilly and Kevin Hennelly

November 2020

1 Introduction

In 1637 Fermat wrote a note in the margins of a copy of Arithmetica about a fact of mathematics that wasn't proved until 1994 , by an english mathematician **Robert Wiles** (source : Wikipedia). This fact was that no three positive integers a, b, c can satisfy the equation

$$a^n + b^n = c^n$$

for any n greater than 2.

Pythagorean triples , how many ? There is sufficient evidence to prove that there is an infinite amount of Pythagorean triples that exist according to Fermat's theorem. If you take one example of a Pythagorean triple , for instance with the numbers 6,8 and 10 and multiply them by a natural integer such as 2 or 3 , it will also result in a set of three integers which are a Pythagorean triple. This can be repeated and proves that if you have an infinite number of integers in which you can multiply a Pythagorean triple by it was also result in an infinite number of Pythagorean triples produced (source : Quora)

2

Primitive Triples A primitive triple is one where a,b and c are all coprime. This means that their gcd (greatest common divisor) is equal to 1. For any primitive triple a or b must be even and the other must be odd with c always being odd (source : mathcs.clarku.edu). We assume that a and b are both odd and therefore for some positive integers n and m , a = 2n-1 and b = 2m-1. Therefore,

$$a^2 + b^2 = c^2$$

$$(2n-1)^2 + (2m-1)^2 = c^2$$

$$4n^2 - 4n + 4m^2 - 4m - 2 = c^2$$

Since a and b are both odd that means that c must be even so we let c = 2i.

$$4n^2 - 4n + 4m^2 - 4m - 2 = 4i^2$$

$$4n^2 - 4n + 4m^2 - 4m - 4i^2 = 2$$

Factorise by 4 on the left hand side of the equation which results in 4 dividing 2 which is a contradiction. Therefore a and b can not both be odd and c must be odd. (whitman.edu)

3

How can we generate primitive triples? Euclid's formula is a fundamental formula for generating Pythagorean triples given an arbitrary pair of integers m and n with m ¿ n ¿ 0. The formula states that the integers

$$a = m^2 - n^2, b = 2mn, c = m^2 + n^2$$

form a Pythagorean triple. The triple generated by Euclid's formula is primitive if and only if m and n are co-prime and at least one is even. Also , dividing a , b and c by 2 will create a primitive triple when m and n are co-prime and both are odd. Every primitive triple arises (after the exchange of a and b, if a is even) from a unique pair of co-prime numbers m and n , one of which is even. (source : wikipedia)

An example can be done using a = 3 , b = 4 and c = 5. m = 2 and n = 1 (since m ¿ n).

$$3 = 2^2 - 1^2$$

$$4 = 2 \times 2 \times 1$$

$$5 = 2^2 + 1^2$$

(source : primes.utm.edu)

4

Is Fermat's last theorem still true when we work in modular arithmetic systems? If Fermat's equation had a solution (a,b,c) for exponent p¿2 and p is also prime, then it could be shown that the elliptic curve

$$y^2 = x(x - a^p)(x + b^p)$$

would make it unlikely that it is modular. It is believed that any solution to Fermat's equation for a prime number could be used to create a elliptic curve that could not be modular. (source : Wikipedia) Using modular arithmetic, If c is even and can be written as 2x for some integer x, then a and b are odd and can be written as 2x'+1 where x' is another integer. We then see that

$$c^2 = 4x^2 + 4x + 1$$

is congruent to 1 (mod 4) and

$$c^2 = 4n^2$$

is congruent to 0 (mod 4). This proves that c is odd. (source : whitman.edu)

5

$$(a + b + c)^p = a^p + b^p + c^p mod p$$

why is this true? We know that

$$(x + y + z)^2 = x^2 + y^2 + y^2 + 2*$$

(for lots of terms) And Thus,

$$(x + y + z)^2 = x^2 + y^2 + y^2 modulo 2$$

This is true as it works for any prime P in the question So therefore, will work for any prime P value which leads us to believe this is true.

6

Does that give us a way to find mod p solutions to the equation?

If we simplify

$$(a + b + c)^p$$

we get:

$$a2p + 2apb + b2p + 2bcp + 2acp + c2p$$

If we simplify

$$a^p + b^p + c^p mod p$$

we get:

$$Pa^p + Pb^p + Pc^p$$

Therefore:

$$a2p + 2abPb2p + 2bcp + 2acp + c2p = Pa^p + Pb^p + Pc^p$$

$$ap + 2ab + bp + 2bc + 2ac + cp = a^p + b^p + c^p$$

all (a,b,c) satisfy the equation

$$(a+b+c)^p = a^p + b^p + c^p mod p$$

This would allow us to find mod p solutions for the various equations for any value of P prime, the binomial coefficients are all 0 mod leaving us with only

$$a^p + b^p (mod p)$$

7

Conclusion In conclusion Fermat's 1673 note in the margins of copy Arithmetical about a fact of maths was indeed true and can be visually seen from the above questions and statements. The cases n=1 and n=2 have been known since antiquity to have infinitely many solutions (source: Wikipedia). Prior to the theorem being solved it was regarded as ''the most difficult mathematical problem" of that time, with the largest number of unsuccessful proofs. Fermat claimed to have a proof for this theorem, but no record was ever found. It is now among the most notable thermos in the history of mathematics. Mathematicians now believe that no real doubts remain over Fermat's last theorem.

Project 2 - Divisibility

Evan Duffy,
Erika Kaladinskas,
Molly Flannelly,
Niall Cahalan,
Christopher Burke

Aisling McCluskey

November 2020

1 Introduction

To check if a number is divisible by 3, all we have to do is to sum the digits and check if that sum is divisible by 3 – why? Are there similar rules for 5 and 9 (and why)? How do we check if a number is divisible by 7? Can you use modular arithmetic to prove it? What about 11? 99? or 101? Now, let's work in a different base. Let's write our numbers in base 60. Is there a quick way to check whether or not a number is divisible by 2, 3, 5? by 59?

2 Divisibility by 3

To check if a number is divisible by 3, all we have to do is sum the digits of that number and check if that sum is divisible by 3. Can we prove this?

Consider a number x where:
$x = a_n...a_3a_2a_1a_0$

We can also write this number as
$x = a_0 + a_1(10) + a_2(10^2) + ... + a_n(10^n)$

Let y = the sum of the digits of x
$y = a_0 + a_1 + a_2 + ... + a_n$

$x - y = (a_0 + a_1(10) + ... + a_n(10^n)) - (a_0 + a_1 + ... + a_n)$
$x - y = (a_0 - a_0) + (a_1(10) - a_1) + ... + (a_n(10^n) - a_n)$
$x - y = a_1(10 - 1) + a_2(10^2 - 1) + ... + a_n(10^n - 1)$
$x - y = a_1(9) + a_2(99) + a_3(999) + ... + a_n(99..99_n)$

As we can see, we can factor out a 3,

$x - y = 3(a_1(3) + a_2(33) + a_3(333) + ... + a_n(33..33_n))$

x-y has a factor of 3 so it is divisible by 3.
So, this means that if, and only if, x is divisible by 3, then y is also divisible by 3. i.e the sum of the number's digits is divisible by 3.

3 Division by 5 and 9

We can say that similar rules apply to check if a number is divisible by 9 with that of 3 and it can be proved in a similar manner, however to check if a number is divisible by 5 the rule differs.

A number is divisible by 5 if the last digit is either 0 or 5. Can we prove this?

First, let us consider how the "divisibility by 5" rule can be proved for the concrete number 735, for example.

We can write 735 = 7*100 + 3*10 + 5.

The first two additives, 7*100 and 3*10, have the common multiple 10, which is divisible by 5. Hence, the sum of these additives 7*100 + 3*10 is divisible by 5. Therefore, the divisibility by 5 of our original number depends on and is determined solely by the last additive, which is the last digit of the number, i.e. 5 in our case.

For the general case, the proof follows the same arguments. Let $a_n a_{n-1}...a_2 a_1 a_0$ be the decimal record of our integer number N

Then, $N = a_n * 10^n + a_{n-1} * 10^{n-1} + ... + 10^2 * a_2 + 10 * a_1 + a_0$
The first n additives, $a_n * 10^n, a_{n-1} * 10^{n-1}, ..., 10^2 * a_2 + 10 * a_1$
have the same common multiple of 10 which is divisible by 5
Hence, the sum of these additives $a_n * 10^n + a_{n-1} * 10^{n-1} + ... + 10^2 * a_2 + 10 * a_1$
is divisible by 5.

Therefore, the divisibility by 5 of our original number depends on and is determined solely by the last additive, which is presented by the last digit of the number. It is what has to be proved.

4 Division by 7

It is easier to tell whether a number is divisible by say 3, 5 or 9. However, testing for divisibility by 7 is not as common.The steps for calculating a number divisible by 7 is as follows:

1. Remove the last digit from the number.
2. Double it.

3. Subtract it from the first part of the number.
Do this repeatedly until you compute something that is divisible by 7 or not.

4.1 Division by 7 and Modular Arithmetic

We can use modular arithmetic to prove if a number is divisible by 7 or not. Lets assume that we want to find the divisibility proof for 7 of a given number N.

$N = a_n(10^n) + a_{n-1}(10^{n-1}) + ...$
based upon the digits $a_0, a_1, a_2, ..., a_n$ of N.

In order to do so we apply the modular arithmetic to consecutive powers of 10 until we find the smallest exponent $n \geq with 10^n \equiv 1(mod 7)$.
We obtain

$10 \equiv 3(mod 7)$
$100 \equiv 10 * 10 \equiv 3 * 3 \equiv 2(mod 7)$
$1000 \equiv 10 * 100 \equiv 3 * 2 \equiv -1(mod 7)$ (1)
$10000 \equiv 100 * 100 \equiv 2 * 2 \equiv -3(mod 7)$
$100000 \equiv 100 * 1000 \equiv 2 * -1 \equiv -2(mod 7)$
$1000000 \equiv 1000 * 1000 \equiv (-1) * (-1) \equiv (1 mod 7)$

In (1) we reduce 1000 to -1 and not to the smallest positive value 6 because in this way we will find a smaller number than n with the same residue modulo 7 somewhat easier.
Now we can formulate a divisibility proof for 7 of a given number N which is valid.
$N = a_n(10^n) + a_{n-1}(10^{n-1}) + ... + a_2(10^2) + a_3(10^3)$
$\equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a_9 - 3a_{10} - 2a_{11} + ...(mod 7)$
Note the repeating sequence 1, 3, 2, -1, -3, -2.

Example: Check the divisibility of $N = 9476$ with respect to modulus 7.
$N = 9476 = 9 * 10^3 + 4 * 10^2 + 7 * 10^1 + 6 * 10^0$
$\equiv 6 + 3 * 7 + 2 * 4 - 9 = 26$
$\equiv 2 * 10^1 + 6$
$\equiv 2 * 3 + 6 = 12 \equiv 5(mod 7)$

We conclude that N = 9476 is not divisible by 7, since the division gives the remainder of 5.

5 Division by 11, 99 and 101

To check if a number is divisible by 11 we get the alternating sum of the number from left to right then get the modulo of 11 by the new number. If it is

equivalent to 0 then we know it is divisible by 11

Example: Check to see if the number 70824776 is divisible by 11

70824776 turns to 7-0+8-2+4-7+7-6

$7-0+8-2+4-7+7-6 = 11 \equiv 0(mod 11)$

This shows us that 70824776 is divisible by 11

To check if a number is divisible by 99 we must use the divisibility rule of 9 and 11. The divisibility rule of 9 is similar to the divisibility rule of 3. This is because $9 = 3^2$ The divisibility rule of 9 is to add all figures in a number and divide by 9 essentially the divisibility rule of 3 twice. If the number passes the divisibility test of 11 and 9 then it is divisible by 99

Example: Is 66710457 divisible by 99

First we check if it is divisible by 9 $6+6++7+1+0+4+5+7 = 36 \equiv 0(mod 9)$

Now we check if it is divisible by 11 $6-6+7-1+0-4+5-7 = 0 \equiv 0(mod 11)$

This proves that 66710457 is divisible by 99

To check if a number is divisible by 101 we separate the numbers into groups of two from right to left.Then we get the alternating sum of these groups similar to how we did in the divisibility rule of 11

Example: Is 6559546 divisible by 101

First we separate the numbers into their groups 6 55 95 46
Now we get the alternating sum of these groups and find out if it is divisible by 101

$6-55+95-46 = 0 \equiv 0(mod 101)$

This tells us that 6559546 is divisible by 101

6 Division in Base 60

The Ancient Babylonian's used a base 60 number system rather than a base 10 system. What advantages does this have over a base 10 system?

The number 60, a superior highly composite number, has 12 factors,

(1,2,3,4,5,6,10,12,15,20,30,60) of which the set, (2,3,5) are prime. With so many factors, many fractions are simplified.

Let us try and find quick methods to check whether a number is divisible by certain numbers in base 60.

Let us start simple with the number 2. As 2 is a factor of 60, the numbers in base 60 are divisible by 2, if and only if the "units" digit is divisible by 2. This is true for all single digit factors of 60 1,2,3,4,5,6. This shows the advantage of a number system whose base has many factors.

But how do we find out whether a number is divisible by a number that is not a factor of 60? Let's take 59 for example.

It is know that for a base N, a number is divisible by (N-1) if the sum of its digits equals (N-1). In this instance, a number is divisible by 59 base 60 provided the sum of its digits is equal to 59.

7 Conclusion

In conclusion we confirm that to check if a number is divisible by 3, all we have to do is to sum the digits and check if that sum is divisible by 3. There are similar rules for 5 and 9. In addition, to check if a number is divisible by 7 you follow the method outlined in Section 4.1 and you can in fact use modular arithmetic to prove it. The same method can be applied to the numbers 11, 99 and 101. Working in base 60 there is also quick ways to check whether or not a number is divisible by 2, 3, 5 and 59.

Maths Project Fibonacci Numbers

Ben Sheehan, Ruth Tansey, Ross Tynan, Matthew Talbot, Eve Walsh
Workshop Tutor - Dr. Aisling McCluskey

October - November 2020

What are Fibonacci Numbers?

The Fibonacci number sequence is a series of numbers where a number is the addition of the last two numbers starting with 0 and 1 such that N = (N-1) + (N-2). The first ten numbers in the series are 0,1,1,2,3,5,8,13,21,34....

Leanardo Pisano Bogollo (Fibonacci was his nickname) first introduced the Fibonacci sequence in his book 'Liver Abaci' in 1202. He discovered the sequence by posing the following question:

If a pair of rabbits is placed in an enclosed area, how many rabbits will be born there if we assume that every month a pair of rabbits produces another pair and that rabbits begin to bear young two months after their birth?

1. At the start no rabbits are born, as the first pair has not had time to be pregnant and born (0).
2. The first month: One pair of rabbits are born (1).
3. The second month: Again, one pair of rabbits are born as the new rabbits have not yet matured to bear young (1).
4. The third month: Two pairs of rabbits reproduce, and one pair is not ready, so two pairs of rabbits are born (2).
5. The fourth month: Three pairs of rabbits reproduce and 2 pairs of rabbits are not ready, so three pairs of rabbits are born (3).
6. The fifth month: Five pairs of rabbits produce and three are not ready, so five pairs of rabbits are born (5).

And so on.

There is an interesting pattern:

- Look at the number x3 = 2. Every 3rd number is a multiple of 2 (2, 8, 34, 144, 610, ...)
- The number x4 = 3. Every 4th number is a multiple of 3 (3, 21, 144, ...)
- The number x5 = 5. Every 5th number is a multiple of 5 (5, 55, 610, ...)

And so on (every nth number is a multiple of xn).

The Importance of the Fibonacci Sequence

While this series of numbers from this simple brain teaser may seem inconsequential, it has been rediscovered in an astonishing variety of forms, from branches of advanced mathematics to applications in computer science, statistics, nature, and agile development.

Can We Use The Euclidean Algorithm on Fibonacci Numbers?

The question we are asking ourselves in this project is 'Can the Euclidean Algorithm be used to prove Fibonacci Numbers'.
Fibonacci Numbers are numbers which take the form of each number being the sum of the two preceding numbers, or $\mathrm{F}_n = F_n - 1 + F_n - 2$.
By using the Euclidean Algorithm we have to prove that the GCD of two Fibonacci Numbers is also a Fibonacci Number.

The Euclidean Algorithm takes the form:

$$\mathrm{a}= \mathrm{q}_0 b + r_0 Q = quantity$$
$$\mathrm{b}= \mathrm{q}_1 r_0 + r_1 R = Remainder$$
$$\mathrm{r}_0 = q_2 r_1 + r_2$$
$$\mathrm{r}_1 = q_3 r_2 + r_3 ...$$

You can already see there is a strong correlation between the way in which the Euclidean Algorithm and the Fibonacci Sequence is carried out.But can the Euclidean Algorithm be used to prove that the GCD of two Fibonacci Numbers is a also a Fibonacci Number (ie. the Fibonacci Sequence)

(1) Simple example:
GCD(34,5)-
34= 5(6)+4
5 = 4 +1

The final number of the sequence(1) is the GCD, 1 is a Fibonacci Number but can also just indicate the two numbers are co-prime

(2) More Advanced Example:
GCD(1346269, 4181)-
1346269= 4181(321)+4168
4181= 4168+ 13
4168= 13(320)+ 8
13= 8+ 5
8= 5+3
5= 3+2
3=2+1

The GCD of this sequence is 1 once, again could they just be co-prime?

(3) Example where GCD definitely isn't 1: GCD(610,5)- 610= 5(122)+0
The final number of the sequence is 0, thus the previous number must be the the GCD, in this case it's 5, a Fibonacci Number
(4) Example where GCD isn't 5: GCD(832040,610)- 832040= 610(1364)+0
The GCD is 610, another Fibonacci Number

Building on the similarities in form between the the Euclidean Algorithm and Fibonacci numbers/ sequence, we worked through the four examples to conclude (1)That the GCD of two Fibonacci Numbers is in fact another Fibonacci Number, (2) The vast majority of the GCD's of the Fibonacci Numbers are 1, (3) The Euclidean Algorithm can be used to prove the Fibonacci sequence/ numbers.

Proof By Induction

Say there are 2 rabbits. After two months they produce another pair of rabbits. This pattern continues on and each pair behaves the same as the last. We begin the proof by letting fn be the number of pairs of rabbits in total after n months. Let f1=1 and f2=1. month 3, f3=3. In month 4, f4=4 and in month 5, f5=5. This forms a pattern and a formula fn=(fn-1)+(fn-2) If we assume the growth is exponential we can find some real number r is greater than 1 so fn is greater than or equal to r*n.

Claim First we claim r=(1+(5)**-1)/2 which is roughly 1.62 that satisfies r**2=r+1. Then fn greater than or equal to r**n-2.

P(1) and P(2) 1=r**1-2=r**-1 less than 1. f2=r**2-2=r**0=1

Induction For a fixed n greater than 1 and n greater than 2. The induction hypothesis is P(1), P(2)....P(n) are true for all. We assume this is true and therefore try to show P(n+1). We want to show fn+1 greater than r**n-1

Consider fn+1=fn+fn-1

Substitute the inequalities fn greater than or equal to rn-2 and fn-1 greater than or equal r**n-3** fn+1 greater than or equal to r**n-2 + r**n-3

Factor out common term of rn-3** fn+1 greater than r**n-3

Plug in r2=r+1** fn+1 greater than or equal to (r**n-3)(r+1)=r**n-3.r**2=r**n-1

This concludes the proof and is true for 1,2,3 and for all positive values of n.

Conclusion

In our study of the Fibonacci numbers, we were able to make some interesting observations about how the Fibonacci numbers apply to our everyday lives, such as the example with the rabbits. We also learnt that when putting two Fibonacci numbers into the Euclidean Algorithm, the outcome is almost always 1, not just because they are co-prime, but because they are Fibonacci numbers, or else the outcome was another Fibonacci number. This was an interesting connection to make as it shows how the Fibonacci numbers all interconnected. We were able to see how each consecutive Fibonacci number increases from one to the next in the proof by induction. These proofs and observations gave us a better understanding of the Fibonacci numbers and their significance and importance.

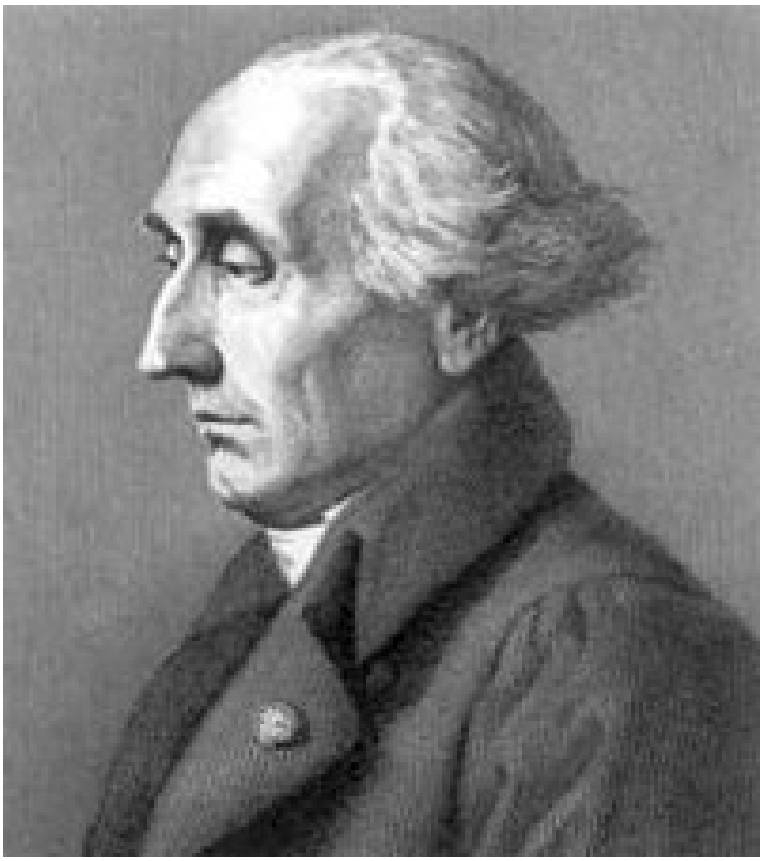
Project 4: Lagrange's Four Square's Theorem

Finn Timon, Jack Cashell, Sarah Boyle and Darragh Core

November 2020

Tutor- Aisling Mccluskey

1 Joesph-Louise Lagrange



2 Introduction

It is said that every branch of mathematics was progressed by the contributions of the Italian-born French mathematician Comte Joseph Louis Lagrange (1736-1813). Joseph's arithmetic work lasted 9 years from (1768 - 1777), during a period of transition in relation to the number theory. Joseph synthesised a series of results obtained by Pierre De Fermat and Leonard Euler He is best known for his analytical formulations of the calculus of variations and mechanics, but what we will be looking at in this project is his internationally-known Four Square Theorem

The Uses of Langrange's Theorem

Due to the theorem being correct we can use it in various computer systems and programming and can be sure the program will be correct. Lagrange's theorem also proves Fermat's Little theorem which can be used in cryptography and other fields. It can be used to find equations of motion for systems that newtons second law is harder to use because of obscure forces. The theorem can also be used in differential geometry called geodesic. It gives the shortest path between 2 points on a curved surface or straight line with respect to the surface.

3 Outline of Theory

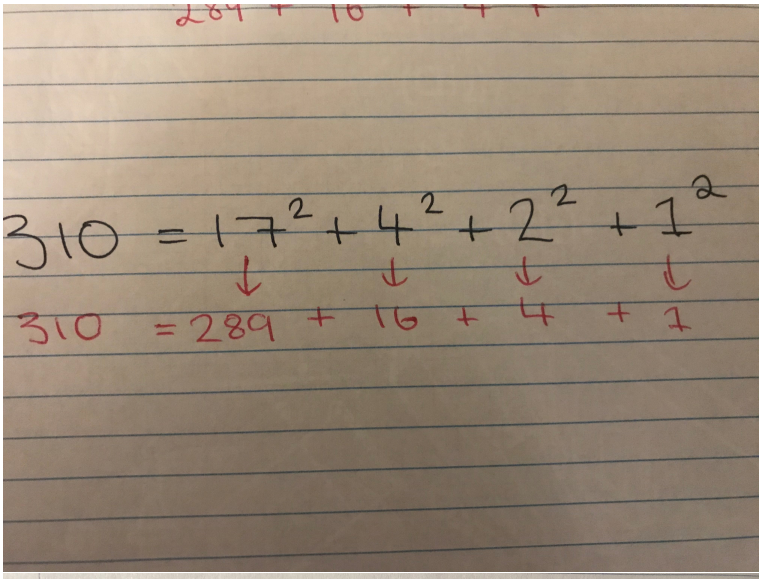
Langranges square theorm: Every natural number n can be written as $n = a^2 + b^2 + c^2 + d^2$ Where a, b, c, d are positive integers Such as $1 = 1^2 + 0^2 + 0^2 + 0^2$

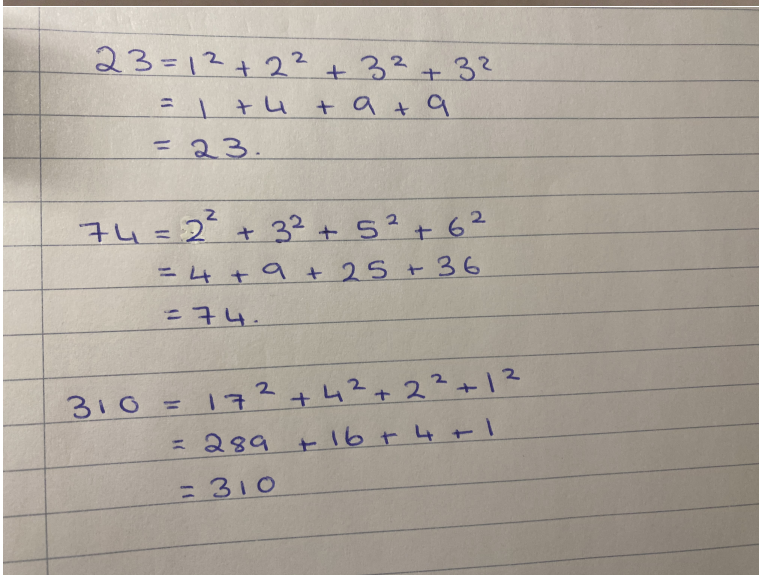
Square theorm or Bachet conjecture, compiled by Bachet for the lack of status mentioned by Diophantus. It says that the whole number can be written as the number of four squares. Theory was proven by Fermat using infinite descent, but the evidence was not published. Euler could not prove this point but helped to establish Langranges. The first published evidence was provided by Lagrange in 1770 and used Euler's four-square-one identity.

Euler's four-square identity tells us that the product of two numbers, each of which is a sum of four squares, is actually a sum of four squares . Which is like the following format below.

$$
\begin{aligned}
&(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\
&(a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + \\
&(a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 + \\
&(a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + \\
&(a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2.
\end{aligned}
$$

4 Examples


310 = 17² + 4² + 2² + 1²
310 = 289 + 16 + 4 + 1


23 = 1² + 2² + 3² + 3²
= 1 + 4 + 9 + 9
= 23.
74 = 2² + 3² + 5² + 6²
= 4 + 9 + 25 + 36
= 74.
310 = 17² + 4² + 2² + 1²
= 289 + 16 + 4 + 1
= 310

5 Conclusion

To conclude, Lagrange's square Theorem has various useful functions that we can apply to real world conundrums. This theory discovered in 1770 still helps us understand and solve numerous problems and mathematical puzzles. We cannot give full credit to Joseph-Louis Lagrange's and not recognise Euler's massive contribution with his Four-square identity theorem that catalysed Lagrange's proof.

Pascal's Triangle

Investigating the different number patterns and sequences within the triangle, both obvious and complex and the numerous practical applications

Claire Nolan
Jack Slevin
Cormac Reidy
Molly O' Connor
Jason O' Reilly

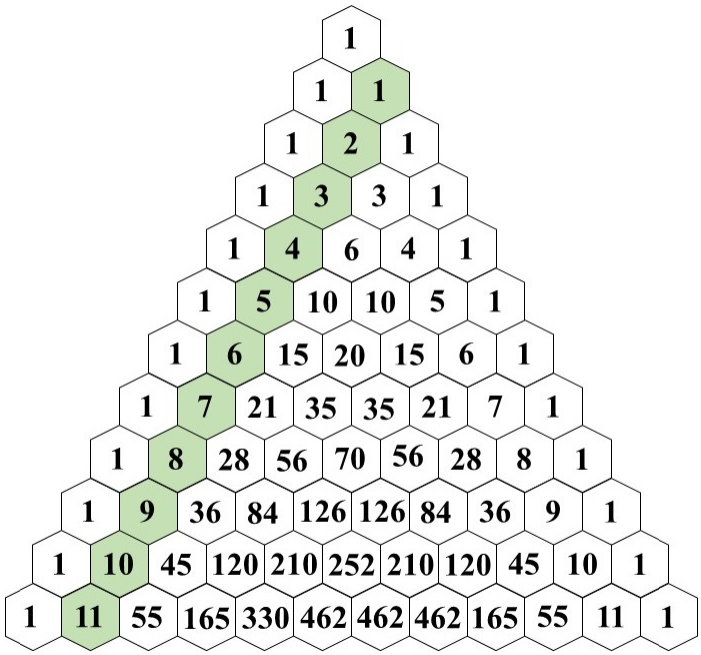
Tutor: Aisling McCluskey

2 November 2020

1 Introduction

Pascal's triangle is a triangular array of numbers in which each row begins and ends with 1 and the numbers in between are the sum of the two numbers directly above them. Although named after French mathematician Blaise Pascal in the 1600s, it dates back centuries before this with evidence of its study found in Persian, Indian and Chinese cultures to name a few. In fact, Chinese Mathematician Jia Xian is credited with writing the triangle out to the 6th row in the 11th century.

This report aims to identify the different patterns that can be seen in the triangle and provide proof where necessary, with particular focus on combinations and binomial expansion and how this can be extended to modular arithmetic.



2 Interesting patterns and observations

- The triangle is symmetrical. The numbers on the left are the same as those on the right
- The 0th diagonal is just a sequence of the number 1
- The first diagonal is the so called counting numbers (1,2,3, etc) These numbers squared are also equal to the sum of the two numbers next to it in the second diagonal.
- The Second diagonal is the triangular numbers (the numbers that can make a triangular dot pattern.) The formula $\frac{n(n+1)}{2}$ can be used to calculate these. For example the 5th triangular number is $\frac{5(5+1)}{2}$ = 15

- The third diagonal contains the tetrahedral numbers. The formula $\frac{n}{3!}(n+1)(n+2)$ is used to calculate these numbers
- The horizontal sum of each row is 2^n. For example the sum of the third row is $1+3+3+1=8=2^3$
- Each row is also the power of 11 ($11^4 = 14641$). This continues up until row 5 when the numbers begin to overlap ($11^5 = 161051$)
- If you shade every multiple of 2, you end up with a pattern the same as the Sierpinski Triangle.
- The Fibonaci Sequence is found in Pascal's Triangle. Every number below in the triangle is equal to the sum of the two numbers diagonally above it to the left and the right, with positions outside the triangle counting as zero

3 Common Applications

- Pascal's triangle can be used in probability theory, when calculating combinations. For example if you have 10 bracelets and you want to choose 2 to wear. The question here is how many different ways can you pick 2 items from a set of 10. Using Pascal's triangle, the answer is the number in the 2nd position on the 10th row (counting from 0). We can see from the diagram above that the answer is 45.

  We can use the general formula ${}_nC_r = \frac{n!}{r!(n-r)!} = \frac{10!}{2!(10-2)!}$ to prove this.

- When multiplying out binomial expressions such as $(x+y)^2$ the coefficients of successive powers of x and y follow the numbers in the appropriate row. For example, the coefficients in row 5 (1, 5, 10, 10, 5, 1) can be seen in the expansion below:

  $(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5x^1y^4 + y^5$

  This pattern makes it easier and saves a lot of time when dealing with complicated equations such as $(x+y)^{10}$

4 Pascal's Triangle and Modular Arithmetic

Consider $(a+b)^p$ mod p. Can Pascal's triangle be extended to modular arithmetic. Fermat's Little Theorem states that if p is a prime number, then for any integer a,

a^p = a (mod p)

ie. a^p and a have the same remainder when divided by p

It's easy to observe that the numbers in the pth row, except for the ends, are divisible by p. For example, when p = 5, the numbers are 1, 5, 10, 10, 5, 1. When p = 7, the numbers are 1, 7, 28, 35, 35, 28, 7, 1.

> *A gambler's dispute in 1654 led to the creation of a mathematical theory of probability by two famous French mathematicians, Blaise Pascal and Pierre de Fermat.*

This led to an exchange of letters between the two, which laid the foundation for probability theory. (Apostol, 1969)

5 Conclusion

Pascal's Triangle is an extremely useful tool available to mathematicians around the world and was created centuries ago. It is extremely useful when calculating the probability of an event happening, with the triangle helping to calculate combinations and also when multiplying out complicated binomial expressions. The triangle's uses in modular arithmetic have also been outlined. Perhaps the most important aspect of Pascal's Triangle is how easy it is to lay out, making it accessible to various age groups. The first few rows could be calculated by primary school children, while third level students can use it whilst studying probability and mathematics. This contributes massively to the Triangle's appeal and popularity.

6 References

- Apostol, T., 1969. Calculus. Vol. II. 2nd ed. New York: Wiley.

Game of Nim

Ellen Grey, Ciarán Stanley, Ciaran Durkan

October 2020

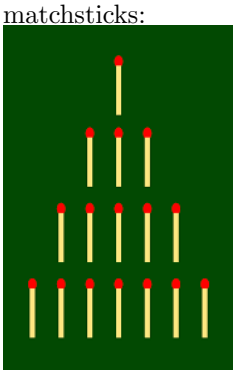
1 Introduction

Workshop Lecturer: Aisling McCluskey

Game of Nim:

The Game of Nim is a mathematical strategy game which originated in China in the 16th century. The game starts off with the two players having several piles containing several objects which range from match sticks to stones, on each turn players alternate in removing at least one of the objects, but each object must come from the same pile, the traditional game consists of four rows of match sticks in the sequence of 1,3,5 and 7 and you could take as many match sticks from each row i.e you could take all 7 matchsticks from the last row but none from any of the others. The game can be won using many different strategies which will be talked about later, but in order to win (depending on the version of the game your playing) you must either avoid taking the last object which is referred to as 'misere' or take the last object which is referred to as 'normal play'. Nim is described as an impartial game which means player no matter who made the first or second move either player can always win. However if the nim sum at the beginning of the game is none 0 and the players dont make any mistakes than the player who started is guaranteed to win. The nim sum is described as cumulative XOR value ob objects in each pile at any point in a game. The XOR value is a function with two inputs and one output in which the output is different to the inputs, mod 2 addition is applied to the XOR function, i.e if the XOR function is 1O1 than this is equal to 1+1 mod 2, which is congruent to 0. This is why one popular strategy is to split the piles into multiples of two.

Figure 1: Example of Nim game with matchsticks:

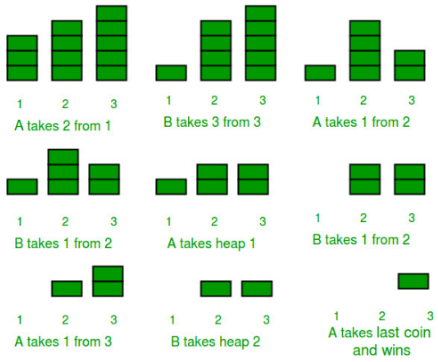


2 Playing the game

2.1 Rules

1. The game starts with two players and several piles (the objects in this case are blocks).
2. A player must take at least one block.
3. A player may take more then one block as long as they all come from the same pile.
4. The game its ends when there is no blocks left.
5. In a game of **'Normal Nim'** the looser is the player unable to move
6. In an alternative variation of the game called **'Misère Nim'**, the player unable to move wins instead; this is equivalent to the player taking the last block losing.

Figure 2: Visual representation of the Nim game seen under the subsection 2.2



2.2 Example game

Table of moves			
Starting number of blocks	Pile1= 3	Pile2= 4	Pile3= 5
Alice	1	4	5
Bob	1	4	2
Alice	1	3	2
Bob	1	2	2
Alice	0	2	2
Bob	0	1	2
Alice	0	1	1
Bob	0	0	1
Alice	0	0	0

From this example, we can see that Alice has won, as she has taken the last block thus leaving Bob unable to make a move. In **'misère play'** Alice would lose instead. Although in this case Alice would have changed her 7th move to take an extra block from the third pile and therefore forcing Bob to take the last block and lose. Alice has played a clever game to win. We will now look at the general game strategy one can use to win the game.

3 General game strategy

3.1 How to win

The winning strategy of Normal Nim is to finish every move with a Nim-sum of 0. If the Nim-sum = 0 after a player's turn, then the next move must change it, meaning there is no way of keeping the Nim-sum 0 after a move if it was 0 before the move.If the Nim-sum = 0 at the start of a game it is impossible to lose if one goes 2nd if no mistakes are made. If the $Nim - sum \neq 0$ at the start and one goes 1st and makes the Nim-sum = 0 after their turn it is impossible to lose without making a mistake.
A common strategy is to reduce the number of heaps to two heaps with the same number of items each. When there is two equal heaps of items the Nim-sum = 0. Now one needs just mimic their opponent's move each time on the opposite heap to keep the two heaps equal until you are able to take the final item.

3.2 The maths of the Nim-sum

Calculating the nim-sum $a \oplus b$:
Take two non-negative integers a and b can be written as sums of distinct powers of two. Cancel powers of two appear twice(mod 2 arithmetic), and add up the remaining numbers(powers of 2).

- Example, $5 \oplus 3$ can be calculated as follows. We have $5 = 2^2 + 2^0 and 3 = 2^1 + 2^0$ We cancel 2^0 for appearing twice, $(1(2^2) + 1(2^1) + 2(2^0) = 1(2^2) + 1(2^1) + 0(2^0) mod 2)$ and 2^1 is the only remaining power of 2 so $7 \oplus 5 = 2$.
- Example, $3 \oplus 5 = 011 \oplus 101$ in binary =110. 110 in binary = 6 in decimal therfore $3 \oplus 5 = 6$.Converting numbers into binary and adding them using mod 2 arithmetic (essentially adding binary but neglecting all carries from one digit to another)
- Alice and Bob Example, $3 \oplus 4 \oplus 5 = (2^0 + 2^1) + (2^2) + (2^0 + 2^2) = 2^1 = 2 = 3 \oplus 4 \oplus 5$

We observe that the nim-sum obeys the following several properties for all integers $a, b, c \geq 0$

- Associativity: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
- Commutativity: $a \oplus b = b \oplus a$
- Identity: $0 \oplus a = a$
- Self-inverse: $a \oplus a = 0$

3.3 proof of winning strategy

Suppose that the move is on pile k; then for all $i \neq k, a_i = b_i$
$t = 0 \oplus t$ (identify)
$= (s \oplus s) \oplus t$ (self inverse)
$= s \oplus (s \oplus t)$ (associative)
$= s \oplus ((a_1 \oplus a_2 \oplus \ldots \oplus a_n) \oplus (b_1 \oplus b_2 \oplus \ldots \oplus b_n))$
$= s \oplus ((a_1 \oplus b1) \oplus (a_2 \oplus b_2) \oplus \ldots \oplus (a_n \oplus b_n))$
$= s \oplus (0 \oplus 0 \oplus \ldots \oplus 0 \oplus (a_k \oplus b_k) \oplus 0 \oplus \ldots \oplus 0)$
$= s \oplus (a_k \oplus b_k)$

If the Nim-sum=0, then the player that makes the next move has no choice but to change the Nim-sum to a non zero value. If s=0, then $t \neq 0$.The moving player is losing (they must make the nim-sum nonzero).
We claim that $x_k \oplus y_k \neq 0$ Indeed, suppose it is, then

$$\begin{aligned} x_k &= x_k \oplus 0 \text{ (identity)} \\ &= x_k \oplus (x_k \oplus y_k) \\ &= (x_k \oplus x_k) \oplus y_k \text{ (associative)} \\ &= y_k. \end{aligned}$$

Thus $x_k = y_k$ But this contradicts the fact that the moving player moved on pile y_k and thus must make the size different.
therefore since $x_k \oplus y_k \neq 0$ we have

$$\begin{aligned} t &= s \oplus (x_k \oplus y_k) \\ &= 0 \oplus (x_k \oplus y_k) \\ &= x_k \oplus y_k \\ &\neq 0. \end{aligned}$$

If $s \neq 0$, it's possible to make t = 0. If the Nim-sum of the originally is not zero, the moving player is winning (they can make the nim-sum zero). Consider the largest power of 2, 2^k, not greater than s. There must be at least one x_i such that it also contains 2^k, otherwise 2^k cannot appear in s. Now, take $y_i = s \oplus x_i$.The value y_i decreases by 2^k, and increases by at most $2^{k-1} + 2^{k-2} + \ldots + 2^0 = 2^k - 1$(each remaining powers of 2 making up s adds to the value; for example $s = 2^2 + 2^1 + 2^0$ and $x_i = 2^3 + 2^2$ gives $y_i = 2^3 + 2^1 + 2^0$, so $x_i < y_i$. Moreover,

$$\begin{aligned} t &= s \oplus (x_i \oplus y_i) \\ &= s \oplus (x_i \oplus (s \oplus x_i)) \\ &= (s \oplus s) \oplus (x_i \oplus x_i) \text{ (associative)} \\ &= 0. \text{ (self inverse)} \end{aligned}$$

Therefore proving the fact a player moving while the Nim-sim = 0 have no choice but to change the Nim-sum to a non zero value, but if the Nim-sum $\neq 0$ the moving player can change the Nim-sum=0 .

4 Reference page

1. http://web.mit.edu/sp.268/www/nim.pdf
2. https://brilliant.org/wiki/nim/
3. https://plus.maths.org/content/play-win-nim

Maths and Magic Tricks!

Maeve Meehan, Paulina Krungleviciute, Patrick Horne, Roc Mehigan.

November 2020

1 Introduction

Is it magic or is it maths? Maths can explain and solve many undecipherable problems, but is it magic? Try this trick! Step 1:Think of a number, any number. Step 2:Multiply it by 3. Step 3:Add 6. Step 4:Divide this number by 3. Step 5:Subtract the number in step 1 from the answer in step 4. Abracadabra, your number is 2. So there is some magic in the universe and it can be seen in maths.

Figure 1: The Universe

Is this trick really magical maths or is it just a coincidence? Let us try another trick. First, think of any three-digit number where all 3 of the digits are the same like, 333 or 666. Now add up the digits and divide the three-digit number by your answer. The answer is 37.

2 Conclusion

"I always thought something was fundamentally wrong with the universe" [**?**]

3 Is It Maths Or Is It Magic ?

Ever wonder what is the magic behind a magic trick ? Or do you just sit there amused at the "magic" trick that someone perfected the performance of to the

tiniest details ? Well, either way, today I will reveal the maths behind quite an impressive magic trick.

3.1 Imagine this

Imagine this. A magician hands out a 3 or 4-digit integer chosen by yourself. Using a calculator, your friend multiplies this number by some secret 3-digit number which they choose freely and keep for themselves. Either one of you withholds one of these digits and reveals all the others in a random order. The magician then goes onto revealing the withheld digit and both of you are astounded by the fact that he actually got it correct. So the question now is how ?

3.2 The Secret

This trick is based on arithmetic modulo 9, which is what underlies the process of casting out nines from an integer. Casting out nines is a quick way to obtain the remainder when an integer N is divided by 9.The key observation is that 10 and all the powers of 10 leave a remainder of 1, therefore, a number and the sum of its digits leave the same remainder. in simpler terms, the number handed out by the magician is a multiple of 9. Therefore, the result a multiple of 9 and the sum of all its digits is a multiple of 9. When all the digits but one are revealed, the last one is therefore modulo 9. This maths does usually reveal the withheld number unless it is 0 or 9. In an ambiguous case, the magician will guess 9 and almost always be right because people will less than likely skip 0 when told to skip any digit they like. If the magician wants to be extra safe and correct all the time, they would simply instruct his audience to skip a non-zero digit. So there it is, the secret of the magic trick that seemed to be unattainable for someone that does not practice "magic". It turns out that the greatest magicians are great mathematicians and on top of that have great skills with people to make them in awe of what they do best.

4 Simple Yet Amazing

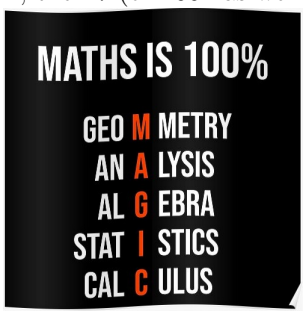
The explanation of these tricks is usually behind some very simple mathematics, but the subjects usually aren't too bothered in working it out. This helps the 'magician' keep up the act and keeps the people in awe. A few examples of these are "Hailstone Numbers" and "Three Digits Become Six"

4.1 Hailstone Numbers

First choose any number at all. Now is the number odd or even? If it is even, take your number and divide it by 2; if it is odd, take the number, multiply it by 3 and add 1. Repeat this step over and over. Eventually you will reach the goal of the number 1. For example take the number 59. It's odd so I'll multiply by 3 and add 1, and repeat my step over and over until I reach 1. 59 ¿ 178 ¿ 89 ¿ 268 ¿ 134 ¿ 67 ¿ 202 ¿ 101 ¿ 304 ¿ 152 ¿ 76 ¿ 38 ¿ 19 ¿ 58 ¿ 29 ¿ 88 ¿ 44 ¿ 22 ¿ 11 ¿ 34 ¿ 17 ¿ 52 ¿ 26 ¿ 13 ¿ 40 ¿ 20 ¿ 10 ¿ 5 ¿ 16 ¿ 8 ¿ 4 ¿ 2 ¿ **1** Admittedly, this took much longer than anticipated, but that only helps my case that this is magic, as no matter how long it goes on, you will always reach 1. The trick behind this is the adding of 1 after multiplying by 3. This guarantees the next number will be even therefore making the number half. Every now and again you'll get a streak of even numbers so your number drops closer and closer to the 1 mark.

4.2 Three Digits Become 6

Pick any three digit number at all. Multiply the number my 7, then by 11, then by 13. Your 3 digit number will appear twice in a 6 digit number. For example **724**: 724*7=5068 ¿ 5068*11=55748 ¿ 55748*13=**724724** This trick is even more simple than the last, here's why: 7*11*13 = 1001. Any 3 digit number multiplied by 1001 equals itself repeated twice. The 1001 being broken down into three numbers multiplied tricks the audience into thinking the trick is much more complex than it actually is. This trick works the other way also, starting with a six digit number in the form of XYZXYZ, then dividing by 13, then 11, then 7 (or 1001 as we know).



5 In Conclusion

Magic tricks will always amaze the masses, the key word to pay attention to though, is **tricks**, there's always a trick to them and often this can be worked out with mathematics, it's all down to whether you're interested enough to find this out. The more you learn the more magic you find within maths.

Pascal's Triangle

Fiachra Gavin, Daire Elberse, Ailbhe Keane, Tom Farrell.

November 2020 Aisling McCluskey

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

1 Introduction

2 10 bracelets problem

3 How are these related

4 $(a+b)^p$ mod p for some prime p

Introduction

Pascal's triangle is a triangular array constructed by summing adjacent elements in preceding rows. Pascal's triangle contains the values of the binomial coefficient. It is named after the 17th century French mathematician, Blaise Pascal (1623 - 1662)

To construct Pascal's triangle begin by placing a 1 at the top center of a piece of paper. The next row down of the triangle is constructed by summing adjacent elements in the previous row. Because there is nothing next to the 1 in the top row, the adjacent elements are considered to be 0. This process is repeated to produce each subsequent row and this can be repeated infinitely. The first 8 rows should look like this.

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

One of the biggest uses of Pascal's triangle is the binomial theorem which can be used to expand numbers in the form $(x + y)^n$ using Pascal's triangle.

10 bracelets problem

If you have 10 different bracelets, how many ways can you choose exactly two of them to wear?

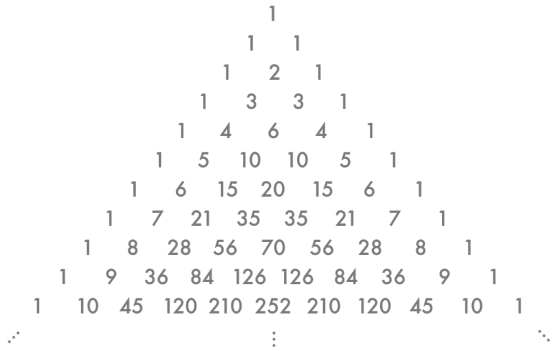
We can begin with labeling each bracelet A-J. There are 9 combinations that include bracelet A. (A and B ,A and C ,A and D....) For bracelet B there is 8 different combinations (because we have already counted the combination counted A and B). As we go through the bracelets we notice that each bracelet has one less combination then the previous. Then we add all the combinations together to get our final answer i.e. 9+8+7+6+5+4+3+2+1 or 10C2 = 45.

How are these related?

These problems are related to Pascal's Triangle as the triangle also shows you how many combinations of objects are possible. For example with the 10 bracelets problem,you have 10 bracelets how many different ways could you choose just 2 of them (ignoring the order that you select them)?

Go down to the start of row 10 (the top row is 0) and then go across 2 places (the first place is 0) and the value there is your answer, 45.

Here is an extract at row 10



In fact there is a formula from combinations for working out the value at any place in Pascal's Triangle. It is commonly called "n choose k" and is written like this

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

So Pascals Triangle could also be a binomial coefficient triangle like the one below

$$\binom{0}{0}$$
$$\binom{1}{0}\ \binom{1}{1}$$
$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$
$$\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3}$$
$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$$
$$\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}$$

This allows us to work out any value in Pascal's Triangle directly.

because P choose k is a multiple of k whenever k=1. By using Fermat's little theorem that states if p is a prime number then $a^p = a(modp)$ for any integer a and so this is true for a=a+b hence the binomial formula reduces to (a+b)$^p x + y(modp)$.

Game of Nim

Eve Regan, Konrad Kizielewicz, Luke Roberts, Moya Reynolds, Tomás Nolan

Workshop lecturer: Dr. Aisling McCluskey

November 2020

Project brief

Game of Nim - In this game two players have three piles of coins. Players take turns removing coins from one pile at a time. The goal is to take the very last coin. Is there a winning strategy? You'll use mod 2 arithmetic. You'll also learn about the "nim-sum" which is an operation satisfying some familiar properties. Which properties does it satisfy?

Introduction

Nim is a game where two players take turns removing coins from different piles. The objective of the game is to remove the very last coin. In this project we are going to address what is the winning strategy for this game, what is Nim-Sum and what are some of its properties.

What is Nim-Sum?

Nim-sum, is the digit-wise modulo 2 sum of the heap sizes expressed as binary numbers. To explain clearly what this means, lets walk through an example of how you calculate nim-sum.

In this example there are three stacks of coins which have 2, 3 and 5 coins respectively. First you need to write the number of coins in each stack in their binary expansions

$$2 = 010$$
$$3 = 011$$
$$5 = 101$$

Now that we have each stack written individually in binary, we add them together along the columns mod 2

$$\begin{array}{r} 010 \\ 011 \\ 101 \\ \hline 100 \end{array}$$

So our value for Nim-Sum in this example 111. The value of Nim-Sum changes every round of the game as coins are removed, and the configuration of the stacks changes.

Properties

Because calculating the Nim-Sum is similar method to addition it carries some similar properties. Consider a Game of Nim with three piles of coins, with a, b and c coins, respectively, the following properties are satisfied:

1. **Nim-Sums are commutative:** - $a \oplus b = b \oplus a$
   This means that the order, either $a \oplus b$ or $b \oplus a$, has no influence on the output

2. **Nim-Sums are associative:** - $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
   Nim-sums are associative, this means that no matter how the elements are grouped, $(a \oplus b) \oplus c$ or $a \oplus (b \oplus c)$, the outcome will be the same

3. $a \oplus a = 0$
   This third property is an unfamiliar one. It means that the nim sum of any stack and itself, $a \oplus a$, will always be 0 no matter what the value of the stack is.

4. $a \oplus b \neq 0$ provided that $a \neq b$
   This is another property of nim sum meaning that the nim sum of two stacks, a and b, will never be 0 so long as a and b are not equal

Winning Strategy

Tthe winning strategy is to always ensure your turn reduces the opponent's Nim-Sum to 0. If both players make use of this theorem then the one who starts at a total Nim-Sum of 0 will always lose. To prove this requires the use of the following two lemmas.

Lemma 1 - If a player finishes their turn with a Nim-Sum of 0, the next player's turn must change that. This is proven below
Let,
Piles of coins = x_1, x_2, x_3
Piles of coins after the moves = y_1, y_2, y_3
s = Nim-Sum
t = the Nim-Sum of the heaps after any move

$$\begin{aligned} t &= 0 \oplus t \\ &= s \oplus s \oplus t \\ &= s \oplus (x_1 \oplus x_2 \oplus x_3) \oplus (y_1 \oplus y_2 \oplus y_3 \oplus) \\ &= s \oplus (x_1 \oplus y_1) \oplus (x_2 \oplus y_2) \oplus (x_3 \oplus y_3) \\ &== s \oplus x_k \oplus y_k \end{aligned}$$

This Lemma shows that if a player begins their turn on a nim-sum of 0, they will always finish it on a non-zero nim-sum. This is because the total of one pile of coins will have changed, therefore changing the nim-sum

Lemma 2 - A player can always end their turn with a Nim-Sum of 0, provided the Nim-Sum was non-zero at the begining of their turn
Let,
Nim-sum of the coins per pile = K = $y_1 \oplus y_2 \oplus \dots y_n$
Choose a pile x_m

$$\begin{aligned} K &= s \oplus x_m \oplus y_m \\ &= s \oplus x_m \oplus x_m \oplus s \\ &= s \oplus s \oplus x_m \oplus x_m \\ &= 0 \end{aligned}$$

Lemma 2 is essentially the reverse of Lemma 1, showing that a player starting their turn on a non-zero nim sum is always able to end their turn on a nim-sum of 0.
These lemmas illustrate that if player 1 starts with a non zero nim-sum, they will always be able to change it to 0 and in turn player 2 will have to make the nim-sum non-zero. If player one plays using the winning strategy throughout, they will eventually win the game by taking the last piece.

References

As a reference for our lemmas we used:
2009, Theory of impartial games, MIT, accessed November 2020: link to Theory of impartial games pdf

Project: Casting Out Nines

Aoife Clarke, Róisín Culligan, Siobhan O' Riordan,
Hannah Cummins, Eloise Donohoe
MA180

November 6, 2020

Abstract

This paper will provide a concise introduction into the mathematical process of 'casting out nines'. Within this process there are subdivisions pertaining to the application of 'casting out nines' in the 4 mathematical procedures of addition, subtraction, multiplication and division. The method can be used to check accurately and concisely if an equation has been computed correctly. This process has been in use for centuries, it can be traced back to Hindu-Arabic scholars of the Middle Ages (Lauber, M., 1990). The modern invention of the pocket calculator has caused the method to fall out of everyday use. However, in our opinion the knowledge of this method greatly enriches a mathematical science student's development and understanding of mathematics.

1 Introduction

'Casting out nines' is an arithmetic process. It involves adding all of a positive integer's decimal digits, while optionally ignoring any 9s or digits that amount to a multiple of 9. It uses the congruence:

$$9^n \equiv 0 \pmod 9 \tag{1}$$

The procedure is repeated until a final single digit integer is found. This final digit is called the 'digital root' of the original integer.

2 Addition

91234 → (1) we 'cast out' numbers that are multiples of 9 or sum to 9
+ 49263 → (4+2=6) again we 'cast out' 3,6 and 9 as 3+6=9
+ 13211 → (1+3+2+1+1=8) no multiples of or sums to 9
153,708 (1+6+8=15)
↓ ↓
(15) →→→ (1+5=6)

This example using addition shows that the digital roots of the addends and sum are equal after 'casting out nines'.

3 Subtraction

7541 → (8) we 'cast out' numbers that are multiples of 9 or sum to 9
- 1462 → (4) again we 'cast out' 1,2 and 6 as 1+2+6=9
- 2413 → (1) 2,3 and 4 are 'casted out' as they sum to 9
3666 (8-4-1=3)
↓ ↓
(12) →→ (1+2=3)

This example using subtraction shows that the digital roots of the addends and sum are equal after 'casting out nines'.

4 Multiplication

9170 → (8) we 'cast out' numbers that are multiples of 9 or sum to 9
x 852 → (15) we cannot 'cast out' as there are no multiples of or sums to 9
x 18 → (0) 8 and 1 are 'casted out' as they sum to 9
140,631,120 (8x15x0=0)
↓ ↓
(0) →→→ (0)

This example shows using multiplication that the digital roots of the addends and sum are equal after 'casting out nines'.

5 Division

372451 ÷ 241 = 1545 R 106
↓ ↓ ↓ ↓
4 (7 x 6) + 7 = 49 → 4+9=13 → 1+3=4

This example shows using division that the digital roots of the addends and sum are equal after 'casting out nines'.

6 Limitations to Casting Out Nines

- Casting Out Nines is very useful, however, it does not catch all errors made while doing calculations. For example, the Casting Out Nines method would not recognize the error in a calculation of 5×7 which produced any of the erroneous results 8, 17, 26, etc, that is, any result congruent to 8 modulo 9.
- The method only catches erroneous results whose digital root is one of the 8 digits that is different from that of the correct result.

7 Practical Applications to Casting Out Nines

- The method of Casting Out Nines is often used to verify correct credit card numbers. A secret formula is applied to the last four digits of a credit card. If the result is determined to be evenly divisible by nine, by casting out nines, then the number is considered to be valid.
- Casting Out Nines is occasionally used by computer programs to verify that data has been transmitted correctly. Nine is cast out of both the original data and the copy, and the two results are compared. The fact that this method will overlook transposed numbers makes it somewhat unreliable

8 Remarks

Though it has limitations, the mathematical procedure of 'casting out nines' has multiple beneficial uses. Based on a modulo 9 congruence, it is a concise and accessible method that can be used even with no prior knowledge of modular arithmetic. The ability to check if equations have been computed correctly allows for an expedience within calculations should a calculator or calculating program not be available. The mathematics behind the process is a fantastic insight into modular arithmetic as a whole. The timeline behind the procedure shows the depth of mathematical science's history and gives students a greater understanding of the prevalence of mathematics through the ages. In conclusion the procedure can be summarised as follows:
Take two numbers X and Y. Let their product be Z. Let the sums of their digits be A B and C respectively. This will imply the following:

$$X \equiv A \pmod 9 \tag{2}$$

$$Y \equiv B \pmod 9 \tag{3}$$

$$Z \equiv C \pmod 9 \tag{4}$$

9 Bibliography

[1] Wolfram Mathworld. https://mathworld.wolfram.com/CastingOutNines.html
[2] Lauber, M., 1990. Casting out nines: an explanation and extensions. The Mathematics Teacher, 83(8), pp.661-665

https://www.saddleback.edu/faculty/pquigley/teacher/cast$_o ut_9 .pdf$

$https : //en.wikipedia.org/wiki/Casting_o ut_n ines : \ : text = Limitation$

There are Infinitely many Prime Numbers

WS3 Project-Group 2: Kate, Asha, Ella, Doireann, Jack

October 2020

1 Introduction

In this project we wish to present a number of different proofs for **Euclid's Theorem; *That there are infinitely many primes.*** Euclid first proved this c.300 BC, and since then there have been a several more proofs devised. We will be looking at:

1. Euclid's Proof c.300 BC
2. Goldbach's Proof 1730
3. Furstenberg's Topological Proof
4. Filip Saidak's Proof

2 Euclid's Proof

- **Theorem:** There is no finite list of prime numbers.
- **Proof:**

We start by assuming that there is a finite list of primes.

$$p_1, p_2, p_3 \ldots, p_n$$

We take a number N as the product of these primes plus one.

$$N = p_1 p_2 p_3 \ldots p_n + 1$$

As we are assuming that there is a finite list of primes, then N can't be a prime number. We also know that all non-prime numbers can be written as a product of prime numbers. (Fundamental Theory of Arithmetic)
For example:

$$42 = 2 \times 3 \times 7$$

However N isn't divisible by any of the primes in our finite list, as none of them can divide 1.

Therefore N must either be a prime, or is divisible by a prime, which isn't among our finite list of primes;

$$p_1, p_2, p_3 \ldots, p_n$$

Either way, this contradicts our original assumption and proves that:
There is no finite list of prime numbers.

3 Goldbach's Proof

Goldach's proof uses the Fermat numbers, which are defined as:

$$F_n = 2^{2_n} + 1 \quad \text{for} \quad n = 0, 1, 2, 3 \ldots$$

- **Theorem:**
  There is no finite list of prime numbers.
- **Proof:**

First we show that any two distinct Fermat numbers are relatively prime.
Using the induction hypothesis, we can show that

$$F_n - \prod_{i=0}^{n-1} F_i = 2 \quad (n \geq 1)$$

Let d be a divisor of two distinct Fermat numbers F_m *and* F_n.
Then, d divides 2 and *hence*, d= 1 or 2
But d= 2 is not possible since all Fermat numbers are odd... Therefore, d= 1.
Thus, prime divisors of distinct Fermat numbers will be distinct as they are *infinitely* many Fermat numbers, *infinitely* many distinct prime numbers will exist.

4 Furstenberg's Topological Proof

- **Theorem**:
  There are an infinite number of primes
- **Proof**:
  Using Arithmetic Sequences $-/+\infty$ as support, define a toplogy on the set of integers *"Z"*. Declare the subset A, to be part of the set of integers Z. A is an open subset if it is an empty set,$A \neq 0$, or if it is part of arithmetic sequences S(a,b) where A is not equal to 0.
  S(a,b)= $an + b|\ n \in Z$ + *a Z.*
  Prime = p. Let A_p consist of all multiples of p. A_p is closed because:.

  A'= union of all other arithmetic progressions with a difference of p.
  Let $A = U$ *of progressions* A_p.
  If the Number of primes is *limited*, then A is a *limited* union of closed sets.
  All integers except -1 and+1 are multiples of a prime.

A'= -1,1 ≠ open set.
Therefore A is not a limited prime and **Furstenberg's Theorem** that there is an infinitude of Primes is **True**.

5 Filip Saidak's Proof

- **Proposition**: There are infinitely many prime numbers
- **Proof:**

  We assume that n > 1 is a positive integer. Since n, n+1 greatest common divisor is 1, they are coprimes

  We take a number N as the product of these coprimes. Coprime means that two numbers share no common prime factors. n and n+1 share no prime factors, so n(n+1) must have at least 2 prime factors.Hence, the number N must have ***at least*** *two prime numbers.*

  $$N = n(n+1)$$

  Similarily, the numbers n(n+1) and n(n+1)+1 are consecutive, and hence coprime, the number

  $$N_2 = n(n+1)n(n+1) + 1$$

  must have at least three different prime factors. This continues indefinitely, proving the number of prime numbers is infinite.

Canonical Representation

Workshop tutor: Tobias Rossmann

Martyna Bajdak, Rachel Gbinigie, Nial O'Reilly,
Keelin Stafford, Adam Rafter

28 October 2020

1 Introduction

1.1 Definition

The canonical decomposition of an integer is a unique form of factorization in which a number is represented as a product of its primes, with the resulting factors written in ascending order.

The canonical decomposition of a positive integer n is of the form:

$$n = {p_1}^{a_1} {p_2}^{a_2} \dots {p_k}^{a_k}$$

,where p_1, p_2, . . . , p_k are distinct primes with $p_1 < p_2 < \cdots < p_r$ and each exponent ak is a positive integer. There are two commonly used techniques for finding the canonical decomposition of a composite number. The first method involves finding all prime factors, beginning with the smallest prime, as the following example demonstrates. A canonical form specifies a unique representation for every object, while a normal form simply specifies its form, without the requirement of uniqueness.

1.2 Existence

The Fundamental Theorem of Arithmetic states that every natural number greater than 1 can be written as a unique product of prime numbers. This means that every natural number greater than 1 has its own unique prime representation.

Proof. It's known that 2 is a prime. Let's assume, by strong induction that this applies to every number 1 < x < n. If n is a prime, then there's nothing to prove. However if n is a product of primes such that $n = a \cdot b$, with 1<a,b<n. Therefore, n is always a product of primes; as $n = n \cdot 1$, if n is a prime, or $n = a \cdot b$ □

This property is fundamental cryptosystems such as RSA encryption because when you multiply two prime, the result is a number that can only be broken down into those primes, itself and 1.

1.3 Uniqueness

Proof. Assume that integer n is the product of prime numbers in two different ways:

$$n = p_1 p_2 \dots p_i = q_1 q_2 \dots q_j$$

According to Euclid's Lemma(*If a prime p divides the product ab of two integers a and b, then p must divide at least one of those integers a and b.*), since q_1, q_2, ... q_j are co-prime integers, p_1 must divide one of them. Since p_1 is the smallest, then $p_1 = q_1$. Using this method we arrive at: $p_i = q_j$, or $i = j$. Therefore, the combination of primes is the same and that canonical representation is.

□

2 Methods for finding canonical decomposition

2.1 Method 1

Problem 1. *Find the canonical decomposition of 2520.*

Solution 1. Beginning with the smallest prime 2, since 2520 is divisible by 2 ($2520 = 2 \cdot 1260$). Now 2 is also a factor of 1260, with $1260 = 2 \cdot 630$, so $2520 = 2 \cdot 2 \cdot 630$. Again, 2 is a factor of 630, so $2520 = 2 \cdot 2 \cdot 2 \cdot 315$. Now 315 isn't divisible by 2, but it is by 3, so $2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 105$; 3 is a factor of 105 also, so $2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 35$. Continuing like this we get $2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ which is the desired canonical decomposition

Remark 2. This method can be quite time consuming if the integer is fairly large

2.2 Method 2

The second method, which is generally more efficient, involves splitting n as the product of two positive integers, not necessarily prime numbers, and continuing to split each factor into further factors until all factors are primes. To make this method short, its best to look for large factors; the fewer factors there are, the fewer steps required

Problem 3. *Find the canonical decomposition of 2520 by the second method.*

Solution 2. Notice that $2520 = 40 \cdot 63$. Since none of the factors are primes, split them again: $40 = 4{\cdot}10$ and $63 = 7{\cdot}9$, so $2520 = (4{\cdot}10) \cdot (7{\cdot}9)$. Since 4, 10, and 9 are composites, split each of them: $2520 = (2 \cdot 2)(2 \cdot 5)(7)(3 \cdot 3)$. Now all the factors are primes, so the procedure stops. Rearranging them yields the canonical decomposition: $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

The diagram below, known as a factor tree is a visual representation of the second method : if one integer is divisible by another, they are connected by a line. Figure 1 shows the factor tree for 2520 using the steps from method 2: To find the canonical decomposition, simply take the product of all primes at the "leaves": $2520 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 3 \cdot 3 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

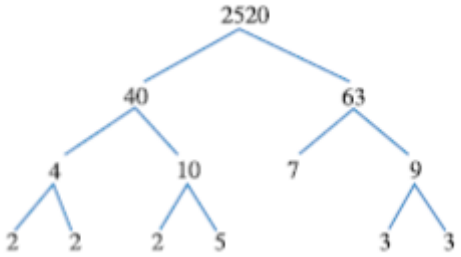


Figure 1: Factor Tree

3 Applications

3.1 Greatest Common Divisor

The GCD of 2 integers is is the largest positive integer that divides each of the integers. Canonical decomposition of an integer can also be used to find the GCD of two numbers.

Proof. Let a and b be positive integers with the following canonical decomposition

$$a = {p_1}^{a_1} {p_2}^{a_2} \dots {p_n}^{a_n} \quad \text{and} \quad b = {p_1}^{b_1} {p_2}^{b_2} \dots {p_n}^{p_n}, \quad \text{where} \quad a_i, b_i \geq 0$$

.. (By letting exponents zero, we can always assume that both decomposition contain exactly the same prime bases p_i.) Then

$$(a, b) = {p_1}^{min(a_1;b_1)} \cdot {p_2}^{min(a_2;b_2)} \dots {p_n}^{min(a_n;b_n)}$$

□

Using this proof, we can solve problem 4

Problem 4. *Find the greatest common divisor of 89346 and 223365*

1. Firstly, break down each number into their primes
2. 89346= $2 \cdot 44673$
   - 2 is a factor of 89346
   - 2 is not a factor of 44673
3. However 44673= $3 \cdot 14891$, with 14891 being a prime number.
4. Therefore 89246 in canonical form is

   $$89246 = 2 \cdot 3 \cdot 14891.$$

   Using the same method, 223365 in canonical form is

   $$223365 = 3 \cdot 5 \cdot 14891$$

5. We now see that 89346 and 223365 have two common divisors, 3 and 14891, which can also be written as:

   $$(89246, 223365) = 2^{min(1;0)} \cdot 3^{min(1;1)} \cdot 14891^{min(1;1)}$$

   The Greatest common divisor of these two numbers is therefore:

   $$14891 \cdot 3 = 44673$$

3.2 Least Common Multiple

The least common multiple of 2 integers a and b is the smallest possible integer that is divisible by both a and b. Much like the gcd, canonical decomposition can be used to find the lcm of 2 integers.

Proof. Let a and b be positive integers with the following canonical decomposition

$$a = {p_1}^{a1}{p_2}^{a2}\dots{p_n}^{an} \quad \text{and} \quad b = {p_1}^{b1}{p_2}^{b2}\dots{p_n}^{pn}, \quad \text{where} \quad a_i, b_i \geq 0$$

. (Again, we assume that both decompositions contain exactly the same prime bases p_i.) Then:

$$(a, b) = {p_1}^{max(a_1 \cdot b_1)} \cdot {p_2}^{max(a_2 \cdot b_2)} \dots {p_n}^{max(a_n \cdot b_n)}$$

□

Problem 5. *Find the Least Common Multiple of 9116 and 2002*

1. Firstly, just like for the GCD, break the integers down into primes
   - $2002 = 2 \cdot 7 \cdot 11 \cdot 13$
   - $9116 = 2^2 \cdot 43 \cdot 53$
2. Then, we use the equation from the proof
   $$(2002, 9116) = 2^{max(1;2)} \cdot 7^{max(1;0)} \cdot 11^{max(1;0)} \cdot 13^{max(1;0)} \cdot 43^{max(0;1)} \cdot 53^{max(0;1)}$$
3. Finally, we calculate the product of the multiplication
   $$LCM = 2^2 \cdot 7 \cdot 11 \cdot 13 \cdot 43 \cdot 53 = 9125116$$
   9125116 is the least common multiple of 2002 and 9116.

References

[1] `https://brilliant.org/wiki/prime-factorization/`

[2] `https://www.mathsisfun.com/prime-factorization.html`

[3] `https://www.coursera.org/lecture/number-theory-cryptography-existence-of-prime-factor`

[4] Thomas Koshy, Elementary Number Theory with applications, 2nd ed. (Academic Press 2002)

[5] `https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic`

The modern proof of the Chinese Remainder Theorem

Project Group 3: Precious Olotu, Mia Shanley-Brookes, Michael Harrold

November 6, 2020

Tutor; Tobias Rossman

1 Introduction

The Chinese remainder theorem (CRT) states that if we are aware of the remainders of the Euclidean division of an integer 'n' by several other integers, then one can ascertain through analysis or investigation uniquely the remainder of the division of 'n' by the product of these integers 'n' circumstances different from those present or considered that the divisors are pairwise Co-prime.

1.1 Background, O.G Use, and The Actual Theorem

Background: The earliest known statement of the theorem, as a problem with specific numbers, appears in the 3rd-century book Sun-tzu Suan-ching by the Chinese mathematician Sun-tzu:

There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there¿'

Sun-tzu's work contains neither a proof nor a full algorithm. What amounts to an algorithm for solving this problem was described by Aryabhata in the 6th century. Special cases of the Chinese remainder theorem were also known to Brahmagupta in the 7th century, and appear in Fibonacci's Liber Abaci (1202).The result was later generalized with a complete solution called Ta-yan-shu in Ch'in Chiu-shao's 1247 Mathematical Treatise in Nine Sections, (Shu-shu Chiu-chang) which was translated into English in early 19th century by British missionary Alexander Wylie.

The notion of congruence's was first introduced and used by Gauss in his Disquisitiones Arithmeticae of 1801. Gauss illustrates the Chinese remainder theorem on a problem involving calendars, namely, "to find the years that have

a certain period number with respect to the solar and lunar cycle and the Roman in-diction. Gauss introduces a procedure for solving the problem that had already been used by Euler but was in fact an ancient method that had appeared several times.

The original use

The Chinese remainder theorem is widely used for computing with large integers, as it allows replacing a computation for which one knows a bound on the size of the result by several similar computations on small integers. It can be likened to sorting a basket of eggs, but not knowing how many eggs are in the basket, but one knows that if they take out n number of eggs they have n amount leftover, and if they take another n amount of eggs they have another amount of n left over. Therefore according to the Chinese remainder theorem, this is enough information to solve the problem of figuring out the least number of eggs that one could have in the basket.

The Actual Theorem: 'The Chinese remainder theorem states that a linear system of congruence equations with pairwise relatively prime moduli has a unique solution modulo the product of the moduli of the system.'

Requirements for the theorem to be applied:

- The number has to be co-prime eg.

  The G.C.D (Greatest Common Divisor) of the integers must be equal to 1 for all of them to be Co-prime.

- A given remainder for each euclidean division of a co prime divisor

2 The Theory: Problem 1

We are looking for the smallest non negative integers, x, such that these statements hold true.

$x \equiv 1\ Mod\ 2$
$x \equiv 7\ Mod\ 3$
$x \equiv 3\ Mod\ 5$

We must first ensure that all values for n ($Mod\ n$) are Co-prime before we continue.
The G.C.D (Greatest Common Divisor) of the integers must be equal to 1 for all of them to be Co-prime.

$(G.C.D)\ (2,3) = 1$
$(G.C.D)\ (2,5) = 1$
$(G.C.D)\ (3,5) = 1$

Now we know that they all values of n are Co-prime we can continue with the Chinese remainder theory.

Solution;
Let; Step 1

a$\equiv 3^{-1}$Mod2
b$\equiv 5^{-1}$Mod2

A first attempt at solving this system is

$X\equiv 1 \times 3\times$a$\times 5\times$b

X=1 Mod 2
X=0 Mod 3
X=0 Mod 5

Step 2

c$\equiv 2^{-1}$Mod3
d$\equiv 5^{-1}$Mod3

A second attempt at solving this system is

Y=7$\times$2$\times$c$\times$5$\times$d

Y=0 Mod2
Y=7 Mod3
Y=0 Mod5

Step 3

e$\equiv 2^{-1}$Mod5
f$\equiv 3^{-1}$Mod5

A third attempt at solving this system is

z=3$\times$2$\times$e$\times$3$\times$f

Z=0 Mod2
Z=0 Mod3
Z=3 Mod5

Combine the three statements and set

$x = X + Y + Z$

Note when attempted with Modn

x=$X + Y + Z$= 1+0+0 Mod2
x=$X + Y + Z$ 0+7+0 Mod3
x=$X + Y + Z$ 0+0+3 Mod5

From here figure out the values of the unknown integers in X,Y and Z;

$a \equiv 3^{-1} \text{Mod} 2$
$= 1 \ Mod 2$

$b \equiv 5^{-1} \text{Mod} 2$
$= 1 \ Mod 2$

$c \equiv 2^{-1} \text{Mod} 3$
$= 2 \ Mod 3$

$d \equiv 5^{-1} \text{Mod} 3$
$= 2 \ Mod 3$

$e \equiv 2^{-1} \text{Mod} 5$
$= 3 \ Mod 5$

$f \equiv 3^{-1} \text{Mod} 5$
$= 2 \ Mod 5$

$X = 1 \times 3 \times \text{a} \times 5 \times \text{b}$
$X = 1 \times 3 \times 1 \times 5 \times 1 = 15$

$Y = 7 \times 2 \times \text{c} \times 5 \times \text{d}$
$Y = 7 \times 2 \times 2 \times 5 \times 2 = 280$

$Z = 3 \times 2 \times \text{e} \times 3 \times \text{f}$
$Z = 3 \times 2 \times 3 \times 3 \times 2 = 108$

$x = X + Y + Z$
$x = 75 + 140 + 108$
$x = 403$

Now to work out the smallest possible value that satisfies the original statement, we must multiply all values of n by each other to create the new Mod.

$2 \times 3 \times 5 = 30$
$x = 403 \ Mod 30$
$\Rightarrow \text{x} = 13 \text{Mod} 30$
Q.E.D

2.1 Theoretical Process Example

This method works because the greatest common divisor of (2,3)=1, (2,5)=1, (3,5)=1

The CRT will works for any system;

$x = \text{a} \ Mod \ \text{l}$
$x = \text{b} \ Mod \ \text{m}$
$x = \text{c} \ Mod \ \text{n}$

with the condition;

$G.C.D(l * m) = 1,$
$G.C.D(l * n) = 1,$
$G.C.D(m * n) = 1.$

This is called The Chinese Remainder Theorem and clearly extends to systems of more than 3 equations.

3 How to apply the CRT ; Problem 2

Suppose we have a system of 3 congruence's;

$x\equiv$ 1mod2
$x\equiv$ 2mod3
$x\equiv$ 3mod5

such that;
G.C.D(2,3) = 1,
G.C.D(2,4) = 1,
and G.C.D(3,4) = 1.

One way to proceed is to solve the system consisting of only the first two congruence's, which gives x d (mod n*m), and then solving the resulting system of two congruence's.
. Let us find x Z such that;

$x \equiv 2,$
$x \equiv 3,$
$x \equiv 5.$

The first step is to find

α, β, γ

$for = [2, 3, 5].$

One way to produce such a trio of numbers is to compute many modulo inverses. To give some idea for how to come by this, for , we want a number divisible by m‘ but which leaves remainder 1 when divided by n. Since their gcd's is 1.

$\alpha \equiv (3.5)^{=1} \equiv 1$
$-1 \equiv 1\ mod 2$

$\beta \equiv (2.5)^1 \equiv 1$
$-1 \equiv$ 1mod3

$\gamma \equiv (2.3)^1 \equiv 1$

$-1 \equiv 1 \mathrm{mod} 5$

Thus
$= 1 \times 3 \times 5 = 15$
$= 1 \times 2 \times 5 = 10$
$= 1 \times 2 \times 3 = 6$

$x \equiv 1 \times 15 + 2 \times 10 + 4 \times 6 \equiv 29 \mathrm{mod} 30$

(In fact, the original system is x $\equiv_2 1, x \equiv_3 1, and x \equiv_5 1. Notice x \equiv_3 01.$)

3.1 Theoretical Process Example

This method works because the greatest common divisor of (2,3)=1, (2,5)=1, (3,5)=1

The method works for any system

x=a Modl
x=b Modm
x=c Modn

with the condition G.C.D (lm)=1, G.C.D(ln)=1, G.C.D (m TIMES n)=1

This is called The Chinese Remainder Theorem and can extends to systems of more than 3 equations providing they are all co-prime.

3.2 Modern Day Applications

The CRT is a functional part of our modern lives. The three examples we will focus on in this paper, however are CRT's role in;

- RSA cryptography,
- Secret sharing
- algebraic ring theory.
- RSA Cryptography: RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept private. An RSA user makes and releases a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

  The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA

encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used. RSA is a relatively slow algorithm. Because of this, it is not commonly used to directly encrypt user data. More often, RSA is used to transmit shared keys for symmetric key cryptography, which are then used for bulk encryption-decryption. A special case of the CRT is used and referenced in the 'RSA Cryptography Standard, RSA Laboratories, Version 2.0, September 1998' to simplify and make more manageable numbers for deciphering. This paired with Eulers function form a solid foundation for deciphering and RSA cryptography principles.

- Secret sharing: Secret sharing (SS) was originally designed by Adi Shamir and G.R Blakley in 1979. The basic principle of a multi SS Scheme (SSS) is that the Data (D) can be shared n times in such a way that it is possible to reproduce D from any L pieces but even with a complete L piece it is not possible to decipher D. The CRT forms a basis for this system in the ability of it to distinguish individual units independent of but related to D. MSSS is a fundamental cryptographic primitive responsible for practices including security for data storage, multi-party computation, group key management, and informative communication. Although Shamirs version of SSS is based on polynomial there are types such as Asmuth-Bloom's scheme based on the CRT. Currently SSS is a cryptographic primitive seen extensively in multiple programs such as multiparty computations, threshold cryptography and generalized oblivious transfer.

- Algebra; Quadratic Fields Number Theory; Ring Theory:

  The CRT'S ability to deduce rational integers from the remainders of related co-prime divisors relates it to specific elements of algebraic ring theory. The CRT can be rewrote in ideals and rings enabling the computation of algebraic integers. Consequently the integers form multi-dimensional lattices in Euclidean space through canonical embedding. The implementation of CRT over rings of algebraic integers will create subsets of optimum lattices as a result of prime decomposition or co-prime sub-arrays. In such cases the conditions related to the co-primality of algebraic integers and ideal lattices are non-trivial. As a result CRT becomes a key stepping stone in the original formation of Ring theory.

3.3 References

- https://en.wikipedia.org/wiki/Chinese$_r emainder_t heorem : \ : text = In$

- https://www.dave4math.com/mathematics/chinese-remainder-theorem/

- https://en.wikipedia.org/wiki/Chinese$_r emainder_t heoremStatement$

- Chen, Zhenhua, Li, Shundong, Zhu, Youwen, Yan, Jianhua, and Xu, Xinli. "A Cheater Identifiable Multi-secret Sharing Scheme Based on the Chinese Remainder Theorem." Security and Communication Networks 8.18 (2015): 3592-601. Web.
- C. Li, L. Gan and C. Ling, "Coprime Sensing via Chinese Remaindering Over Quadratic Fields—Part I: Array Designs," in IEEE Transactions on Signal Processing, vol. 67, no. 11, pp. 2898-2910, 1 June1, 2019, doi: 10.1109/TSP.2019.2910498.
- https://dl-acm-org.libgate.library.nuigalway.ie/doi/10.1145/359168.359176
- https://en.wikipedia.org/wiki/RSA$_{(}cryptosystem$)
- PKCS 1, RSA Cryptography Standard, RSA Laboratories, Version 2.0, September 1998 (RFC 2437)

Abelian Groups

Workshop tutor: Tobias Rossmann

Liadhan Farrell, Siobhan Griffin, Aisling McAuliffe Hickey, Diana Tikhomirova

28 October 2020

1 Introduction

An abelian group, more commonly known as a commutative group, plays a role within many structures and concepts including rings, fields, vector spaces and algebras. In this project we will look at abelian groups in algebraic structures. There are certain properties binary operations must satisfy in order to be classified as an abelian group.

2 Properties of abelian groups

To qualify as an abelian group, it must satisfy the following requirements:

- **Closure**: For all a,b in a set $A, a + b$, is also in A
- **Associativity**: For all a, b, c in A, (ab)c = a(bc)
- **Identity element**: There exists an element e such that, ea = ae = a
- **Inverse**: For each a in A, there exists an element b in A such that ab = ba = e, where e is the identity element
- **Commutativity**: For all a,b in A, ab = ba

Most binary functions satisfy these properties. These would include the addition and multiplication of complex numbers, real numbers, rational numbers and integers inclusive. Although it seems like nothing more could be included or excluded, we must consider matrix multiplication. Is this an abelian group?

Matrix multiplication is one of the most common pieces of evidence of non-abelian groups simply because it is non-commutative.

3 Examples of Abelian Groups

We know that $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all part of abelian groups. However, considering the set $\mathbb{Z}_{\mathbb{N}} = \{0, 1, ..., N-1\}$, it is clear that $\mathbb{Z}_{\mathbb{N}}$ can not be a group under multiplication modulo n as 0 does not have an inverse. Hence, we must find out if $\mathbb{Z}_{\mathbb{N}} \backslash \{0\}$ is a group.

- **Example 1**

Prove that the set $A = 1, 2, 3, 4, 5, 6$ is an abelian group modulo 7

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	1	3
3	3	6	2	5	1
4	4	1	5	2	6
5	5	3	1	6	4

Cayley table for multiplication modulo 7 on the set $\mathbb{Z}_7 \backslash \{0\}$

- $3 \cdot 4 = 5 \mod 7$. As $5 \in A$, the set is closed under the operation
- $1(3 \cdot 2) = (1 \cdot 3)2 = 6 \mod 7$, Therefore the set is associative.
- $4 \cdot 1 = 1 \cdot 4 = 1$, 1 is the identity element
- $4 \cdot 2 = 2 \cdot 4 = 1 \mod 7$, Each element has an inverse
- $2 \cdot 5 = 5 \cdot 2 = 3 \mod 7$, Therefore the set is commutative

As this set satisfies all the requirements, it is an abelian group
Consider the set $A = 1, 2, 3, 4, 5, 6 \mod 10$

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	0
3	3	6	9	2	5
4	4	8	2	6	0
5	5	0	5	5	5

Cayley table for multiplication modulo 10 on the set $\mathbb{Z}_{10} \backslash \{0\}$

- $5 \cdot 2 = 0 \mod 10$. As $10 \notin A$ the set is not closed under the operation
- $3 \cdot 5 = 5 \cdot 3 = 5 \mod 10$, Therefore the set is associative
- $5 \cdot 1 = 1 \cdot 5 = 5$, 1 is the identity element
- In this set each element does not have an inverse
- $3 \cdot 4 = 4 \cdot 3 = 2 \mod 10$, Therefore the set is commutative

While this set is associative, commutative and has an identity element, it fails to satisfy all the requirements needed and therefore is *not* an abelian group

- **Example 2**

Q; Prove that the addition and multiplication of some integers a, b are defined as abelian groups.

- First, we must choose integers a, b for all $\in \mathbb{Z}$.Then we can prove the abelian properties
  1) Closure; the addition of 2 integers gives us some integer c. This principle is satisfied.

$$a+b = c = b+a, \text{ where } c \in \mathbb{Z}$$

2) Associativity; no matter what order you put a, b or c, their product will remain the same. This principle is satisfied.

$$(ab)c = (ba)c$$

3) Identity; when 0 is added to any integer in any order, the sum remains the same. This principle is satisfied.

$$0+a = a = a+0$$

4) Inverse; when an integer is added to its inverse, the sum is always 0 regardless of the order. This principle is satisfied.

$$a+(-a) = 0 = (-a)+a$$

5) Commutativity; the product of two integers will always be the same no matter the order they are multiplied in. This principle is satisfied.

$$ab = c = ba$$

We have proven that the addition of some integers a, b satisfy the abelian principles. This concludes that the addition, and multiplication, of integers are abelian groups.

- **Example 3**

+	1	2	3	4	5
1	2	0	1	2	0
2	0	1	2	0	1
3	1	2	0	1	2
4	2	0	1	2	0
5	0	1	2	0	1

Cayley table for addition modulo 3 on the set $\mathbb{Z}_3 \setminus \{0\}$

- $4 + 4 = 4 + 4 = 1 \mod 2$.Therefore this is an example of closure.
- $1 + 5 = 5 + 1 = 0 \mod 3$, shows the inverse.
- $2 + 2 = 1 \mod 3$. This is an example of the identity.
- $3 + 5 = 5 + 3 = 2 \mod 3$ demonstrates associativity.

Project: Binary Relation and Equivalence Relation

Lorcan Lamy de la Chapelle, Madeleine Mitchell,
Orla Loughran, Paula Hillenbrand
MA180

November 2020

1 Introduction

This paper deals with Binary Relations and Equivalence Relations, which define relations from a set A to a set B.

2 Definitions

- **Cartesian product**

  Let A and B be two sets.

  The set of all possible pairs (a,b), where $a \in A$ and $b \in B$, is called the Cartesian Product $A \times B$.

  $A \times B$: $(a, b) \| (a \in A) and (b \in B)$

- **Binary relation**

  A binary relation R from set A to set B is a subset of the Cartesian Product. This means that subsets included in R are also included in the Cartesian Product. However, unlike the Cartesian Product $A \times B$, R does not necessarily include all possible pairs (a,b).

  $R \subseteq A \times B$

  To express a binary relation from a set A to a set B $(if(a, b) \in R)$ we say 'a is related to b' or aRb.

- **Equivalence relation:**

  There are different characteristics, which a relation can show. If a relation R from set A to set B is reflexive, symmetric and transitive we call this relation equivalent. The idea of equivalence relation abstracts three properties.

  - 1.Reflexive:

    if aRa, which means that a is related to itself.

    Example:

    Let $a \in A$ =2.

    a=a = 2=2

    → Since a=a is a true statement, a is related to a, which makes the statement is reflexive.

  - 2.Symmetric:

    if aRb = bRa, which means that a is related to b in the same way that b is related to a.

    Example:

    Let $a \in A = 1$ and $b \in B = 2$.

    $a \neq b = 1 \neq 2$ and $b \neq a = 2 \neq 1$

    → a and b are interchangeable which means the statement is symmetric.

  - 3.Transitive:

    If aRb and bRc then aRc, which means that if a is related to b and b is related to c, then a must be related, in the same way, to c.

    Example:

    Let $a \in A = 1$, $b \in B = 2$ and $c \in C = 3$.

    $a < b = 1 < 2$ and $b < c = 2 < 3$ then $a < c = 1 < 3$.

    → a is related to c in the same way that a is related to b and b is related to c, which means the statement is transitive.

3 Problem: Congruence modulo n

- Reflexive

  For $a \in A$=1

  $a \equiv a$ mod n $\rightarrow 1 \equiv 1$ mod 5

  $\rightarrow$ this statement is reflexive.

- Symmetric

  For a $\in$ A=2 and for $b \in B$ =9

  a $\equiv b$ mod n = b $\equiv a$ mod n

  $\rightarrow 2 \equiv 9 \text{ mod } 7 = 9 \equiv 2 \text{ mod } 7$

  $\rightarrow$ This statement is symmetric.

- Transitive

  For $a \in A$=2; for $b \in B$=9 and for $c \in C$=18

  If a$\equiv$ b mod n and b $\equiv$ c mod n then a $\equiv$ c mod n

  $\rightarrow$ If $2 \equiv 9$ mod 7 and $9 \equiv 18$ mod 7, then $2 \equiv 18$ mod 7

  $\rightarrow$ The statement is transitive because $a \equiv$ b mod n and b $\equiv$ c mod n requires a $\equiv$ c mod n.

  Conclusion

  The congruence modulo n statement is an equivalence relation because it is reflexive, symmetric and transitive.

4 Problem: Divisibility

- Reflexive

  For $a \in A = 1$ a/a = 1/1=1

  $\rightarrow$ a divides a, therefore, divisibility is reflexive.

- Symmetric

  For $a \in A = 1$ and $b \in B = 2$ a/b=1/2 and b/a=2/1

  $\rightarrow$ a/b $\neq$ b/a, the statement is not symmetric

- Transitive

  For $a \in A = 1$; $b \in B = 2$ and for $c \in C = 3$

  a/b=1/2; b/c=2/3; a/c=1/3

  $\rightarrow$ Since c divides a, the statement is transitive

  Conclusion

  The divisibility statement is not an equivalence relation because it is not symmetric (a/b $\neq$ b/a)

5 Problem: "less than or equal to"

- Reflexive

  For $a \in A = 1$:

  a $\leq$ a $= 1 \leq 1$

  $\rightarrow$ this statement is true, therefore "less than or equal to" is a reflexive statement.

- Symmetric

  For $a \in A = 1$ and for $b \in B = 2$

  $a \leq b = 1 \leq 2$ and for $b \leq a \neq) 2 \leq 1$

  $\rightarrow$ this statement is only true if a=b

- Transitive

  For $a \in A = 1$; for $b \in B = 2$ and for $c \in C = 3$

  If $a \leq b = 1 \leq 2$ and $b \leq c = 2 \leq 3$ then $a \leq c = 1 \leq 3$

  $\rightarrow$ This statement is true

  Conclusion

  "less than or equal to" is not an equivalence relation because, even though the statement is reflexive and transitive, it is not symmetric.

6 References

[1] http://math.cmu.edu/ wgunther/127m12/notes/day11.pdf
[2] https://www.math24.net/binary-relations/
[3] https://www.youtube.com/watch?v=rPPUL0KVj2s
[4] https://www.youtube.com/watch?v=Jqkja2ODQyI
[5]https://www.khanacademy.org/computing/computer-science/cryptography/modarithme
tic/a/equivalence-relations

Wilson's Theorem

Eveline Nee, Eva Langan, Rachael Timon O Hare, Luke Gallagher.

6 November 2020

1 Introduction

John Wilson was a French Mathematician that proved Wilson's Theorem in 1771. The Wilson's Theorem states that (P-1)!= -1 Mod P if and only if P, an integer, is prime and greater than 1.

2 Proof

To prove: (p-1)! = -1 mod p if and only if p is prime.

Suppose p is prime. Every number from 1 to p-1 has a multiplicative inverse, therefore, if $k \in \{1, \ldots, p-1\}$ then k is relatively prime to p. So there are integers a and b such that

ak + bp = 1, or ak = 1 mod p

Reducing a mod p, we can assume $a \in \{1, \ldots, p-1\}$.

Thus, every element of $\{1, \ldots, p-1\}$ has a reciprocal mod p in this set. The lemma shows that from 1 to p-1 there are only 2 numbers, 1 and $p-1$, that are their own reciprocals. Thus, since p is odd, $2, \ldots, p-2$ can be grouped into pairs. $\{x, x^{-1}\}$. There are p-3/2 pairs so that the product of each pair is 1 mod p. Hence,

$$(p-1)! = 1 \cdot 2 \cdots (p-2) \cdot (p-1) = 1 \cdot 1 \cdot (p-1) = p-1 = -1p.$$

Show that p is a prime. Start by rewriting the equation (p-1)! = -1 mod p as $(p-1)! + 1 = kp$.

Taken $p = ab$. We may take $1 \leq a, b \leq p$. If $a = p$, the factorization is, so $a < p$. Then $a \mid (p-1)!$ (since it's one of $\{1, \ldots, p-1\}$) and $a \mid p$, so $(p-1)! + 1 = kp$ shows $a \mid 1$. Therefore, $a = 1$.

Therefore, (p-1)! = -1 mod p iff p is prime. QED.

3 Examples

Here are some examples of what happens when we apply this theory and proof to prime numbers. Example: prime = 7 (7-1)!+1 // 7 = 103 this shows that the prime number(7) is divisible by that prime minus one plus one. QED.

Example2: prime = 3 (3-1)!+1 // 3 = 1 this again demonstrates that a prime number (3) is divisible by that prime minus one plus one. QED.

4 References

Wilson's Theorem- Wikipedia:

A proof of Wilson's Theorem- The Prime Pages:

Wilson's Theorem- From Wolfram Mathworld:

Alan Turing

Mege Convery, Nadia Buczek, Katherine Johnston, Maria McHale
Group 7, James Cruickshank

November 6, 2020

Biography

A great contribution was made to science by none other than the English mathematician, Alan Turing [2]. Turing was a pioneer in a wide range of fields, including cryptoanalysis, modern computing, artificial intelligence, and mathematical biology. His work and research had a major impact on scientific discovery at the time and affected the technological progression of the world.

Born on June 23, 1912, Turing was part of an upper-middle-class British family. Science was a passion for the young man, who from a young age often took part in primitive chemistry experiments. Even before applying to schools, Turing was already theorizing on relativity and quantum mechanics. He attended King's College, Cambridge, where he found his passion for probability theory and mathematical logic, which eventually propelled his career forward.

Alan Turing's most substantial contribution to mathematics was undoubtedly the breaking of the Enigma code in World War II.[5] Historians estimate Turning's deciphering of the Enigma's code ended the war 2 years early and saved between 14- 21 million lives. As well as this, he also laid the groundwork for modern computing and theorized about artificial intelligence. In addition, his thesis about morphogenesis and cell differentiation in mathematical biology was validated by scientists in the University of Pittsburgh in 2014.

Turing was arrested in 1952 for "Gross Indecency", a law that prohibited being homosexual at the time, and was forced to undergo chemical castration. He continued his work in quantum physics and in cryptanalytics,

however British law at the time prohibited people with a criminal record to work in British Intelligence. Bitter over being turned away from the field he had revolutionized, Turing committed suicide in 1954 by ingesting cyanide [3], concluding his life at the age of 41. There was given little recognition for his advancements in science and mathematics due to the prevalence of homophobia and the Secrets Official Act. In 2009, Prime Minister Gordon Brown publicly apologized for how the scientist was treated, followed by Queen Elizabeth II formally pardoned him in December 2013. A British government statement encapsulated Turing's devotion to science by saying, "Turing was an exceptional man with a brilliant mind" who "deserves to be remembered and recognized for his fantastic contribution to the war effort and his legacy to science."

The Engima code

The Enigma machine was a rotor crypto-machine used by Nazi German forces throughout World War II to encode messages for all branches of their military. Although an original Enigma machine was never captured by the Allies, the Polish Cipher Bureau (PCB) reverse engineered *Double Enigmas* in 1932 with the aid of captured cipher materials and plugboard settings. These machines became vital as groundwork for Turing's team in Bletchley Park.

In 1938 German forces added complexity to Enigma with the addition of 2 extra rotor options to the machine. The additional rotors increased the amount of possible starting combinations from $(3)(2)(1) = 6$ combinations to $(5)(4)(3) = 60$ combinations . The PCB's original *Bomba*, a machine that could find rotor settings, proved to be inefficient for this new complexity. The code had surpassed their possible *Bomba* permutations ten fold, rendering the machine too slow. The solution to this problem came from Turing's study of the machine much later, when he himself invented an improved version of this machine, *Bomba*.

the mechanics

The complexity of the Enigma code arises from the construction of the machine itself, which when used became the algorithm encrypting the plaintext. The machine consisted of a keyboard, a plugboard, a set of rotors, a reflector and finally a lightboard. When a key of plaintext was hit on the keyboard,

an electrical current ran through the plugboard and into the first rotor which turned and clicked the next rotor into place. All rotors followed this pattern and until the current reached the reflector, which sent the current right back through all the mechanisms it just went through until it finally caused a light to shine on the lightboard, indicating the encrypted ciphertext letter. Each of the machine's parts contributed to the layers of complexity of the code and thus to the difficulty that Alan Turing and his team in Bletchley Park had solving it.

the plugboard

The Plugboard consisted of 10 cables which could connect any pair of letters together. The purpose of this was to mix up the letters before the enciphering process began in the rotors, and once again when the reflector sent the electrical current back.
For example, if you were to type in the plaintext 'apple' with a plugboard cable connecting the letter A to Z, the current would run along A, into Z, and tell the rotors to encode ZPPLE instead. The cable would also swap Z with A should one of the enciphered letters come back as that.

Since there are 26 letters in the alphabet, there are 26! letter combinations. However there are only 10 cables, and therefore 20 letters involved in the pairs with 6 unpaired ones, leaving

$$(6!)(10!)(2^{10})$$

to divide out of the possible permutations.That leaves you with the total letter combinations given by the plugboard to be

$$\frac{26!}{(6!)(10!)(2^{10})} = 150,738,274,937,250$$

the rotors

The rotors are a set of wheels with 'rings' of letters (A-Z) on them. The rotors could be taken out and swapped around for different cipher combinations. There were 5 possible rotors to choose from for the 3 rotor positions. This gave the operator

$$(5)(4)(3) = 60$$

options for the starting positions.

Once the order of the rotors had been chosen, starting positions on the rings could be chosen by turning the rotors. Each time a key of the plaintext was pressed on the keyboard, the far right rotor would move by one position. Once it had made a full rotation (26 positions), it would 'kick' the middle rotor forward by one position. Once it had completed the full turn again, it would 'kick' the middle rotor forward one position again. When the middle rotor had completed a full revolution, it would kick the left-hand rotor forward.

There are 26 letters, ergo 26 positions on each rotor, giving

$$26^3 = 17,576$$

options. The specific points at which each consecutive rotor would kick the next forward one position could be altered, which was called *Ring Settings*.

The first and second ring could be set to any 26 letters to kick the next, giving a total of

$$26^2 = 676$$

options for the 2 ring settings in a standard 3 rotor enigma.

If you gather together all the possible permutations on letter encryption, you get a total of

$$(150,738,274,937,250)(60)(17,576)(676) = 1.07458687(10^{23})$$

ways to set up an Enigma machine.

the ciphers

The reason that the Enigma machine was as successful as it was was because it used a series of ciphers in succession. Not only that but each cipher could be changed at will and at random for each encryption. In total, the machine made a total of 7 letter substitution ciphers, 3 on the rotors, once by the reflector, and 3 when the current was reflected back.

To break this cipher, Alan Truing and his team at Bletchley Park used *cribs*, or slip ups that the Nazi forces made in their enciphering. For example, the weather forecast was often included into each message, meaning the deciphering team could look for words like "rain" in ciphertext messages. The most crucial detail in breaking the code however, is that no letter could be enciphered as itself. This meant that if they knew a set of ciphertext included the word "rain", no letter combination in the ciphertext could correspond directly to the letters in "rain", ruling out a number of encryption options.

Computers and AI

Alan Turing is known as a founding father of computer science and artificial intelligence. His incredible Turing machines are most famous for their work in the second world war but they had many more uses then just breaking codes. In 1928 David Hilbert asked the question "Is mathematics decidable?"[6] From this he created the Entscheidungsproblem which asks "Is there an algorithm that takes, as its input, a statement written in formal logic, and produces a yes or no answer that is always accurate?"[4] Alan Turing solved this problem using a Turing machine. He envisaged a Turing machine, called for example K, that would work out if a program would halt eventually or if a program would run forever. He then envisaged a new Turing machine that would do the opposite of what K said. Therefore if K gave the answer "Yes", meaning the program would halt, then the new machine would run forever and if K answered "No" then the new machine would halt. So, Turing then used the new machine as the input for K. So if K said the new machine would halt it would run forever and if K said the new machine would run forever it would halt. This clever contradiction became known as the halting problem and , this proved that the answer to the Entscheidungsproblem is no. This conclusion was further explained in the Church-Turing thesis.

Turing is also called a father of artificial intelligence. This is because of his work on the "Turing Test". Turing believed that "a computer would deserve to be called intelligent if it could deceive a human into believing it was human."[4] If a human cannot tell the difference between a person and a computer then the computer is intelligent. This is an example of a turing test. A modern Turing test is called a Completely Automated Public Turing test to tell Computers Humans Apart or CAPTCHA for short.

Biological Mathematics

Turing made immense advancements in mathematical biology through the course of his life, such as his thesis of morphogenesis which stated that exact copies of cells differ. This theory has since been validated by scientists proving that Turing truly should be considered 'the father of computer science and artificial intelligence'. Turing was one of the first to speculate morphogenesis and through intercellular reaction-diffusion, he showed that exact copies of biological cells differ, vary in shape, and form patterns. In this model a series

of chemical reactions require an inhibitory agent to suppress the cell differentiation reaction and an excitatory agent to stimulate it. This was correctly predicted by Turing to give rise to six cell differentiation patterns. Scientists later observed an additional pattern, which showed these exact cell clones are indeed chemically different in structure. The size varied as a result of osmosis which further proved Turing's thesis. [7]

An example of this is the mathematical model of a growing embryo. In one form of this model, Turing idealised the cells as geometric points. In the other form of the model, Turing imagined the matter of the organism as continuously distributed. Both forms consist of mechanical and chemical states and exist simultaneously.
The mechanical aspect depicts the positions, masses, velocities, density, and elasticity of the matter. However the chemical composition of each individual cell is unique, as well as each substance's diffusability between adjacent cells. To identify the change between chemical and mechanical states, four things should be taken into account:
position and velocity of the cells (as stated in Newton's first Law of Motion),
the stresses on the cell as a result of motion and elasticities with osmotic pressure (which is provided by the chemical data),
and the chemical reactions and the diffusion of substances in regions where this process occurs (given by the mechanical information).[1]

Turing was a pioneer across many planes of science and mathematics. His incredible research and achievements across a variety of fields have truly cemented him to be one of the modern ages' great minds.

References

[1] Alan.M.Turing. *The chemical basis of morphogenesis.* 1952.

[2] Elaine J. Hom. Livescience article. - Live Science Contributor June 23 2013.

[3] B.J. Copeland. Professor of Philosophy, Christchurch New Zealand. Author of Artificial Intelligence Director of the Turing Archive for the History of Computing, University of Canterbury, et al. Britannica article.

[4] Carrie Anne Philbin. Alan turing: Crash course computer science 15, 2017.

[5] Ian Stewart. *The Great Mathematical Problems*. 2014.

[6] Jade Tan-Holmes. Turing machines - the accidental birth of computer science, 2020.

[7] Brandeis University. Turing's theory of chemical morphogenesis validated 60 years after his death. 2014.

MA180 Group Project:Katherine Johnson
Workshop tutor- James Cruickshank

Katie Mahon, Katie Mc Gettigan, Amy McLoughlin, Aine McDonagh

October 2020

1 Early Life

Katherine Johnson was born Katherine Coleman in 1918 on August 26th. She was the youngest child to two working-class parents in West Virginia, her father being a labourer, and her mother a local school teacher. Despite her father having an incomplete education he was widely known as a maths whizz and had a natural ability that he seemed to have passed on to his daughter. Katherine was first noticed to have an above-average intelligence at age 3 as she spoke better than her peers and was excellent at forming articulate sentences.

Katherine's love for maths was visible throughout her school years. She skipped first grade and was put into a new school for blacks when she was in sixth grade. While it could be expected for her parents to be immensely proud of this Katherine's father was always sure to instill humility in her teaching her that "she was as good as anyone and could achieve whatever she desired, but she was never to think she was better than others"

Katherine's parents were always supportive and highly valued in their children. So seeing as there was no local high school for black students they moved the family 122miles so the children could all attend high school and achieve a college education. Perhaps this why Katherine went on to achieve such great things, as she encouraged to overcome barriers and to be the best she can.

2 The Azimuth Angle

In 1960 Johnson became the first female mathematician to receive credit on a technical report for NASA entitled, "Determination of Azimuth Angle at Burnout for Placing Satellite Over a Selected Earth Position." The report presents multiple expressions and calculations "for relating the satellite position in the orbital plane with the projected latitude and longitude on a rotating earth surface." (https://ntrs.nasa.gov/citations/19980227091). These mathematical equations became critical in the development of NASA's space program and would be a key element for the USA to overtake the Soviet Union in the "space race." The Azimuth Angle report skyrocketed Johnson's reputation and

career. It also enabled her to partake in the Apollo 11 mission by providing calculations that assisted in landing a man on the moon

Examples of equations used for the calculation of the azimuth angle at burnout are as follows (pg 20 in katherine's report cited above):

$$/t(\theta 2e) - t(\theta 1) \approx (T \div 360)(\lambda 2e - \lambda 1)$$

$$/\Delta\lambda 1 - 2e = (\lambda 2 + n\omega(E)T) + \omega(E) \times (t(\theta 2e) - t(\theta 1)) - \lambda 1$$

3 The Friendship 7 mission 1962

Katherine Johnson's life changed in 1962, as NASA prepared for the orbital mission with astronaut John Glenn, Johnson was asked specifically to double-check the trajectory calculations for it. Because of the complexities of the mission, NASA collaborated with IBM to construct a worldwide communications network that linked tracking stations around the world to computers in Washington, Cape Canaveral in Florida, and Bermuda, so that the engineers could follow the flight live.The computers had been programmed with the orbital equations that would control the trajectory of the capsule in Glenn's Friendship 7 mission from blastoff to landing. Glenn was nervous about putting his life in the hands of the computer, which he believed to be prone to hiccups, according to NASA. During the pre-flight check, Glenn asked engineers to "get the girl"—Katherine Johnson- because of her experience with trajectory analysis. He wanted her to run the same numbers through the same equations that had been programmed into the computer, but by hand, on her desktop calculator. In an interview with CNN, Katherine Johnson remembers Glenn saying while she was working, "If she says they're good, then I'm ready to go."

Glenn's flight was a hit , and marked a turning point within the competition between the us and therefore the Soviet Union in space. In 2015 she was awarded the U.S. Presidential Medal of Freedom, for her work on Friendship 7.

4 Legacy

Although she passed away earlier this year (24 February 2020), her legacy lives on in two of NASA's facilities, the "Katherine G. Johnson Computational Research Facility" which is situated at the Langley Research Centre in Hampton, Virginia and the "Katherine Johnson Independent Verification and Validation Facility" in Fairmont, West Virginia. Johnson was also included in the BBC's list of 100 Women in 2016. She was listed as a pioneer in her field. Johnson was very well respected, and trusted, in the science community and overcame every barrier and obstacle that was in her way. Katherine Johnson was a trailblazer for women in STEM and as a result, Johnson has inspired, and still continues to inspire, many people all around the world.

History of Numbers

Fiona Guiney, Sean Og Gilrane, Olivia Gonsalves, Darragh Creaven,

Tutor- James Cruickshank October 2020

1 Introduction

- Numbers are expressed or represented on number systems. There are numerous different types of number systems example binary number system, decimal number system, octal number system or hexadecimal system.
- Numbers have been a fact of life throughout our history. Early Humans more than likely counted animals and people using tally marks. But as the human race developed the complexity of life did too along with their counting methods.
- Different civilisations throughout history came up with different ways of righting numbers i.e different number systems. Lots of the systems that were discovered were just a progression of the tally marks with new symbols for each quantity like Egyptian numerals or Greek numerals. Roman numerals were a little different. Roman Numerals were a little different. If a numeral was before another numeral with a higher value, it was subtracted instead than added. Even so it was still hard to write large numbers. To achieve a more effective number system was something called positional notation. Positional systems reuse symbols and give them different values depending on there position in the sequence. Examples of positional systems include Aztecs, Babylonians and Ancient Chinese.

2 Negative Numbers

- When we look back on the early work of the Babylonians, Hindus, Egyptians, or Chinese there is no trace of negative numbers. Regardless of this they were still capable of computing subtractions correctly such as: (6 - 4) x (4 - 3) or (8 - 8) x (7 - 5). The first traces of negative numbers in history can be traced back to the Chinese. Starting in 200 BCE, Chinese started using red dot to represent positive numbers and black dots to represent negative numbers. This was known as the Chinese Number Rod System. In around the 4th Century, the Alexandrian mathematician, Diaphantus, wrote his 'Arithmetica',in which he stated that the following equation was

absurd: 4X + 20 = 4. This was absurd to him because this evaluated x=-4. It was not until the 19th Century when British mathematicians such as De Morgan and Peacock started investigating the 'laws of arithmetic' and negative numbers were finally sorted out.

3 Rational Numbers

- The key concept behind rational numbers is that they are numbers that can be expressed as ratios. Ratios can also be described as simple fractions. For example the number one can be written in many different ways:

$$1 = \frac{1}{1} = \frac{-3}{-3} = \frac{17}{17} \tag{1}$$

- Many numbers can be represented in this way as the ratio of two integers:

$$-9 = \frac{-9}{1} = \frac{9}{-1} = \frac{-18}{2} \tag{2}$$

$$5.80 = \frac{58}{10} = \frac{29}{5} \tag{3}$$

- Recurring decimals are also rational numbers:

$$0.333333... = \frac{1}{3} \tag{4}$$

The first known use of numbers expressed in this way dates back to prehistoric times and to the Ancient Egyptians. However, early Greek and Indian mathematicians made books which studied the theory of rational numbers. Euclid's Elements, which is the best known of these, dates back roughly to 300 BC.

4 Irrational Numbers

As the name suggests, irrational numbers are the opposite of rational numbers; they cannot be expressed as a ratio or a simple fraction. Some of the most famous numbers in all of mathematics are irrational numbers:

$$\pi = 3.14159265359... \tag{5}$$

$$e = 2.718281828459045... \tag{6}$$

$$\sqrt{2} = 1.41421356237... \tag{7}$$

The famous Greek mathematician Pythagoras is normally credited for proving the existence of irrational numbers. He first came across it when trying to calculate the length of the hypotenuse of a right angle triangle with the other two sides of length 1. According to his theorem the length of the hypotenuse should be the square root of 2. After failing to express this number as a fraction he thereby proved the irrationality of this number.

5 Real Numbers

- In mathematics, a real number is a value of continuous quantity, that can be represented as an infinite decimal expansion. The real numbers comprise of; all rational numbers (integers such as -7 and fractions such as $\frac{7}{8}$) and all irrational numbers, including transcendental numbers such as e = 2.718281828... The set of real numbers is represented using the symbol **R**

- Around 500 BC a Greek mathematician, Pythagoras, noticed the need for irrational numbers, specifically the irrationality of the $\sqrt{2}$.This lead to the development of the fundamental theorem which is nowadays known as Pythagoras Theorem.
$$a^2 + b^2 = c^2 \tag{8}$$

- However the term 'real' was first applied to express this set of rational and irrational numbers by Descartes in the 17th century. A man by the name of Georg Cantor first revealed that the set of real numbers were uncountable and an infinite set in 1874, which he later proved with his famous 'diagonal argument' proof in 1891.

Finding a Primitive Pythagorean Triple

Stephen Hynes, ID: 20321261 Aisling Howe, ID: 20396546
Caoimhe Keeler, ID: 20387153
Cian Hughes, ID: 20357611 Tutor: James Cruickshank

November 6, 2020

1 Introduction

A Pythagorean Triple is a triple of positive integers (a, b, c) such that $a^2+b^2 = c^2$. e.g. $(3, 4, 5)$

A Pythagorean Triple is said to be *primitive* if $gcd(a, b, c) = 1$. For example, $(3, 4, 5)$ is a primitive Pythagorean Triple, whereas $(12, 16, 20)$ is a Pythagorean Triple but it is not primitive because $12, 16$ and 20 are all divisible by 4.

2 Background

Pythagoras was born in Samos circa 570 BC. He was incredibly important in the development of mathematics and is regarded by many historians as the first mathematician. [1] Pythagoras is credited with the founding of the geometric theorem that the sum of the squares of two sides of a right-angled triangle is equal to the square of the hypotenuse, however, the origins can be traced back further to Babylonian tablets from circa 1900-1600 BC that display knowledge of the theorem. It is also proposition number 47 in Book 1 of Euclid's Elements. [2]

3 Our Task

The goal of our project is "to find a primitive Pythagorean Triple (a, b, c) such that a, b, c are all greater than 300." i.e. The properties of the triple are as follows:

$$a^2 + b^2 = c^2$$

$$gcd(a, b, c) = 1$$

$$a > 300, \quad b > 300, \quad c > 300$$

4 Deriving a Method to Generate Primitive Pythagorean Triples

Suppose (a, b, c) is a primitive Pythagorean triple.
Q1: Is it possible that a and b are both even?

$$\text{Let} \quad a = 2x \quad b = 2y$$

$$\begin{aligned} a^2 + b^2 &= 4x^2 + 4y^2 \\ a^2 + b^2 &= 4(x^2 + y^2) \\ \Rightarrow c^2 &= 4(x^2 + y^2) \\ \Rightarrow 4 \mid c^2 \quad &\text{and} \quad 2 \mid c \end{aligned}$$

Therefore c is also even.

If a and b are both even, $gcd(a, b, c) = 2$, therefore a and b cannot both be even in a primitive Pythagorean triple.

Q2: Is it possible that a and b are both odd?

$$\text{Let} \quad a = 2x + 1 \quad b = 2y + 1$$

$$\begin{aligned} a^2 + b^2 &= (2x + 1)^2 + (2y + 1)^2 \\ a^2 + b^2 &= 4(x^2 + y^2 + x + y) + 2 \\ c^2 &= 4(x^2 + y^2 + x + y) + 2 \end{aligned}$$

c^2 is not the square of a natural number because it is a multiple of 2, but not a multiple of 4. As c is not a natural number in this case, a and b cannot both be odd in a primitive (or in any) Pythagorean Triple.

We have established by **Q1** and **Q2** above that in a Primitive Pythagorean Triple, a and b must have opposite parity, that is to say that if a is odd, b must be even, and vice versa.

Let's take a to be odd and b to be even, whilst remembering that $a^2+b^2 = c^2$. Therefore, c must be odd because if c were even, the greatest common divisor of b and c would be 2 and the triple would not be primitive.

We can rewrite the equation as $b^2 = c^2-a^2$. We can factorise this equation as a difference of two squares, giving us $(c-a)(c+a)$, noticing that $c-a$ and $c+a$ are even. We can write $c-a = 2m$ and $c+a = 2n$, where m and n are natural numbers.
From this, we can say

$$\begin{aligned} b^2 &= c^2 - a^2 \\ b^2 &= (c-a)(c+a) \\ b^2 &= (2m)(2n) = 4mn \end{aligned}$$

Also,

$$\begin{aligned} b &= 2k \qquad \text{(Because b is even)} \\ b^2 &= 4k^2 \\ 4k^2 &= 4mn \\ \rightarrow k^2 &= mn \end{aligned}$$

In order for this to work, we claim that $mn = k^2$, which is a perfect square. Next we need to claim that m and n are coprime.

Claim: $gcd(m, n) = 1$
Proof: Take some integer d and suppose that

$$d \mid m \quad \text{and} \quad d \mid n$$

$$\rightarrow d \mid m+n$$

$$\rightarrow d \mid c$$

$$\text{(Because } m+n = \frac{c-a}{2} + \frac{c+a}{2} = c\text{)}$$

Similarly

$$d \mid a \rightarrow d \mid gcd(a, c)$$
$$d \mid 1 \rightarrow d = 1$$

From this we can see that $mn = k^2$ is a perfect square, with the $gcd(m, n) = 1$.

It follows from this that $m = p^2$ and $n = q^2$ with $gcd(p, q) = 1$. Note that both m and n are themselves perfect squares.

Finally, we can obtain three equations for values of (a, b, c) as follows:

$$\begin{aligned} 2m &= c - a & \qquad 2n &= c + a \\ m &= \frac{c-a}{2} & \qquad n &= \frac{c+a}{2} \\ p^2 &= \frac{c-a}{2} & \qquad q^2 &= \frac{c+a}{2} \\ 2p^2 &= c - a & \qquad 2q^2 &= c + a \end{aligned}$$

$$\begin{aligned} \text{Recall} \quad b^2 &= (c-a)(c+a) \\ b^2 &= (2p^2)(2q^2) \\ b^2 &= 4p^2q^2 \\ \Rightarrow b &= 2pq \end{aligned}$$

$$\begin{aligned} q^2 - p^2 &= \frac{c+a}{2} - \frac{c-a}{2} = \frac{2a}{2} = a \\ \Rightarrow a &= q^2 - p^2 \end{aligned}$$

$$\begin{aligned} p^2 + q^2 &= \frac{c-a}{2} + \frac{c+a}{2} = \frac{2c}{2} = c \\ \Rightarrow c &= p^2 + q^2 \end{aligned}$$

We used a YouTube video [3] as a guide to finding these three equations for a, b and c.

5 Finding the Triple

From the method above, we have found that if (a, b, c) is a primitive triple then there exists a co-prime pair of integers $p, q \in \mathbb{N}$, one even, one odd, such that

$$\begin{aligned} a &= q^2 - p^2 \\ b &= 2pq \\ c &= p^2 + q^2 \end{aligned}$$

The three equations above can be used to generate Pythagorean Triples. (Note that for these equations to make sense in the context of a right-angled triangle q should be greater than p, otherwise the equation for a will yield a negative length).

Example Pythagorean Triple:

$$\text{let} \quad q = 29 \quad p = 6$$

We chose these values for p and q because they are co-prime.

$$\begin{aligned} a &= q^2 - p^2 \\ a &= (29)^2 - (6)^2 \\ a &= 841 - 36 \\ \rightarrow a &= 805 > 300 \end{aligned}$$

$$\begin{aligned} b &= 2pq \\ b &= 2(6)(29) \\ \rightarrow b &= 348 > 300 \end{aligned}$$

$$\begin{aligned} c &= p^2 + q^2 \\ c &= (6)^2 + (29)^2 \\ c &= 36 + 841 \\ \rightarrow c &= 877 > 300 \end{aligned}$$

Now we have to test if $a^2 + b^2 = c^2$:

$$\begin{aligned} a^2 + b^2 &= 805^2 + 348^2 \\ a^2 + b^2 &= 648025 + 121104 \\ a^2 + b^2 &= 769129 \end{aligned}$$

$$\begin{aligned} c^2 &= 877^2 \\ c^2 &= 769129 \end{aligned}$$

$$\Rightarrow a^2 + b^2 = c^2$$

Finally, we have to prove that gcd(a,b,c)=1. We can do this by using the Euclidean Algorithm.

$$\begin{aligned} &gcd(805, 348): \\ 805 &= 2 \times 348 + 109 \\ 348 &= 3 \times 109 + 21 \\ 109 &= 5 \times 21 + 4 \\ 21 &= 5 \times 4 + 1 \\ 4 &= 4 \times 1 + 0 \\ \Rightarrow &gcd(805, 348) = 1 \end{aligned}$$

$$\begin{aligned} &gcd(877, 805): \\ 877 &= 1 \times 805 + 72 \\ 805 &= 11 \times 72 + 13 \\ 72 &= 5 \times 13 + 7 \\ 13 &= 1 \times 7 + 6 \\ 7 &= 1 \times 6 + 1 \\ 6 &= 6 \times 1 + 0 \\ \Rightarrow &gcd(877, 805) = 1 \end{aligned}$$

$$\begin{aligned} &gcd(877, 348): \\ 877 &= 2 \times 348 + 181 \\ 348 &= 1 \times 181 + 167 \\ 181 &= 1 \times 167 + 14 \\ 167 &= 11 \times 14 + 13 \\ 14 &= 1 \times 13 + 1 \\ 13 &= 13 \times 1 + 0 \\ \Rightarrow &gcd(877, 348) = 1 \end{aligned}$$

In conclusion, $(a = 805, b = 348, c = 877)$ is a primitive Pythagorean Triple such that (a, b, c) are all greater than 300.

References

[1] https://link.springer.com/article/10.1057/jt.2009.16#Sec14.

[2] https://www.britannica.com/science/Pythagorean-theorem.

[3] https://www.youtube.com/watch?v=F3dR41ItmSg.

The Life and Work of Sophie Germain

By Mark Shivnan, Dylan Walsh, Sarah Moran and Fionn Walsh

James Cruickshank

Introduction

Marie-Sophie Germain was a French Mathematician, Physicist and Philoso- pher. She was born on the 01/04/1776 on Rue Saint-Denis, Paris, France. She is best known for her work in Number Theory and Elasticity. Both of which we will discuss in the below project.

What we have to understand is that Sophie faced great difficulty having her work and opinions listened to due to the fact that she was a woman. She received no formal education. She did not attend school or college. She was a self-taught Mathematician. She was a true believer in herself and in her work and was courageous and sometimes rebellious in her manner. She was no doubt a role model in later years after her death but still continues to be one, not only just for women in Science and Maths but also for women in general as her bravery and her determination, despite all that she faced, she managed to over come that and therefore had a huge impact on the Mathematical Community.

She faced difficulty straight from the start. Her parents didn' t believe it was proper for a woman to be pursing a career in Maths or even a career in general. The society in which she lived also believed that it was improper for a woman to go to school and receive an education and also it was improper that a woman had any job outside the home. These parental and societal restraints did not hinder her. She educated herself by reading books in her fathers library. She read books by people like Euler, Lagrange, Legendre and Gauss. Despite all this her work made a huge impact on the Mathematical world as her work on Fermat Last Theorem provided a foundation for Mathematicians for years to come.

Early Life

Her Father Ambroise-Francois according to sources was a wealthy silk mer- chant.He was a Poloitician and was elected to the Etats-Generaux. During his time there he oversaw many changes to the Constitution.Many Believe that the conversations she witnessed that occurred between her Father and his Colleagues sparked her interest in Politics and Philosphy.

First Interest and Work In Mathematics

Sophie grew up during the French Revolution and was forced to stay inside. She however made the best of her time. She found herself in her Father' s library more often than not. She read and stuied many books there most notably L' Histoire des Mathematiques by J.E Montuclas which spiked her interst in Archimedes and thus mathematics. To Study Archimedes and other books she

taught herself Greek and Latin. with these languages under her belt she read and study more works by Euler and Newton. Her Interest in Mathematics continued but was not viewed highly by her parent . They thought it was inappropriate due to the fact that she was a girl. They denied her a fire and candles to quench her interest in studying, however Sophie was devious and determined, she hid candles and blankets to have light and keep her warm as she studied into the night.

When she was 18 the Ecole Polytechnique opened. However, again due to the fact that she was female she was unable to attend, despite her intelligence. She did manage to obtain notes and lectures from the college. She sent her applictaion form to Joseph Louis Lagrange, a faculty member, under a false name, M LeBlanc. After seeing the extraordinary intelligence shown by M LeBlanc, Lagrange requested a meeting. Knowing that her identity was going to be reveled, Sophie still decided to attend the meeting. Lagrange was shocked but was not put off as he believed that Sophie had a great talent for Mathematics. He became her mentor.

Number Theory

Sophie is well known for her work in Number Theory. She first became interested in this Theory in 1798 when Adrien-Marie Legendre published his work on Number Theory. She began corresponding with Legendre on his Theory. Some of Sophie' s work was published by Legendre in his Supplement, the second edition of Theorie Des Nombres. He called her work very ingenious. Her ienterst in Number Theory was again spiked and reignited when she read Carl Friedrick Guass' Disquistianses. In 1804 after years of work in Number Theory, she claimed to have proven n=p-1 where p is a prime number of the form p=8k+7. She wrote to Gauss under the name M LeBlanc showing him her work how ever her proof contained a weak assumption and Gauss didn' t reply to her.

Gauss lived in Braunschweig, Germany during the Napoleonic Wars. Afraid that Gauss would suffer the same fate as Archimedes she made contact with a family friend in army, General Pernety. When he checked on Gauss, Gauss was fine but was confused as to who Sophie was. Her true identity was revealed to him but this did not affect their friendship and correspondence. Gauss stated that she was brave and determined to follow her desire to make a living out of Mathematics even though the odds where stacked against her due to her gender.

Also that year Sophie claimed to Gauss that

$$x^n + y$$

is of the form

$$h^2 + nf^2$$

then x + y is also of that form.

However Gauss countered with

$$15^{11} + 8^{11}$$

can be written in the form

$$h^2 + nf^2$$

but 15 + 8 cannot

Work in Elasticity

In the year 1809, Sophie Germain began her work on elasticity. She completed and submitted her paper in 1811 to the Paris Academy of Sciences. However, Germain did not win a prize for her work.

A contest at the Paris Academy was extended by a further two years, this gave Germain the opportunity to once again try to win the prize. Unfortunately, in 1813, her anonymous submission was only given an honourable mention as it contained mathematical errors.

Luckily for Germain, once again the contest had furthermore been extended by another year. She was able to work on her third attempt. She submitted her third paper, which was entitled, "Recherches sur la théorie des surfaces élastiques". On this occasion, she submitted it under her own name on the 8th of January 1816.

It was in the in that third paper where Germain had finally received some recognition for her work. As a result, she became the first woman in the Paris Academy of Sciences to win a prize.

Sophie Germain came up with an equation to prove the vibration of a plane lamina:

$$N^2(\frac{\alpha^4 z}{\alpha x^4} + \frac{\alpha^4 z}{2\alpha x^2 \alpha y^2} + \frac{\alpha^4 z}{\alpha y^4}) + \frac{\alpha^2 z}{\alpha t^2} = 0, where$$

N^2 is a constant. (1)

From the year 1821, Sophie Germain began to publish her prize-winning essay. In 1826, she submitted a revised copy of her 1821 to the Paris Academy. Her work was approved by Augustin-Louis Cauchy, who was appointed to review her work.Cauchy advised Germain to publish her work.

One other pieces of work from Sophie Germain was when she used mean curvature in her research in elasticity in her "Mémoire sur la courbure des surfaces" in 1831.

1 Number Theory

Sophie Germain's most significant work is widely considered to be her work on Fermat's last thereom. In the year 1815 the academy put forth a prize for the proof of Fermat's Last Thereom. This challenge restored her interest yet again in number theory.

Fermat's Thereom is divided into two cases. Case 1 entails all powers "p" that do not divide any "x","y","z". Case 2 consists of all "p" that divide at least one of "x","y","z". "Sophie Germain's Thereom" suggested the following.

Let p be an odd prime. If there exits an auxillary prime p=2Np+1(where N is any opositive integer not divisible by 3) such that:

1. if $x^p + y^p \equiv 0 mod p, then p divides x, y, z$
2. p is not a $p^p power residue mod p$,

Then the first case of Fermats Last Thereom holds true

This result enabled Germain to prove Fermat's Last Thereom for all odd primes where p<100, however according to Del Centina she had rather shown that it holds true for every exponent where p<197. Following this American Mathematician L.E Dickson applied Germain's Thereom to prove Fermat's Last Thereom for odd primes<1700.

Enclosed within an unpublished manuscript entitled "Romarque sur l'impossibilité de satisfaire en nombres entiers a l'equation $x^p + y^p = z^p$.

Germain proved that counterexamples to Fermat's Last Thereom for p¡5must be numbers "whose size frightens the imagination", which is approximately 40 digits long. Despite this Germain never published this work, however her ingenious thereom is only known because of reference in Legendres tretise regarding number theory, to where he incorporated it in order to prove Fermat's Last Thereom for all p=5. Germain continued to prove or closely prove numerous results which associated or later rediscovered to Lagrange. Del Centina is quoted in saying that her ideas were central, however conclusively her method did not work.

Later Life In 1829 she was diagnosed with Breast Cancer but still continued with her work. She died on the 27th of June 1831 at the age of 55. Despite not receiving the recognition she deserved during her life, her name has been given to different equations ie, A Sophie Germain Prime : is a prime p such that 2p+1 is also a prime

The Germain Curve : $(k_1+k_2)/2, where k_1 and k_2 are min and max values of the curve.$

References: https://en.wikipedia.org/wiki/Sophie$_{G}ermain$
https://www.agnesscott.edu/lriddle/women/germain.htm
https://www.britannica.com/biography/Sophie-Germain

Who is Ronald Rivest?

Adam Bellew, ID:20324221 Sinéad Maloney, ID:20314633
Romana inic, ID:20323931 Agatha White, ID:20350906
Workshop tutor: James Cruickshank

October 2020

1 Introduction

Ronald Rivest (born May 6, 1947) is a cryptographer and professor in the Department of Electrical Engineering and Computer Science in MIT. Rivest is largely known for his contributions to modern cryptography. In particular, one of his contributions which he is known for is having, along with Adi Shamir and Leonard Adleman, founded what is known as the RSA public-key cryptosystem. Research interests of Rivest vary from algorithms, cryptography to contemporary issues such as voting security, climate change, and as a result of the coronavirus pandemic, contact tracing.[2]

2 The RSA public-key cryptosystem

Cryptography is the encryption of text so that outsiders to the code would not be able understand the messages being sent but the desired reader would be able to decrypt the encryption and be able to read the messages. For years mathematicians have been trying to discover the perfect cryptosystem, but no one had been successful until 1977. The RSA public-key cryptosystem was developed by Ron Rivest alongside Adi Shamir, a computer scientist and Leonard Adleman, a mathematician. The concept of an asymmetric public-private key cryptosystem was first published by Whitfield Diffie, Ralph Merkle and Martin Hellman in 1976. Rivest, Shamir and Adleman, inspired by their work, then started to work on developing a one-way function that was hard to invert.[2]

Rivest and Shamir worked together develop an unbreakable system while Adleman was responsible for finding weaknesses in their workings. Adleman did this 42 times over a course of a year. Their failed approaches included knapsack-based algorithms and permutation polynomials. Rivest, unable to sleep one night, lay on his couch with a math book and started to think hard about the problem they had been facing all year. That night Rivest had a breakthrough and started formalizing his ideas. By the next morning the majority of the mathematical paper on the RSA cryptosystem had been written. The algorithm is known as the initials of the three mathematicians' surnames, RSA.

This new method of cryptography stood out as it did not require the exchange of keys to encrypt and decrypt messages. RSA could also mark messages with a digital signature and allowed originators to create messages accessible only to intended recipients. RSA has lots of uses today such as securing internet connection and keeping personal information private online.

To begin using the RSA cryptosystem,the user must choose two distinct random prime numbers p and q. Each of these numbers must be of a great value of digits long) to minimise the risk of the message being deciphered if intercepted.[4] Following this, a user must take a number e such that e is not divisible by either p nor q. Following this the user must use Euclid's algorithm in order to find:

$d \cong e^{-1} mod(p-1)(q-1)$

After this, the user must find multiply p and q such that:

$n = pq$

The user can make public their enciphering key $E = (n, e)$,however they must keep their deciphering code $D = (n, d)$ secret.

Now that the public and private keys have been generated, the sender can now begin to encipher their message. This can be done by the following. The sender picks their message they'd like to send a.

$F_(n, e)(a) \cong a^e modn$

3 Example of RSA cryptography

For example, let's say Bob wants to message Alice the following message using a 26 letter alphabet where $A = 0, B = 1, ...Z = 25$:

DOG

As it is public information, Bob can see that Alice's public key $K_{(n,e)} = (46927, 39423)$

The letters of the message "DOG" correspond to the numbers 3,19,6 in our alphabet respectively. We can then compute the following:

$3x26^2 + 19x26^1 + 6x26^0 mod 46927$

$ans = 2528^{39423} mod 46927$

After some workings, we can find this to be:

$ans = 5338 mod 46927$

We can also find this to be:

$5338 = 0x26^3 + 7x26^2 + 23x26^1 + 8x26^0 mod 46927$

The numbers 0,7,23,8 correspond to the letters AHXI respectively. Therefore, Bob sends Alice the following message: "AHXI"

To decipher this, Alice must calculate the following:

$0x26^3 + 7x26^2 + 23x26^1 + 8x26^0 mod 46927$ (using the corresponding numbers given in the ciphertext)

$ans = 5338 mod 46927$

Alice alone knows that her d value $d = 26767$

Using this knowledge, Alice can convert these numbers back to the original plaintext by knowing the following:

$plaintext = x^d mod n$ [3]

$5338^{26767} mod 46927$

$= 2528 mod 46927$

$2528 = 3x26^2 + 19x26^1 + 6x26^0$

The numbers 3,19,6 given above correspond to the letters DOG respectively.

Thus, Alice has safely deciphered her RSA encrypted message sent from Bob.

4 The ThreeBallot Voting System

Rivest is also responsible for the invention of the 'ThreeBallot Voting System' which he published on the 1st of October 2006. The 'ThreeBallot' system provides benefits of a cryptographic voting system without the need to use cryptography, only using paper ballots

Each voter is given 3 ballot papers. They cast all 3: 1 verifiable cast and 2 anonymous casts. They then receive a receipt of their vote as proof.

So how does it work? To vote FOR a candidate, the voter fills in exactly 2 circles on the candidate's row that they wish to vote for. To vote AGAINST a candidate the voter fills in exactly one circle on the candidate's row they wish to vote against.

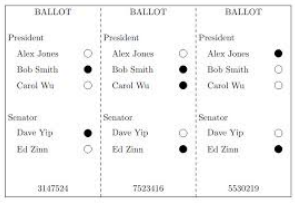


Figure 1: Example of a ballot paper

The total number of votes FOR a candidate is calculated by subtracting the total number of voters from the total number of marks for that candidate.
[1]

5 Use of RSA in information security

The RSA cryptosystem not only guarantees the privacy,allowing communication between two parties by encrypting the original message to be transmitted over, but it also provides other information security services or functions such as they are the authentication or origin.

When two parties want to communicate each of them will generate their own key pair both public and private eg. party A will have the pair(KPA,kpa) and party B will have the pair(KPB,kpb), where KP are the public keys and kp are the private keys.

We assume that A wants to send an M message confidentially to B using the cryptosystem. These are the steps you have to follow:

Get the public key of party B, (eB, nB) Represents the clear text that you want to send as a positive integer M ¡n Compute the encrypted message: C = (M) eB mod nB Finally, it transmits crypto message C through the channel

In order for the recipient to decode the encripted message sent they must use the private key (dB, nB) to compute M = (C) dB mod nB Retrieve the original text from its representative M

Digital signalling: If A wants to send a signed message to B so that B can be sure the message has origniated from A and not any other sender The steps that A will follow are:

Create a digest (digest) of the message you want to send, using a hash function Represent this summary as an integer M between 0 and n-1 Use your own private key (dA, nA) to compute the signature S = (M) dA mod nA Send that signature S to receiver B together with the original message (which can be encrypted or not, as desired). Obviously, the signature S cannot be manipulated by anyone once generated, because if a single bit of the signature is changed, verification of the signature at destination will fail.

References

[1] Ronald rivest. *The ThreeBallot Voting System*. Oct. 2006. URL: https://people.csail.mit.edu/rivest/rivest-TheThreeBallotVotingSystem.pdf.

[2] *Ronald Rivest, people-MIT*. URL: https://www.csail.mit.edu/person/ronald-rivest.

[3] *Understanding RSA Algorithm*. URL: https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_understanding_rsa_algorithm.htm.

[4] *What is RSA encryption and how does it work?* Oct. 2019. URL: https://www.comparitech.com/blog/information-security/rsa-encryption/.

Maths Project: Generating an Enciphering Key and Enciphering Using Public Key Cryptography

Maeve Samali, Rosín Keogh, Leah O'Driscoll

6th November 2020

1 Introduction

In this project we will illustrate how to generate an enciphering key and how to encipher a message using an RSA cryptosystem where the enciphering key is publicly known but can only be deciphered by the person who knows the deciphering key.

2 Generating the encryption key

In order to encipher we must first generate an enciphering key. To make the enciphering key $K_E = (n, e)$ you must do the following:

2.1 Find two distinct random prime numbers

Select two distinct prime numbers, p and q, at random. Where p and q are kept secret. (Usually p and q are very large but, for the purposes of demonstration, we will use smaller prime numbers.)

For example:

Let $p = 2,069$ and $q = 2,161$.

2.2 Find n

$n = pq$.

Therefore, $n = pq = (2,069)(2,161) = 4,471,109$.

As a result, now we know that $K_E = (4471109, e)$

2.3 Find e

To find e we must choose an integer such that $gcd(e, p-1) = 1 = gcd(e, q-1)$. The easiest way to calculate this is by using Euler's Phi function to find $\phi(n)$.

We know that
$\phi(n) = \phi(pq)$
$\phi(p) = p - 1$ and $\phi(q) = q - 1$
because p and q are prime. That means we are looking for
$(p-1)(q-1) = 4466880$.

Now, we must choose a value for e where $gcd(e, 4466880) = 1$. Due to the fact that the public key is known to everyone it is not so important for e to be random. The most commonly used value for e is 65,537 because with larger numbers encryption becomes less efficient. For our problem in particular, $e = 65,537$ satisfies all the requirements for e, and so I will use $e = 65,537$ for the encryption.

2.4 The encryption key

We now know the values for enciphering function $K_E = (n, e)$:
$n = 4,471,109$ and $e = 65,537$.

So, $K_E = (4471109, 65537)$.

3 Enciphering

If we wish to encipher a message, we must designate a number to each letter. In this case I will use a 27 letter alphabet where $A = 0, B = 1, C = 2, ...Z = 25, \_ = 26$. We then must decide how we wish to encipher our message. That is, how many letters there will be in each plaintext message unit (k) and likewise how many letters there will be in each ciphertext message unit (l). This means that for every k letters we encrypt of the plaintext we end up with l letters of ciphertext. The plaintext message is:

I_LOVE_CRYPTOGRAPHY_

In this instance we will let
$k = 4$ i.e. 4-letter plaintext message units,
$l = 5$ i.e. 5-letter ciphertext message units.

3.1 Dividing up the message and converting it into numbers

Now we must divide the plaintext into 4-letter message units. This gives us:

I_LO, VE_C, RYPT, OGRA, PHY_

Now we need to convert each of the letters into numbers. This gives us:

I_LO $= 8, 26, 11, 14$
VE_C $= 21, 4, 26, 2$
RYPT $= 17, 24, 15, 19$
OGRA $= 14, 6, 17, 0$
PHY_ $15, 7, 24, 26$

3.2 Encipher the message

Now that we have converted all the letters into numbers we can begin to encipher. The enciphering key $K_E = (4471109, 65537)$, in the form $K_E = (n, e)$, is used as follows:
$f_{(n,e)} = x^e \ mod \ n$,
where x is found by converting each message unit into a number by doing as follows:

I_LO $= 8(27)^3 + 26(27)^2 + 11(27)^1 + 14(27)^0$
$x_1 = 176729$,
VE_C $= 21(27)^3 + 4(27)^2 + 26(27) + 2(1)$
$x_2 = 416963$
RYPT $= 17(27)^3 + 24(27)^2 + 15(27) + 19(1)$

$x_3 = 352531$

$\text{OGRA} = 14(27)^3 + 6(27)^2 + 17(27) + 0$

$x_4 = 280395$

$\text{PHY\_} = 15(27)^3 + 7(27)^2 + 24(27) + 26$

$x_5 = 301022$

where 27 is the number of letters in the alphabet and the series of coeffiecients, $\{8, 26, 11, 14\}$ etc. are the letters converted into numbers.

Now, we need to encipher each message unit using the enciphering function, $f_{(n,e)} = x^{65537}\ mod\ 447110$.

For example for message unit 1, x_1 this is

$f_{(n,e)} = 176729^{65537}\ mod\ 447110$

$f_{(n,e)} = 355109\ mod\ 447110$

We can now use this new number, 355109 to find the ciphertext of message unit1.

Since we previously decided that $l = 5$ (5-letter ciphertext message units), this means that for every four letters of plaintext (for each individual message unit k) we will generate five letters of ciphertext. We find these five letters by essentially doing the opposite of what we did to find x, such that for our first message unit:

$355109 = a(27)^4 + b(27)^3 + c(27)^2 + d(27) + e(1)$.

We now have five coefficients $\{a, b, c, d, e\}$, as there will be five letters.

$355109 = 0(27)^4 + 18(27)^3 + 1(27)^2 + 3(27) + 5(1)$

We now convert these coefficients back into letters.

$0 = A, 18 = S, 1 = B, 3 = D, 5 = F$

Therefore, I_LO = ASBDF.

If we do this for all the message units we get a fully encrypted message.

For VE_C, we get:

$f_{(n,e)} = 416963^{65537}\ mod\ 447110$

$f_{(n,e)} = 232653\ mod\ 447110$

$232653 = 0(27)^4 + 11(27)^3 + 22(27)^2 + 3(27) + 21(1)$

$0 = A, 11 = L, 22 = W, 3 = D, 21 = V$

VE_C = ALWDV.

RYPT $f_{(n,e)} = 352531^{65537}\ mod\ 447110$

$f_{(n,e)} = 52321\ mod\ 447110$

$52321 = 0(27)^4 + 2(27)^3 + 17(27)^2 + 20(27) + 22(1)$

$0 = A, 2 = C, 17 = R, 20 = U, 22 = W$

RYPT = ACRUW

OGRA $f_{(n,e)} = 280395^{65537}\ mod\ 447110$

$f_{(n,e)} = 208365\ mod\ 447110$

$208365 = 0(27)^4 + 10(27)^3 + 15(27)^2 + 22(27) + 6(1)$

$0 = A, 10 = K, 15 = P, 22 = W, 6 = G$

OGRA = AKPWG

PHY_ $f_{(n,e)} = 301022^{65537}\ mod\ 447110$

$f_{(n,e)} = 146812\ mod\ 447110$

$146812 = 0(27)^4 + 7(27)^3 + 12(27)^2 + 10(27) + 13(1)$

$0 = A, 7 = H, 12 = M, 10 = K, 13 = N$

PHY_ = AHMKN

So, our resulting ciphertext is
ASBDFALWDVACRUWAKPWGAHMKN.

4 Conclusion

Therefore, in showing this we have illustrated how to generate an enciphering key and furthermore how to then encipher a message using public key cryptography.

The Chinese Remainder Theorem Report

Aedín Horkan
a.horkan@nuigalway.ie

Kaiwen Chen
k.chen2@nuigalway.ie

Philomena Gragory
p.gragory1@nuigalway.ie

Class: Ma180

Professor: Götz Pfeiffer

Date: November 2020

Chinese Remainder Theorem

November 6, 2020

1 Introduction

We have chosen the Chinese Remainder theorem as our project title.

The Chinese Remainder theorem states that a number X can be found by its remainders from divisions of integer(s) n(,m,..) where gcd(n,m) = 1 by the euclidean algorithm [3]

The first written account of the theorem appeared in a Chinese treatise of Sun Zi Suanjing[2] 'Master Sun's Mathematical Manual' :"there are certain things whose number is unknown .A number is repeatedly divided by 3,the remainder is 2; divided by 5,the remainder is 3;and by 7,the remainder is 2. What will the number be"? Which was then solved for

$$x \equiv 140 + 63 + 30 \equiv 233 \equiv 23 \pmod{105}$$

The Chinese remainder theorem was first used to calculate the calendar year in ancient China as early as the 2nd century [2]. More recent applications of the Chinese remainder theorem is widely seen in cryptography, computing and coding [3]

We will use an example of single digit integers to show the working of this theorem. This theorem can then be applied to more complex equations once a basic understanding is gained.

2 An Example of the Chinese Remainder Theorem

Say a basket of eggs is being counted. I know that if I take out three at a time, I end up with two left-over. If I take out five at a time, I get one left-over, and if I take out seven at a time, I get five left-over. We can use the Chinese remainder theorem to find out the least number of eggs the basket can hold.

We know:

$$x \equiv 2 \pmod{3},$$

$$x \equiv 1 \pmod{5},$$

$$x \equiv 5 \pmod{7},$$

Find out the values for x.

$$x \equiv 26, 131, 236...$$

$$x \equiv 26 + (3 * 5 * 7)n$$

Workings: [1] 1.At first we try to use 3 mod 3 to ignore the second and third section as 3 mod 3 is 0.The first section will be left alone as we wanted.

$$mod\ 3\ mod\ 5\ mod\ 7$$

$$x \equiv 0 + \mathbf{3} * + \mathbf{3} *$$

2.We repeat the same process at the start, but this time we will leave second section alone and fill the first and third section with 5 mod 5.

$$x \equiv \mathbf{5} * + 3 * + 3 * \mathbf{5}$$

3. After doing so we come to the third section as we put 7 mod 7 into the gap and leave third section alone.

$$x \equiv 5 * \mathbf{7} + 3 * \mathbf{7} + 3 * 5$$

We multiply them and get this

$$x \equiv 35 + 21 + 15$$

4. We want x to be equivalent to 2 mod 3. If we evaluate x with mod 3 the second and third sections are divisible by three, so they will equal 0.

$$x \equiv \mathbf{35} + 0 + 0$$

$$x \equiv 35 \pmod 3$$

$$x \equiv 2 \pmod 3$$

We repeat the process but with mod 5 this time;

$$x \equiv 0 + \mathbf{21} + 0$$

$$x \equiv 21 \pmod 5$$

$$x \equiv 1 \pmod 5$$

Again with mod 7;

$$x \equiv 0 + 0 + \mathbf{15}$$

But this time we get:

$$x \equiv 15 \pmod 7$$

which is:

$$x \equiv 1 \pmod 7$$

As we can see this is not the result needed, because we need x$\equiv$ 5 $mod\ 7not1\ mod\ 7$.

In order to correct this we need to multiply 1 by 5 to get 5 mod 7, and when we do so we will have to multiply 15 by 5 as well.

$$x \equiv 1 * 5 \pmod 7$$

$$x \equiv 5 \pmod 7$$

$$x \equiv 0 + 0 + 15\mathbf{.5}$$

$$x \equiv 0 + 0 + \mathbf{75}$$

We then add these numbers up to get x:

$$x \equiv 35 + 21 + 75 = \mathbf{131}$$

To make sure that x=131 is equivalent to 2 mod 3, 1 mod 5, and 5 mod 7. We check that the remainders are consistent with our earlier statement:

$$131 = 3.43 + \mathbf{2}$$

$$131 = 5.26 + \mathbf{1}$$

$$131 = 7.18 + \mathbf{5}$$

5. Now we have the value of x, we can use it to get the minimum value by using mod (3*5*7)

$$131 \ mod \ (3 * 5 * 7)$$

$$26 \ mod \ 105$$

$$x \equiv 26 \pmod{105}$$

We can also express

$$x = 26 + (105)n$$

So we get x= 26, 131, 236 ... as those values are all 26 mod 105.

From the Chinese remainder theorem we now know that the minimum amount of eggs found in the basket is 26. If a multiple of 105 is added to 26 we know this will satisfy the equation as well.

3 Conclusion

Through our use of the Chinese Remainder theorem we have shown that we can represent the whole of an integer when its remainders and divisors are known, provided the divisors are co-prime. This understanding of the basic workings of the Chinese Remainder theorem can lead to more nuanced applications in various fields.

References

[1] Randell Heyman. The chinese remainder theorem made easy, 2013. https://www.youtube.com/watch?v=ru7mWZJlRQg,.

[2] Shen Kangsheng. Historical development of the chinese remainder theorem. *Archive for history of exact sciences*, pages 285–305, 1988.

[3] Dingyi Pei, Arto Salomaa, and Cunsheng Ding. *Chinese remainder theorem: applications in computing, coding, cryptography*. World Scientific, 1996.

A Fundamental Analysis of the RSA Cryptosystem

Cillian Collins 20308813 | Keith Rabbitte 19103381 | Ross Cahill 18457402 | Ruben Lewis 19401532

October 2020

Contents

1 Preface

This is a report researched and written by Group 1, detailing the mathematics behind cryptography and cryptosystems.[1]

1.1 What is RSA?

RSA is an example of a public key cryptosystem. It consists of two keys, public and private, which encipher and decipher messages respectively.The user generates a public key using a choice of two very large prime numbers and publishes it. In real-world use, these primes are extremely large (>100 digits). The private key generated is kept secret.

It is believed that calculating the deciphering, or 'breaking' the RSA encryption, requires an prohibitively lengthy prime factorisation calculation on modern computer hardware. There is no known method for breaking RSA effectively for large primes.

RSA is now being used less frequently due to the difficulties involved in implementing it securely. In the past, it has been implemented in Transport Layer Security (TLS), a cryptographic protocol used in securing information exchange over an internet connection.

2 RSA Prerequisites

It requires 2 distinct prime numbers p and q. We then allow $n = p \times q$. Our public key consists of the module n with an exponent e. Our secret key is calculated using Euler's totient function. Since p and q are prime, we know that:

$$\varphi(n) = (p-1) \times (q-1)$$

It is critical for the RSA cryptosystem to work, that the output of the above equation is co-prime to e. This means the greatest common divisor (gcd) is equal to 1:

$$gcd(e, \varphi(n)) = 1$$

We can now identify our decryption key d, since d must be the multiplicative inverse of e mod $\varphi(n)$:

$$e \times d \equiv 1 \ mod \ \varphi(n)$$

Now we can take any message m. To encrypt our message we use the following notation:

$$m_e \equiv m^e \ mod \ n$$

To decrypt our encrypted message, m_e we simply raise it to the power of d.

$$m_d \equiv (m_e)^d \ mod \ n$$

This works since e and d are multiplicative inverses in mod n. It's also true that:

$$m^{e^d} \equiv m \ mod \ n$$

2.1 Euler's Totient Function

Euler's Totient function is defined as:

$$\varphi(n) = |\{x|1 \leq x \leq n, gcd(x,n) = 1\}| \tag{1}$$

In other words, it is the count of all numbers up to n that are *coprime* to n.
Since a prime number has no factors other than itself and 1, for any prime number p,

$$\varphi(p) = p - 1 \tag{2}$$

So if you were asked to find the $\varphi(3947)$, the answer would be $3947 - 1 = 3946$
The Totient function is also multiplicative: Let n be the product of primes p_1 and p_2

$$\varphi(n) = \varphi(p_1 p_2)$$
$$\varphi(p_1 p_2) = \varphi(p_1)\varphi(p_2)$$

Then, using the identity $\varphi(p) = p - 1$

$$\varphi(p_1)\varphi(p_2) = (p_1 - 1)(p_2 - 1) \tag{3}$$

2.2 Greatest Common Divisor

The greatest common divisor "gcd", also known as the highest common factor "hcf", is the greatest/highest divisor of two positive integers (a and b).

For example the gcd of (12 and 78) is 6, the gcd of (14 and 21) is 7. Now, what's the gcd of (5 and 12) ? The answer is 1.

1 is the gcd of these two positive integers and when 1 is the gcd this is known as "relatively prime". This makes sense because when a number is only divisible by itself and 1 it is Prime, and two relatively prime numbers are numbers that only have 1 as their gcd.

2.3 How it Works

The RSA Cryptosystem works like so: You need an encryption pair of numbers, (*a*,*b*) and these numbers are the "lock"; if you want to send a message, you use this lock to lock up (encrypt) your message. Only the person with the unique decryption key can solve this message.

For example, on an Alphabetical system "A to Z", using a 1 - 26 numbering system, if you want to send the letter "C" you use 3, if you want to send the letter "Y" you use 25 and so on.

So in simplistic terms let's say you want to send the letter "C". You first will need to encrypt it using an encryption key.

Let's say you have the encryption key "$e : (5, 14)$". In order to lock(encrypt) your text "C", you first convert it to "3". Then you raise it to the power of the first number in the key as such:

$$3^5 \ mod \ 14 \ \equiv \ 243 \ mod \ 14$$

Then simplify on a mod 14 clock:

$$243 \ mod \ 14 \ \equiv \ 5 \ mod \ 14$$

Therefore your cipher-text will be: "E" because "E" is 5 on a numbering system from 1 to 26.

Now, let's say you have the decryption key (*11, 14*) you do the same. "E" is 5 and you raise it to the power of the first number "11".

$$5^11 \ mod \ 14 \ \equiv \ 3 \ mod \ 14$$

3 is "C" and now it has been received and decrypted.

2.4 Primitive Example

Step 1: Take p and q to be 7 and 11 respectively.

$$p \ \equiv \ 7$$

$$q \ \equiv \ 11$$

Step 2: to find "N": You multiply p by q

$$p \ \times \ q \ \equiv \ 77$$

$$N \ \equiv \ 77$$

This number becomes the modulus in both the encryption and decryption key.

Step 3: You then need to calculate the phi function.

$$\phi(N) \ \equiv \ (p-1) \ \times (q-1)$$

$$\phi(77) \ \equiv \ (7-1) \ \times (11-1) \ \equiv \ 60$$

Step 4: Choose a number "e" and "d" for the encryption/decryption. This cannot be random and must meet certain properties as such:

- It must be between 1 *and* ϕN
- It must also be coprime with N *and* ϕn

After some calculating you find that e = 13 and d = 37.

$$de \ mod \ \phi N \ \equiv \ 1$$

$$37d \ mod \ 60 \ \equiv \ 1$$

$$37 \ \times \ 13 \ \equiv \ 481 \ mod \ 60 \ \equiv \ 1$$

Step 5: Now to test this we know that:

$$K \ \equiv \ P^e \ mod \ N$$

then

$$P \ \equiv \ K^d \ mod \ N$$

Let P = 3

$$K \ \equiv \ 3^1 3 \ mod \ 77 \ \equiv \ 1594323 \ mod \ 77 \ \equiv \ 38$$

$$P \ \equiv \ 38^3 7 \ mod \ 77 \ \equiv \ 2.8313468e + 58 \ mod 77 \ \equiv \ 3$$

So your encryption key is: (*13, 77*) and your decryption key is: (*37, 77*)

To send the message "HI", "H" and "I" are "8" and "9" respectively, on a 1 to 26 numbering system.

$$8^1 3 \ mod \ 77 \ \equiv \ 549755813888 \ mod \ 77 \ \equiv \ 50$$

$$9^1 3 \ mod \ 77 \ \equiv \ 2541865828329 \ mod \ 77 \ \equiv \ 58$$

So: 50 = X and 58 = F

So you send the ciphertext "XF" to the recipient.

X is 24 on a 1 to 26 numbering system and F is 6 so using the unique decryption key we can solve this.

$$24^3 7 \ mod \ 77 \ \equiv \ 1.1690039e + 51 \ mod \ 77 \ \equiv \ 8$$

$$6^3 7 \ mod \ 77 \ \equiv \ 6.1886549e + 28 \ mod \ 77 \ \equiv \ 9$$

And as we know "8" and "9" translate to "HI"

3 Implementation of RSA

To implement RSA for the purpose of this project, we decided to opt for the Python language. Libraries exist in Python, such as *Crypto.Util*, which make it simple to generate large prime numbers for use in our RSA algorithm. We decided, however, against using such libraries for the purposes of this implementation, so we can better understand what each function does, and thus gain more insight into the nature of such a cryptosystem through a ground-up implementation.

3.1 Pythonic Implementation

To implement a python version of the RSA cryptosystem, we first needed to break the challenge up into several important functions which are required for us to build such a system.

```
import random
import math

def gcd(a, b):
    return a if b == 0 else gcd(b, a % b)

def inverse(e, phi):
    for i in range(phi):
       if (e * (i)) % phi == 1:
          return i

def prime(p):
    if p % 2 == 0 or p % 5 == 0:
        return False
    i = 3
    x = 4
    while i <= math.floor(math.sqrt(p)):
        if p % i == 0:
            return False
        if x == 4:
            i += 4
            x = 0
        else:
            i += 2
        x += 1
    return True

def encrypt(pubkey, plaintext):
    return [(ord(char) ** pubkey[0]) % pubkey[1] for char in plaintext]

def decrypt(privkey, ciphertext):
    return "".join(x for x in [chr(int(char) ** privkey[0] % privkey[1]) for char in
    ciphertext])

def keygen(p, q):
    if not (prime(p) and prime(q)):
        raise ValueError("The numbers entered must both be prime.")
    elif p == q:
        raise ValueError("Prime numbers, p and q, must not be the same.")

    n = p * q

    phi = (p - 1) * (q - 1)

    e = random.randrange(1, phi)
    g = gcd(e, phi)

    while g != 1:
        e = random.randrange(1, phi)
        g = gcd(e, phi)
```

```
50
51      d = inverse(e, phi)
52
53      return (e, n), (d, n)
54
55  def main():
56      print("Pythonic Implementation of RSA Cryptosystem")
57      p = int(input("Enter a prime number, p: "))
58      q = int(input("Enter a prime number, q: "))
59      pubkey, privkey = keygen(p, q)
60      print("Your public key is " + str(pubkey) + " and your private key is " + str(privkey))
61      m = str(input("Enter a messaing to encrypt using public key: "))
62      m_encrypted = encrypt(privkey, m)
63      print("Your encrypted message is: ")
64      print(''.join(map(lambda x: str(x), m_encrypted)))
65      print("Your encrypted message is: " + ''.join(map(lambda x: str(x), m_encrypted)))
66      print("Decrypting message using private key " + str(privkey) + " . . .")
67      print(decrypt(pubkey, m_encrypted))
68
69
70  if __name__ == "__main__":
71      main()
```

3.1.1 Greatest Common Divisor

This function is critical to the RSA cryptosystem. As previously detailed above, for any integers a and b, if the $gcd(a, b) = 1$ then we can determine that a and b are *coprime*.

```
1  def gcd(a, b):
2      return a if b == 0 else gcd(b, a % b)
```

We created the above function. It returns a if b is zero. Otherwise, it executes the function again with a now equal to the previous value of b and b now equal to $a \ mod \ b$. This function will eventually return the greatest common divisor when b is equal to zero.

3.1.2 Prime Test

Another important function is one which should, given an integer as input, determine whether this integer is prime or not. This function should be efficient, as it's often the case that similar functions run more computations than needed. As such, we rely on the mathematics behind prime numbers.

Given an integer p, we first check if this number is a multiple of 2 (even). If the number is not even, we can assume it is not divisible by any even numbers, and thus half the number of computations which we must complete (instead of checking if it's divisible by *2, 3, 4, 5, 6...* we can check *3, 5, 7, 9...*

We also check if the number is divisible by 5. If the number is not divisible by 5, we need not check any such multiples. In other words, it may not be divisible by any integer which ends with the digit 5.

```
1  def prime(p):
2      if p % 2 == 0 or p % 5 == 0:
3          return False
4      i = 3
5      x = 4
6      while i <= math.floor(math.sqrt(p)):
7          if p % i == 0:
8              return False
9          if x == 4:
10             i += 4
11             x = 0
12         else:
13             i += 2
14         x += 1
15     return True
```

The above steps are represented on line 2 of the code. Next we set two variables, i and x. We are going to test every odd integer (which is not a multiple of 5) from 3 up until the square root of the number we are testing, p.

This is known as the square root rule, and it's important in prime numbers. Every factor has a corresponding factor, of which the product reveals the number itself. Since it requires two factors to be multiplied by each other to form the number p, we can assume that at least ONE such factor will be less than or equal to $\sqrt{p}$.

For each iteration of this loop, we test if the p is divisible by the integer. If it is, we return *False*... p is not a prime number.

x is used as a control variable, to let us know when we need to add 4 to i as opposed to 2. In general, we always add 2, as we don't need to test even numbers against p. However, we also don't need to test multiples of 5. We begin with $i = 3$ and $x = 4$ so we will immediately be adding 4 to i, thus skipping 5. This repeats every 4^{th} iteration of the loop, making this function more efficient than others.

If the 'while loop' terminates without returning a value of *False*, then we can assume that no factors were found, and thus return a value of *True*.

There are numerous more complicated means by which we could make this function more efficient, but this will suffice for the purpose of this research.

3.1.3 Multiplicative Inverse

Finding the multiplicative inverse is important, as that is how we will identify our decryption key (it's the multiplicative inverse of our encryption key). The python code below illustrates how we can accomplish this programmatically:

```
def inverse(e, phi):
    for i in range(phi):
        if (e * (i)) % phi == 1:
            return i
```

Again we define a function, this time taking 2 inputs, e and phi which represent our encryption key and our mod value respectively.

We must loop through every integer i less than phi, until we find one which satisfies the below equation:

$$e \times i \equiv 1 \ mod \ phi$$

Once the above equation is satisfied, we can assume that the integer i, is the multiplicative inverse of e and thus our decryption key, d.

3.1.4 Encryption Algorithm

Our encryption algorithm is a single line return statement.

```
def encrypt(pubkey, plaintext):
    return [(ord(char) ** pubkey[0]) % pubkey[1] for char in plaintext]
```

It simply iterates through the plaintext string, converting the character to a number, raising it to the power of the encryption key and then converting the number to mod n, where n is derived from the public key.

Each of these now encrypted values of the characters are added to a list which is returned. It's a simple operation which performed key-based encryption across each individual character.

3.1.5 Decryption Algorithm

The decryption algorithm is also a single line return statement.

```
def decrypt(privkey, ciphertext):
    return "".join(x for x in [chr(int(char) ** privkey[0] % privkey[1]) for char in
    ciphertext])
```

It simply iterates over the ciphertext, raising each message unit to the power of the decryption key, d. It then converts this value to mod n, where n is derived from the private key. We then assume each of these values to represent a character in unicode, and convert it back to a character. We iterate over this array one last time, to join it to a string. This string is then returned as our decrypted message.

3.1.6 Key Generation

The key generation algorithm is the heart of the RSA cryptosystem.

```
def keygen(p, q):
    if not (prime(p) and prime(q)):
        raise ValueError("The numbers entered must both be prime.")
    elif p == q:
        raise ValueError("Prime numbers, p and q, must not be the same.")

    n = p * q

    phi = (p - 1) * (q - 1)

    e = random.randrange(1, phi)
    g = gcd(e, phi)

    while g != 1:
        e = random.randrange(1, phi)
        g = gcd(e, phi)

    d = inverse(e, phi)

    return (e, n), (d, n)
```

We receive two distinct prime numbers, p and q. We run initial checks to determine that both of these values are indeed both prime and distinct from one another. Provided this is the case, we generate the integer n which is the product of primes p and q. After this, we compute the variable *phi*, which represents Euler's Totient Function.

Due to p and q both being prime, it's computationally simple to calculate the number of integers below n which are coprime with n since n is the product of primes. This is the foundation of RSA cryptography, since we have now found an algorithm which is true only for numbers with this property. This makes a task which would normally have a complexity of NP now maintain the complexity of P.[2] The actual complexity of Euler's Totient Function can be expressed as $O(\sqrt{n})$[3]

This is why mathematicians have identified the $P = NP$ problem as one of the most notable unsolved equations in computer science and mathematics as a whole. If it is computationally easy for us to verify a solution (and we can verify it in polynomial time), then is it possible for us to actually solve the problem in polynomial time? In other words, does an algorithm exist which would enable us to solve such problems in polynomial time?[4]

It's widely thought by the scientific community that $P \neq NP$, however this has never been proven.[5]

Once we have computed the value for *phi*, we then generate a random encryption key which exists in mod *phi*. This means it must be an integer, N, where $1 < N < phi, N \in Z$ *and* $gcd(N, phi) = 1$

If an integer, N is found to match this criteria, it can then be used as our encryption key, e. To calculate our decryption key, d, we simply find the multiplicative inverse of e *mod phi*. The values are then returned from the key generation function.

4 Importance of Prime Numbers

In an RSA cryptosystem prime numbers play a massively important role, used in the creation of the very keys that encrypt and decrypt our most sensitive and private data.

In generating keys to be used in RSA cryptography one must first find two random prime numbers p and q, these numbers should be similar in magnitude but differ in length by a few digits. This makes them harder to factorize. These prime numbers are then multiplied to give the modulus N, which is part of both the public and private key.

RSA-1024, RSA-2048 and RSA-4096 are the commonly used types of RSA encryption. The number refers to the bit size of N, hence RSA-2048 uses two 1024-bit primes p and q and RSA-4069 uses two 2048-bit primes. RSA-1024 is much less commonly used as 2048 is suitable for most applications and is more secure.

As you can tell, these are incredibly large prime numbers, RSA-2048 using primes p and q of about 309 decimal digits in length. The largest prime number ever found is $2^{77232917} - 1$, having 23,249,425 digits. Finding this Mersenne prime took six days of non stop computing using an Intel i5-6600 CPU. [6]

While using Mersenne primes in RSA would be inconceivably resource heavy and overkill in terms of security it does give one and idea of the need for efficient algorithms and systems for finding these large primes.

In recent years with the exponential growth and advancement of computing hardware, some suggest that RSA-2048 will not be secure enough for long. However, most security experts project that 2048-bits will be sufficient until the year 2030 approximately. This being said, many companies are investing time and resources into 4096-bit RSA as a higher level of security and future-proofing.

There are many different attacks performed on RSA systems, with varying success. Even 4069-bit has been broken using an interesting and unconventional attack known as acoustic cryptanalysis; where researchers (Including Adi Shamir(Co-Creator of RSA)) listened to the CPU of a computer decrypting data and were able to understand the data and find the decryption key.

5 Conclusion

This project was an incredibly interesting insight into the vast world of cryptography, through the tried and tested lens of RSA. Researching deeper into RSA Cryptography we learned about other encryption types, and gained knowledge on the subject of RSA attacks and cipher breaking in general.

Gordon Moore predicted that the number of transistors in an integrated circuit (IC) would double every two years, and this prediction has held since 1975, hence becoming known as a 'Law'. Moore's law essentially means our processing power is increasing exponentially, and therefore the possibility of a more powerful computer being able to factorize the public key for an RSA-2048 system is becoming more and more likely. In response to this, as we mentioned before, RSA-4096 is likely going to become the standard key size in the coming years, since 4096 bit keys are considered to be considerably harder to crack.

With the steady advancement of quantum computing, RSA becoming defunct could possibly be on the 25-year horizon, however we are far away from that reality yet. In 1994 an American mathematician Peter Shor discovered a quantum algorithm to factor large integers, almost exponentially faster than the most efficient known algorithm - the general number field sieve.

So, if an ideal quantum computer with enough qubits is created then the RSA we know today would drastically change, although cryptosystems have been designed in a field known as post quantum cryptography, which would ensure the worlds most sensitive data could be kept secret.

Either way we believe that for now RSA-4096 is about as bulletproof as we could need, and we expect it to become a cryptographic standard in the near future.

Bibliography

[1] Marc Joye. *Security analysis of RSA-type cryptosystems*. PhD thesis, Citeseer, 1997.

[2] Wikipedia. *P (complexity)*.

[3] OmG (https://cs.stackexchange.com/users/64229/omg). Time complexity of euler totient function. Computer Science Stack Exchange. URL:https://cs.stackexchange.com/q/88879 (version: 2018-03-04).

[4] Wikipedia. *P versus NP problem*.

[5] Oded Goldreich. *P, NP, and NP-Completeness: The basics of computational complexity*. Cambridge University Press, 2010.

[6] George Woltman. *Largest Known Prime Number*. 1996.

The Halting Problem

By Dion Collins, Hameed Adagun, Brian Mc Ateer and Cian Larkin
Workshop Tutor: Götz Pfeiffer

October 2020

Contents

1 What is the halting problem?

The Halting Problem is a theoretical problem which asks if it is possible for a computer program which, if ran, will be able to tell whether a given problem will "halt" or go on forever, hence the halting problem.

Example:
1. while (true)
print("Hello World!")
2. print("Hello World!")

Of these two examples, we can tell the first equation does not halt as "(true)" is a constant. The second equation, however, we can tell does halt, as it is told to print the term once, rather than to repeat.
The halting problem was one of the first problem to be definitively proven to be unsolvable and hence definitively proved that mathematics was "incomplete" or incapable of solving all problems posed. Alan Turing was one of the first to provide a proof that a program capable of solving the Halting Problem simply couldn't exist as it defied logic. The proof is as follows:

- In order to prove such a program does not exist, we must assume that it does.
- Suppose we have a machine (A) that given an input (i) and a program (P) (supposed to solve that input), will be able to tell if the program will halt, or continue forever. If it does halt, it will answer "Yes", if not, it will answer "No".
- We then suppose that we have another machine (B) that takes the outputs of machine A. If A answers "Yes" the, program B will make the program loop forever, if it gives "No", it will halt the program. Call the whole machine AB.
- If we then input two AB machines into another AB machine, hence asking does AB halt.
- If AB does halt, we get a "Yes" answer, looping the program forever, if it does not halt, we get a no answer, which will halt the program.
- There if it does halt, it doesn't halt and if it doesn't halt it doesn't halt, causing a paradox.
- The paradox proves that no such machine could possibly exist as it defied logic.

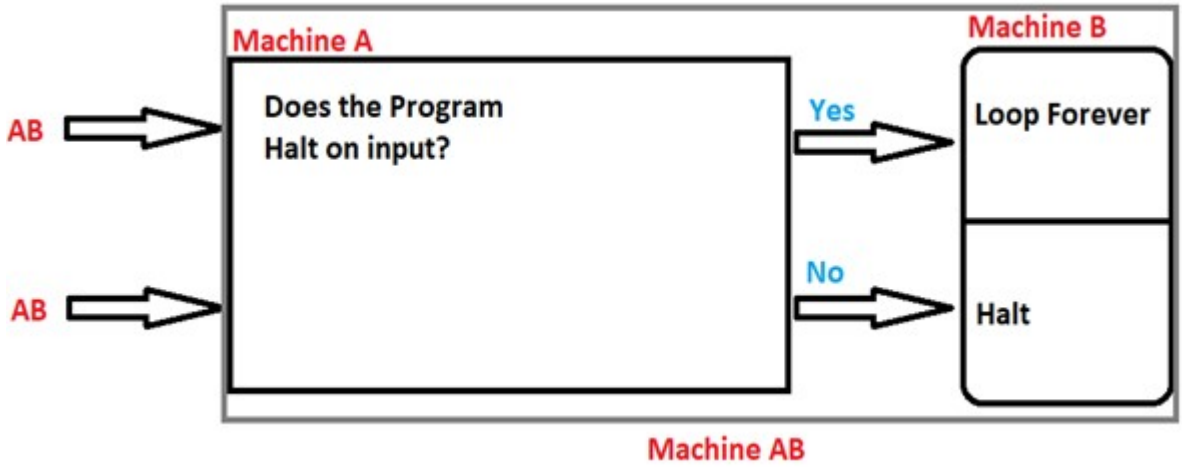


Figure 1: The Halting Problem

2 Background of Alan Turing

Alan Turing was born on the 23rd June 1912. He was an English mathematician, computer scientist, logician, cryptanalyst, philosopher, and theoretical biologist. Turing was highly influential in the development of theoretical computer science, providing a formalisation of the concepts of algorithm and computation with the Turing machine, which can be considered a model of a general-purpose computer. Turing is widely considered to be the father of theoretical computer science and artificial intelligence. Despite these accomplishments, he was never fully recognised in his home country during his lifetime due to the prevalence of homophobia at the time and because much of his work was covered by the Official Secrets Act.

Turing played a crucial role in cracking intercepted coded messages that enabled the Allies to defeat the Nazis in many crucial engagements, including the Battle of the Atlantic, and in so doing helped win the war. Due to the problems of counterfactual history, it is hard to estimate the precise effect Ultra intelligence had on the war, but at the upper end it has been estimated that this work shortened the war in Europe by more than two years and saved over 14 million lives.

It was Alan Turing who came up with the halting problem in 1936. Prior to Turing, The Entscheidungsproblem (decision problem) was originally posed by German mathematician David Hilbert in 1928. The problem asks for an algorithm that considers, as input, a statement and answers "Yes" or "No" according to whether the statement is universally valid, i.e., valid in every structure satisfying the axioms. This was later disproved by Turing. Turing proved that his "universal computing machine" would be capable of performing any conceivable mathematical computation if it were representable as an algorithm. He went on to prove that there was no solution to the decision problem by first showing that the halting problem for Turing machines is undecidable: it is not possible to decide algorithmically whether a Turing machine will ever halt. This paper has been called "easily the most influential math paper in history".

Even though Turing died in 1954 he will still be remembered as one of the most important mathematicians and computer scientists. He is still praised to this day. Turing has been honoured in various ways in Manchester, the city where he worked towards the end of his life. In 1994, a stretch of the A6010 road (the Manchester city intermediate ring road) was named "Alan Turing Way". A bridge carrying this road was widened and carries the name Alan Turing Bridge. A statue of Turing was unveiled in Manchester on 23 June 2001 in Sackville Park, between the University of Manchester building on Whitworth Street and Canal Street. The memorial statue depicts the "father of computer science" sitting on a bench at a central position in the park.

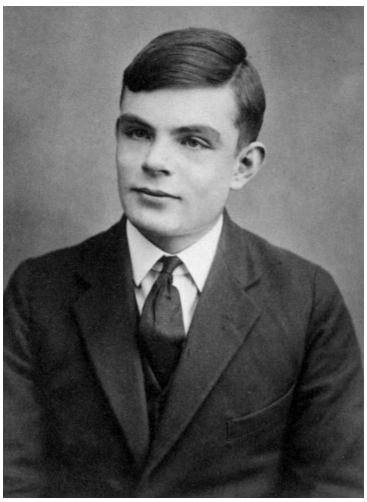


Figure 2: Alan Turing (aged 16)

3 The philosophical implication of the halting problem

Following Alan Turing's answer to the Halting Problem, it was proven definitively that mathematics was not decidable (not every mathematical problem has a step-by-step method that can be followed to tell us if a statement is true or not i.e. not solvable), contrary to David Hilbert's previous proposition that mathematics was decidable.

The philosophical implications of this were immediately apparent. If there are certain mathematical problems that have been proven to be undecidable or unsolvable (such as the Halting Problem), then this implies that not even the most powerful computer, given infinite time, can solve them. It's like asking the computer to produce a triangle with four sides!

The human brain has often been compared to a computer, and its inner workings have been likened to a complex computer program. This implies that there are therefore certain problems that our brains fundamentally cannot solve regardless off the passage of time or advancement in our intelligence, knowledge or our technology.

Conversely, however, Turing's answer to the Halting Problem has also given us some certainty in that it allows us to reason about the relative difficulty of algorithms. It tells us definitively that there are indeed some algorithms that do not exist and that, sometimes, all we can do is guess at a problem, and never know if we've solved it.

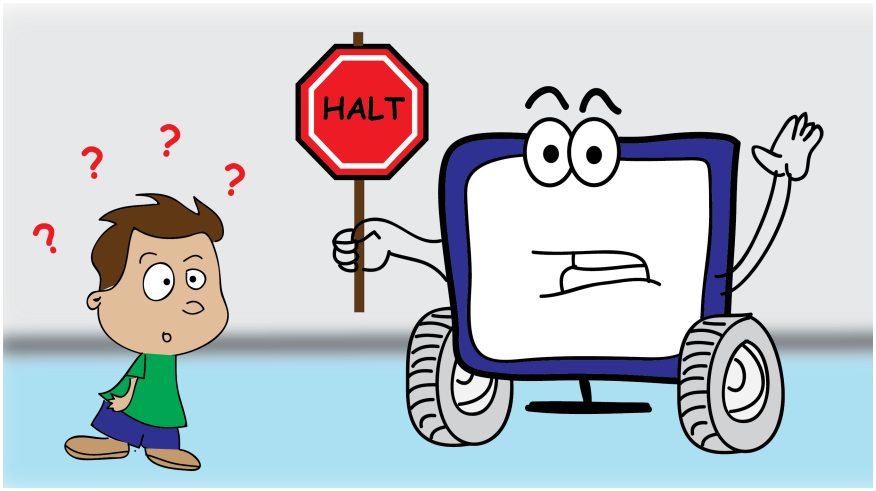


Figure 3: Halting

4 Conclusion

The halting problem is significant because it was one of the first problems to be deemed undecidable. Turing's proof elicited the publications of many more undecidable problems when published in 1936. Papers from John Barkley Rosser, Stephen Cole Kleene, Martin David Davis etc soon followed. Before the halting problem had been proved by Turing there was no boundaries to distinguish between a solvable and unsolvable problem. The significance of this is very profound in coding, programmers must be able to identify and accept imperfections in their code which cannot be solved. The halting problem establishes parameters within which programmers can operate and understand the limits of their code. The halting problem is ever present in all computational facets of the world we live in. It has shaped the development of technology and the world we live in today.

Bibliography

Alan Turing (2020), 'Alan turing — Wikipedia, the free encyclopedia'. [Online; accessed October-2020].
URL: *https://en.wikipedia.org/wiki/Alan*$_T$*uring*

Entscheidungsproblem (2020), 'Entscheidungsproblem — Wikipedia, the free encyclopedia'. [Online; accessed October-2020].
URL: *https://en.wikipedia.org/wiki/Entscheidungsproblem*

Halting Problem (2020), 'Halting problem — Wikipedia, the free encyclopedia'. [Online; accessed October-2020].
URL: *https://en.wikipedia.org/wiki/Halting*$_p$*roblem*

Up and Atom (2018), 'The halting problem - an impossible problem to solve'. [Online; accessed October-2020].
URL: *https://www.youtube.com/watch?v=t37GQgUPa6kt=sab*$_c$*hannel* = *UpandAtom*

Affine Decryption (Question 5)

Connor Adams, Adam Daniels, Marijus Bandziulis, Eoin O Reilly, Derek Kenny

October 2020

0.1 The Problem

5. The following cipher text was produced using an affine enciphering function

$$f : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, x \mapsto \alpha x + \beta$$

on single letter message units over the 37-letter alphabet

$$0,\ 1,\ 2, ..., 9,\ A = 10,\ B = 11, ...,\ Z = 35,\ \_ = 36$$

where underscore represents a blank.
The last nine characters of the plain text are: COMPUTING.
Cipher text:
5_GR4G2LP2GYRKE5_GKE5IFIE2RE1E2R5O4I2
HRPENR5_GRZE5_G4RLZRKLYG42RFLK3O5I2H

0.2 Getting the alpha and beta

To start we must figure out our enciphering function. We must consider the function $x \ \to \alpha x + \beta = y \ mod 37$
We know the last word of our enciphered text is "COMPUTING" when deciphered.
Taking this into account we can map the letters of "COMPUTING" to the corresponding enciphered text which is FLK3O5I2H.

C	O	M	P	U	T	I	N	G
12	24	22	25	30	29	18	23	16
F	L	K	3	O	5	I	2	H
15	21	20	3	24	5	18	2	17

0.2.1 Setting up our simultaneous equations

Because our enciphering function contains two unknowns, we must use simultaneous equations to solve for

$$\alpha \ and \ \beta$$

. To do this we pick 2 letters from 'COMPUTING' and their corresponding letter from 'FLK3O5I2H' For this example, we will use 'C' and 'O' which are mapped to 'F' and 'L'. Using our function:

$$x \to \alpha x + \beta \ mod 37.$$

For our first equation we sub 12 in for x as it is the corresponding value of 'C'. For our second equation we sub 24 in for x as it is the corresponding value of 'O'. Doing this we get our simultaneous equations:

$$1: \quad C \to 12\alpha + \beta = 15 \ mod 37$$
$$2: \quad O \to 24\alpha + \beta = 21 \ mod 37$$

0.2.2 Solving our simultaneous equations

Taking our 1^{st} equation, we let

$$\beta = 15–12\alpha$$

We then sub this into our second equation to solve for 'α':

$$24\alpha + (15 - 12\alpha) = 21 \; mod \, 37$$

$$12\alpha + 15 = 21 \; mod \, 37$$

$$12\alpha = 21 - 15 \; mod \, 37$$

$$12\alpha = 6 \; mod \, 37$$

$$\alpha = 6(12^{-1}) \; mod \, 37$$

$$\alpha = 6(34) \; mod \, 37$$

$$\alpha = 204 \; mod \, 37$$

$$\alpha \equiv 19 \; mod \, 37$$

$$\text{Thus } \alpha = 19$$

To solve for 'β' we sub our 19 in for 'α' into either of our original equations:

$$12(19) + \beta = 15 \; mod \, 37$$

$$\beta = 15 - 228 \; mod \, 37$$

$$\beta = -213 \; mod \, 37$$

$$\beta \equiv 9 \; mod \, 37$$

$$\text{Thus } \beta = 9$$

0.3 Functions

Now that we know that $\alpha = 19$ and $\beta = 9$, we can work out our Deciphering Function.

$$y \ \rightarrow \alpha^{-1}(x - \beta)$$

(inverse of the enciphering function)

$$y \ \rightarrow 19^{-1}(x - 9)$$

(Sub in our results for α and β)

0.3.1 Modulus Inverse

To get $19^{-1}\ mod 37$ we can use the Euclidean algorithm.

$37 = 1 * 19 + 18$ (how many times 19 goes into 37 or the modulus)
$19 = 1 * 18 + 1$ (repeat above step until remainder is 1)

$$1 = 19 - 1(18)$$

$$1 = 19 - 1(37 - 1(19))$$

$$1 = 2(19) - 1(37)$$

$$\text{thus } 19^{-1} \equiv 2\ mod 37$$

Therefore, the function is:

$$2(y - 9)\ mod 37$$

$$2y - 18\ mod 37$$

$$(-18 \equiv 19\ mod 37)$$

$$2y + 19\ mod 37$$

0.3.2 Testing

To test if out Deciphering function is correct, We will use our Deciphering function to decipher the letter 'F' which we already know is equal to the plaintext letter 'C'.

$$F = 15$$

$$2(15) + 19 = 49$$

$$49 \equiv 12\ mod 37$$

Remember C = 12, meaning that our Deciphering function is correct

0.4 Decryption

0.4.1 Application

Now all that's left is to apply our decryption key, which we found to be (2,19).

$$5 \Longrightarrow 2(5) + 19 \ mod \ 37 = 29 \Longrightarrow T$$

$$\_ = 36 \Longrightarrow 2(36) + 19 \ mod \ 37 = 17 \Longrightarrow H$$

$$G = 16 \Longrightarrow 2(16) + 19 \ mod \ 37 = 14 \Longrightarrow E$$

$$R = 27 \Longrightarrow 2(27) + 19 \ mod \ 37 = 36 \Longrightarrow \_$$

This method is then applied to each digit in the cipher-text

$$5\_GR4G2LP2GYRKE5\_GKE5IFIE2RE1E2R5O4I2$$
$$HRPENR5\_GRZE5\_G4RLZRKLYG42RFLK3O5I2H$$

$$\Downarrow$$

$$THE\_RENOWNED\_MATHEMATICIAN\_ALAN\_TURING$$
$$\_WAS\_THE\_FATHER\_OF\_MODERN\_COMPUTING$$

The End.

MA-190 Group Project 1

Callum Bracken, Diarmuid Deeney Curran, Zeiad Elmallah, Lohityh Ganesh Patchipala

November 2, 2020

Contents

1 Question 7

Which subset of the following statements is true?

1. (A) If $5x = 10$, then $x = 2$

   This statement is true since 10 divided by 5 can only be 2, and 10 divided by 2 can only be 5.

2. (B) If $5x \equiv 10 \mod 15$, then $x \equiv 2 \mod 15$

   This statement is false. Proving this by example, when $x = 8$, then $5x$ is equal to $10 \mod 15$. However, x would then be $8 \mod 15$. This is also due to the fact that 10 and 15 are not coprime, so they will have more common multiples than 2 and 15.

3. (C) If $5x \equiv 10 \mod 13$, then $x \equiv 2 \mod 13$

   This statement is correct. 10 and 13 are coprime and 2 and 13 are coprime, but since 2 and 10 are not coprime we can assume that for every case that $x = 2 \mod 13$, $5x$ will be 10 mod 13.

4. (D) If $4x \equiv 8 \mod 15$, then $x \equiv 2 \mod 15$

   This statement is similar to statement C, and is also true. 8 and 15 are coprime and so is 2 and 15, but 2 and 8 are not coprime. Again we can safely assume that at any point where $x = 2 \mod 15$, $4x$ will be equal to $8 \mod 15$.

5. (E) If $4x \equiv 8 \mod 15$, then $x = 2$

   Statement E is false. It states that x must be equal to 2, however x can be any value that satisfies the expression $4x = 8 \mod 15$. For example, $17 * 4 = 68 \equiv 8 \mod 15$.

Therefore, the correct subset is A, C and D.

2 Question 8

Using Euler's Phi function, find $5^{6050} \mod 11466$

$11466 = 1 * 6050 + 5416$
$6050 = 1 * 5416 + 634$
$5416 = 8 * 634 + 344$
$634 = 1 * 344 + 290$
$344 = 1 * 290 + 54$
$290 = 5 * 54 + 20$
$54 = 2 * 20 + 4$
$20 = 5 * 4 + 0$
$5^{\phi(6050)} = 1 \mod 6050$
$\phi(6050) = 2 * 3^2 * 7^2 * 13)$
$= \phi(2) * \phi(3^2) * \phi(7^2) * \phi(13)$
$= 1 * (3^2 - 3) * (7^2 - 7) * 12$
$= 3024$
$\therefore 5^{\phi(6050)} = 1 = 5^{3024}$
$\therefore 5^{6050} = 5^{3024} * 5^{3024} * 25$
$\therefore 5^{6050} \equiv 25 \mod 11466$

3 Question 11

A househusband is travelling to the market with all his eggs in one basket. He has between 100 and 200 eggs in the basket. Counting in threes there is one egg left over. Counting in fives there are four eggs left over and counting in sevens there are five eggs left over. How many eggs are in the basket?

Key information from this question:

- There are 100 to 200 eggs in the basket.
- There is 1 egg left when counting in threes ($1 \mod 3$)
- There are 4 eggs left when counting in fives ($4 \mod 5$)
- There are 5 eggs left when counting in sevens ($5 \mod 7$)

As is typically the case in mathematics, there are different ways to answer this question. One way is to use the Chinese remainder theorem but, in this case, I will be using a simpler method which I believe better fits the question.

Multiples of 3 between 100 and 200	Multiples of 5 between 100 and 200	Multiples of 7 between 100 and 200
102	100	105
105	105	112
108	110	119
111	115	126
114	120	133
117	125	140
120	130	147
123	135	154
126	140	161
129	145	168
132	150	175
135	155	182
138	160	189
141	165	196
144	170	
147	175	
150	180	
153	185	
156	190	
159	195	
162	200	
165		
168		
171		
174		
177		
180		
183		
186		
189		
192		
195		
198		

The answer is a number that meets all of the following requirements:

- 1 egg left over when counting in threes (1 more than a multiple of 3)
- 4 eggs left over when counting in fives (4 more than a multiple of 5)
- 5 eggs left over when counting in sevens (5 more than a multiple of 7)

It cannot be any of the numbers in the table since they are all divisible by 3, 5 or 7 with no remainder. In order to get the answer I will add 5 to each multiple of 7 listed and check if they fit the requirements.

The number that meets all of these requirements is 124, so the answer is 124.

4 Question 12

A function $f(n)$ is defined for all positive integers n as follows. First add the digits of n (in decimal notation) to get a number n_1. Then add the digits of n_1 to get n_2, and repeat the process until a single digit number is obtained. This last number is defined as $f(n)$. For example, $f(989) = f(26) = 8$. Evaluate $f(7 * (1234567)^8)$ and enter your number as an integer.

- Separate the equation into $7 \mod 9 * 1234567^8 \mod 9$
- $7 * (1234567)^8 \mod 9 = 7 \mod 9 * 1234567^8 \mod 9$
- Solve for $7 \mod 9 * 1234567^8 \mod 9$
- $1234567^8 \mod 9$ can be shortened to $1234567 \mod 9$
- $7 \mod 9 = 7$
- $1234567 \mod 9 = 1$
- $7 \mod 9 * 1234567 \mod 9 = 7 * 1 = 7$

$\therefore f(7 * (1234567)^8) = 7$

Group Project 1

Tom Gavin, Tomás Gillanders, Enda Harrigan
and Alannah Healy *

6 November 2020

Abstract

Objective of Project: Discuss the $\varepsilon - \delta$ definition for $\lim_{x \to a} f(x)$ and prove using the definition that if; $\lim_{x \to a} f(x) = L$ and $\lim_{x \to a} g(x) = M$ then $\lim_{x \to a}[f(x)g(x)] = LM$.

1 Introduction

The abstract concept of a limit has existed for millennia; originating from the 'mysterious' geometry of of the circle which perplexed the Ancient Greeks in the form of the concept of infinity. The abstract concept of both arbitrarily large and small numbers was viewed as dubious by the philosophers and mathematicians of this civilization, who depended upon the concrete practicality and certainty of mathematics. However, this vague construct proved to be a powerful tool, whether it being used by the Ancient Greek mathematician, *Archimedes*, to approximate the value of π or being the fundamental concept behind *Isaac Newton's* and *Gottfried Leibiniz's* development of differential calculus in the 1700s.

This abstract, yet intuitive, understanding of a limit is still pertinent and is readily applied throughout mathematics. However, an intuitive understanding of limits has its limitations; resulting in incorrect statements about calculus propagated by great mathematicians such as *Cauchy* and *Ampère*. The need for a precise and rigorous definition for a limit resulted in what is

*Workshop Tutor: Prof. Donal O'Regan

now known as the $\varepsilon - \delta$ definition of a limit. It is this definition and some of the properties that can be derived from it that will be addressed by this project.

2 Precise Definition of a Limit

2.1 Background Information

The precise definition of a limit that we use today was developed by the German mathematician, *Karl Weierstrass*, in response to the vague and often verbose definitions of limits that were commonplace in the mid 1800s. *Weierstrass* wished to convey the abstract concept of a limit in a clear and practical manner that would allow mathematicians to deal with limits through the use of concrete equations, rather than through the medium of abstract thought.

The intuitive definition of a limit that is often used nowadays is inadequate for certain purposed due to the vague nature of its phrasing. The precise definition is therefore a necessary tool; providing a rigorous method that can be used to conclusively prove that the limit of a function exists.

2.2 Defining a Limit

Definition. *Let f be a function defined on some open interval that contains the number a, except possibly a itself. Then we say that the limit of $f(x)$ as x approaches a is L, and we write*

$$\lim_{x \to a} f(x) = L$$

if for every number $\varepsilon > 0$, there exists a number $\delta > 0$ such that

$$\textit{if} \quad 0 < |x - a| < \delta \qquad \textit{then} \qquad |f(x) - L| < \varepsilon$$

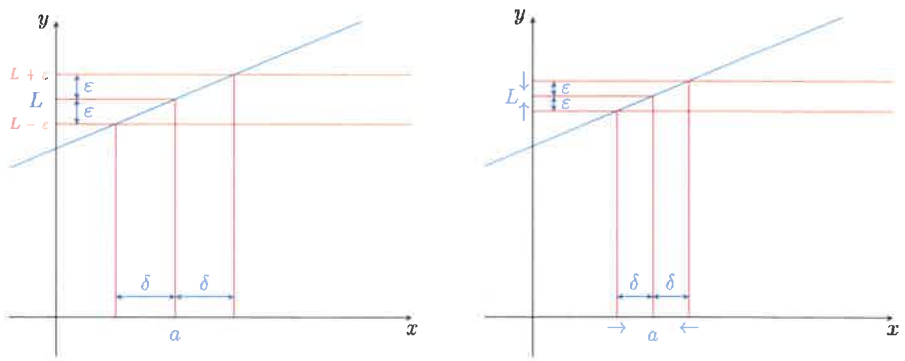
Explanation

The ε and δ used in the above definition ultimately define intervals of both output and input values. The inequalities used in the definition can be reformulated to state these intervals:

$$0 < |x - a| < \delta \quad \text{is equivalent to} \quad a - \delta < x < a + \delta, \quad x \neq a$$
$$|f(x) - L| < \varepsilon \quad \text{is equivalent to} \quad L - \varepsilon < f(x) < L + \varepsilon$$

In order to prove $\lim_{x \to a} f(x) = L$, it must be shown that for any number $\varepsilon > 0$ (that defines the interval $(L - \varepsilon, L + \varepsilon)$), there exists a number $\delta > 0$ (that defines the interval $(a - \delta, a + \delta)$), such that any value of $x \in \mathbb{R}$ and $x \neq a$ that lies within that interval is mapped by f into the open interval of outputs defined by ε.

A geometric interpretation of this definition is to be seen in Figure 1. If $\varepsilon > 0$ is given, then the horizontal lines $y_1 = L + \varepsilon$ and $y_2 = L + \varepsilon$ and the graph of f can be constructed. If $\lim_{x \to a} f(x) = L$, then a number $\delta > 0$ is found to be the magnitude of the difference between the x-values of the points where y_1 and y_2 intersect the curve $y = f(x)$ and the stated value a that the input x is set to approach. (If the graph is not symmetric around a, take $\delta = \min(\delta_1, \delta_2)$.) When x is restricted by the interval $(a - \delta, a + \delta)$ and $x \neq a$, it can be clearly seen that x is mapped by f into the interval $(L - \varepsilon, L + \varepsilon)$.



(a) Graph 1 (b) Graph 2

Figure 1: Geometrical interpretation of limits

Graph 2 of Figure 1 illustrates that when a smaller value for ε is selected, a smaller value for δ is also found. When the $\lim_{x \to a} f(x)$ exists, this process is true for *all* positive values ε. A corresponding δ can always be found.

2.3 Using the Precise Definition of a Limit

2.3.1 Example 1

To Prove:

$$\lim_{x \to 4} (4x + 13) = 29$$

Proof. Suppose $\varepsilon > 0$ has been provided.
Take $\delta = \frac{\varepsilon}{4}$
Since $\varepsilon > 0$, then we also have $\delta > 0$
For x, the expression $0 < |x - a| < \delta$ implies
$|x - 4| < \frac{\varepsilon}{4}$
$|4x - 16| < \varepsilon$
$|(4x + 13) - 29| < \varepsilon$
This lines up with the form $|f(x) - L| < \varepsilon$
Therefore, $\lim_{x \to 4} (4x + 13) = 29$

■

2.3.2 Example 2

To Prove:

$$\lim_{x \to 4} x^2 = 16$$

In order to prove this limit, an analysis of the question must first be done in order to determine a suitable $\delta > 0$ that can be used in the proof.

Given $\varepsilon > 0$, a number $\delta > 0$ must be found, such that

$$\text{if} \quad 0 < |x - 4| < \delta \quad \text{then} \quad |x^2 - 16| < \varepsilon$$

Through manipulation of the expression $|x^2 - 16| < \varepsilon$, observe that

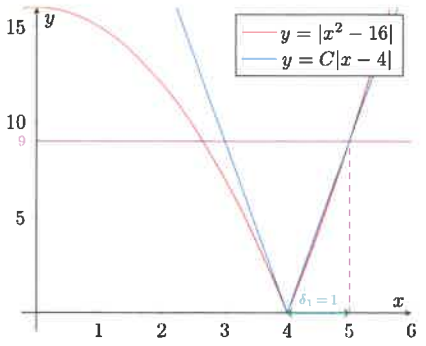
$$\begin{aligned} |x^2 - 16| = |(x + 4)(x - 4)| &= |x + 4|\,|x - 4| \\ &< C|x - 4| \\ &< \varepsilon \end{aligned}$$

where $|x + 4| < C$ for all input values x within a distinct interval defined by a given value $\delta > 0$.

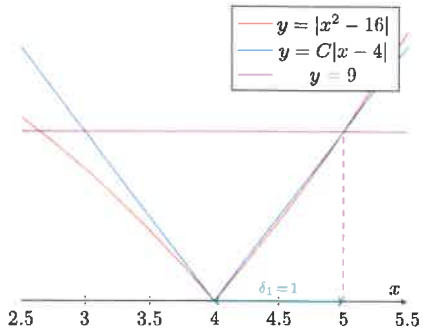
This manipulation suggests that $\delta = \frac{\varepsilon}{C}$. In order to obtain a value for C, x must be restricted to lie within an interval of δ_1 from 4. Since we are concerned with values of x 'close to' 4 (but not equal to 4), $\delta_1 = 1$ is appropriate. Therefore,

$$|x - 4| < 1 \quad \Rightarrow \quad 3 < x < 5 \quad \Rightarrow \quad |x + 4| < 9$$

This shows that when x is within $\delta_1 = 1$ of 4, then $|x + 4| < 9$, thus, showing that 9 is a suitable value for C; giving $\delta_2 = \frac{\varepsilon}{9}$. A geometrical representation of this reasoning to obtain C is shown in Figure 2.



(a) Graph 3



(b) Graph 4

Figure 2:
When $|x + 4| < C = 9$, $y = |x^2 - 16|$ is seen to be lesser than $y = C|x - 4|$ for all $0 < |x - 4| < \delta_1 = 1$. This geometrically shows that if $\delta = \min(1, \frac{\varepsilon}{9})$ then a value $\delta > 0$ can be found that satisfies the condition set by all $\varepsilon > 0$, $\varepsilon \in \mathbb{R}$. This is made more apparent by Graph 4.

Two restrictions are places on the interval $|x - 4|$, defined by δ_1 and δ_2.

$$|x - 4| < \delta_1 \qquad \text{and} \qquad |x - 4| < \delta_2$$

In order to satisfy both of these inequalities, the lesser of δ_1 and δ_2 is chosen:

$$\delta = \min(\delta_1, \delta_2) = \min\left(1, \frac{\varepsilon}{9}\right)$$

Proof. Let $\varepsilon > 0$ be given and take $\delta = \min(1, \frac{\varepsilon}{9})$. If $0 < |x - 4| < \delta$ then

$$|x - 4| < 1 \quad \Rightarrow \quad 3 < x < 5 \quad \Rightarrow \quad |x + 4| < 9$$

Also,

$$|x - 4| < \frac{\varepsilon}{9}$$

Therefore,

$$|x^2 - 16| = |x + 4|\,|x - 4| < 9 \cdot \frac{\varepsilon}{9} = \varepsilon$$

This proves that $\lim_{x \to 4} x^2 = 16$. ■

2.3.3 Example 3

To Prove:

$$\lim_{x \to 4}(x^3 - 4x^2 - x + 5) = 1 \tag{1}$$

First the question must be analysed in order to determine a suitable value for δ that can be used to prove that the limit defined in Line 1 is true.

Given $\varepsilon > 0$, a value $\delta > 0$ must be found such that

$$\text{if} \quad 0 < |x - 4| < \delta \quad \text{then} \quad |(x^3 - 4x^2 - x + 5) - 1| < \varepsilon$$

Through manipulation of the inequality $|(x^3 + 4x^2 - x + 5) - 1| > \varepsilon$, the following is true:

$$\begin{aligned} |(x^3 - 4x^2 - x + 5) - 1| &= |x^3 - 4x^2 - x + 4| \\ &= |(x - 4)(x^2 - 1)| \\ &= |x - 4|\,|x^2 - 1| \\ &< C|x - 4| < \varepsilon \end{aligned}$$

The statement $C|x - 4| < \varepsilon$ is true when $|x + 4| < C$. This suggests that $\frac{\varepsilon}{C}$ is a suitable value for δ. In order to obtain a value for C, x must be constrained to lie within some interval $(4 - \delta, 4 + \delta)$. As values of x 'close' to 4 are pertinent to what is to be proved, $\delta_1 = 1$ is suitable. Therefore,

$$\begin{aligned} 0 < |x - 4| < 1 \quad &\Rightarrow \quad 3 < x < 5 \\ &\Rightarrow \quad 8 < x^2 - 1 < 24 \quad \Rightarrow \quad |x^2 - 1| < 24 \end{aligned}$$

Therefore, when x is constrained by $\delta_1 = 1$, $C = 24$. This suggests that $\delta_2 = \frac{\varepsilon}{24}$. However, this places two restrictions on the inequality $0 < |x - 4| < \delta$. To satisfy both conditions the lesser of δ_1 and δ_2 is taken.

$$\delta = \min(\delta_1, \delta_2) = \min\left(1, \frac{\varepsilon}{24}\right)$$

Proof. Given $\varepsilon > 0$, take $\delta = \min(1, \frac{\varepsilon}{24})$. If $0 < |4 - x| < \delta$ then

$$|x - 4| < 1 \quad \Rightarrow \quad 3 < x < 5 \quad \Rightarrow \quad |x^2 - 1| < 24$$

Also,

$$|4 - x| < \frac{\varepsilon}{24}$$

Therefore'

$$|(x^3 - 4x^2 - x + 5) - 1| = |x^3 - 4x^2 - x + 4| = |x^2 - 1|\,|x - 4| < 24 \cdot \frac{\varepsilon}{24} = \varepsilon$$

This proves $\lim_{x \to 4}(x^3 - 4x^2 - x + 5) = 1$. ■

3 Limit Product Law

3.1 Background Information

When computing the limit for a given function $f(x)$ as x tends to a given value a; using methods of educated "guesswork" and imprecise approximations can often give rise to deceptively incorrect solutions. However, a set of provable properties of limits can be used to accurately evaluate the limit of a function $f(x)$ as it approaches a value. This is done through simplifying the function into more manageable 'sub-functions', whose limits can then be evaluated; ultimately allowing for the evaluation of the limit of the given function as a whole.

These properties of limits are referred to as the *Limit Laws*. For this project we are concerned with the limit *Product Law*, which states

$$\text{if} \qquad \lim_{x\to a} f(x) = L \qquad \text{and} \qquad \lim_{x\to a} g(x) = M, \tag{2}$$

then

$$\lim_{x\to a}[f(x)g(x)] = LM.$$

In proving this law in the next section, use will be made of *The Triangle Inequality*, which states if a and b are real numbers, then

$$|a+b| \leq |a| + |b|.$$

3.2 Proof of Product Law

In order to prove the *Product Law* of limits, allow the conditions listed in the Line 2 be true; stating that the limits of the functions exist as x approaches a.

Proof. Take $\varepsilon > 0$ to be given. A value $\delta > 0$ must be found, such that

$$\text{if} \qquad 0 < |x-a| < \delta \qquad \text{then} \qquad |f(x)g(x) - LM| < \varepsilon$$

In order to isolate the terms $|f(x) - L|$ and $|g(x) - M|$, $Lg(x)$ is added and subtracted from the term $|f(x)g(x) - LM|$ as follows:

$$\begin{aligned} |f(x)g(x) - LM| &= |f(x)g(x) - Lg(x) + Lg(x) - LM| \\ &= |g(x)[f(x) - L] + L[g(x) - M]| \\ &\leq |g(x)[f(x) - L]| + |L[g(x) - M]| \qquad \text{(Triangle Inequality)} \\ &= |g(x)| \cdot |f(x) - L| + |L| \cdot |g(x) - M| \end{aligned}$$

In order to prove this law each of these terms must be shown to be less than $\frac{\varepsilon}{2}$.
Since $\lim_{x\to a} g(x) = M$, there exists a number $\delta_1 > 0$ such that

$$\text{if} \quad 0 < |x-a| < \delta_1 \quad \text{then} \quad |g(x) - M| < \frac{\varepsilon}{2(1+|L|)}.$$

Also, there exists a number $\delta_2 > 0$ such that

$$\text{if} \quad 0 < |x-a| < \delta_2 \quad \text{then} \quad |g(x) - M| < 1$$

and therefore,

$$|g(x)| = |g(x) - M + M| \leq |g(x) - M| + |M|^* < 1 + |M|.$$

Since $\lim_{x\to a} f(x) = L$, there exists a number $\delta_3 > 0$ such that

$$\text{if} \quad 0 < |x-a| < \delta_3 \quad \text{then} \quad |f(x) - L| < \frac{\varepsilon}{2(1+|M|)}.$$

Let $\delta = \min(\delta_1, \delta_2, \delta_3)$. If $0 < |x-a| < \delta$, then $0 < |x-a| < \delta_1$, $0 < |x-a| < \delta_2$ and $0 < |x-a| < \delta_3$ are also true. These inequalities can be combined to obtain

$$\begin{aligned} |f(x)g(x) - LM| &\leq |g(x)| \cdot |f(x) - L| \; + \; |L| \cdot |g(x) - M| \\ &< (1 + |M|) \cdot \frac{\varepsilon}{2(1+|M|)} \; + \; |L| \cdot \frac{\varepsilon}{2(1+|L|)} \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \end{aligned}$$

This proves that $\lim_{x\to a}[f(x)g(x)] = LM$. ■

Using the Product Law

Example 3.2.1. The *Product Law* of limits can be used to efficiently and precisely compute the limit of a function, as shown in this following example.

Let $f(x) = 4x + 13$ and $g(x) = x^2$. In Examples 2.3.1 and 2.3.2 it was proved using the $\varepsilon - \delta$ definition of a limit that

$$\lim_{x\to 4} f(x) = 29 \quad \text{and} \quad \lim_{x\to 4} g(x) = 16$$

*Triangle Inequality

Using the *Product Rule* of limits, the limit of the product of these functions as x approaches 4 can effortlessly be computed, as follows:

$$\begin{aligned}\lim_{x\to 4}[f(x)g(x)] &= \lim_{x\to 4} f(x) \cdot \lim_{x\to 4} g(x) \\ &= \lim_{x\to 4}(4x+13) \cdot \lim_{x\to 4} x^2 \\ &= 29 \cdot 16 \quad = \quad 464\end{aligned}$$

Example 3.2.2. Take $v(x) = x^5 - 4x^4 - x^3 + 5x^2$. When computing $\lim_{x\to 4} v(x)$ one could use the *Sum Law* of limits [†] because the function v is a polynomial and is thus continuous for all $x \in \mathbb{R}$. However, another (and more laborious) method would be to factorise the function into sub-function whose limits are known and then apply the *Product Law* to evaluate the limit required. This process can be applied to $v(x)$ as follows:

$$\begin{aligned}\lim_{x\to 4} v(x) &= \lim_{x\to 4}[x^5 - 4x^4 - x^3 + 5x^2] \\ &= \lim_{x\to 4}[(x^2)(x^3 - 4x^2 - x + 5)]\end{aligned}$$

Let $g(x) = x^2$ and $h(x) = x^3 - 4x^2 - x + 5$. As proven in Examples 2.3.2 and 2.3.3,

$$\lim_{x\to 4} g(x) \;=\; 16 \qquad \text{and} \qquad \lim_{x\to 4} h(x) \;=\; 1$$

Therefore, using the *Product Law* the limit of $v(x)$ as x approaches 4 can easily be evaluated.

$$\begin{aligned}\lim_{x\to 4} v(x) &= \lim_{x\to 4}[g(x)h(x)] \\ &= \lim_{x\to 4} g(x) \cdot \lim_{x\to 4} h(x) \\ &= 16 \cdot 1 \;=\; 16\end{aligned}$$

3.3 Examples of the Product Law

The *Product Law* of limits can be used to prove other properties of limits which aid in the computation of the limit of a function as x approaches a specified value. Examples of these properties and how the *Product Law* can be used to prove them are listed below.

[†] $\lim_{x\to a}[f(x) + g(x)] = \lim_{x\to a} f(x) + \lim_{x\to a} g(x)$

3.3.1 Example 1

The limit of a constant times a function can be shown to be equal to the constant times the limit of the function using the *Product Law* of limits:

$$\lim_{x \to a} cf(x) \;=\; c \lim_{x \to a} f(x) \;=\; cL$$

where c is a constant.

Proof. Let $g(x) = c$. The *Product Law* of limits states:

$$\lim_{x \to a}[cf(x)] \;=\; \lim_{x \to a}[g(x)f(x)] \;=\; \lim_{x \to a} g(x) \cdot \lim_{x \to a} f(x)$$

The limit of a constant as x approaches any value is equal to the constant. In the case of the function $g(x) = c$, the function g does not depend on x. Using the $\varepsilon - \delta$ definition of a limit, for any value $\varepsilon > 0$, all values of $\delta > 0$ satisfy the condition set by the chosen ε because any input value x maps to the constant c. Using this property of the limit of a constant, it is found that

$$\begin{aligned} \lim_{x \to a} cf(x) \;&=\; \lim_{x \to a} c \cdot \lim_{x \to a} f(x) \\ &=\; c \lim_{x \to a} f(x) \\ &=\; cL \end{aligned}$$

■

Use of this Property

Let $f(x) = 4x + 13$ and $c = 2$. As proved using the $\varepsilon - \delta$ definition of a limit in Example 2.3.1, we know

$$\lim_{x \to 4} f(x) \;=\; 29$$

Therefore, using the property of a limit that the limit of a constant times a function is equal to the constant times the limit of the function as x approaches a given value a, it is true that

$$\begin{aligned} \lim_{x \to 4} cf(x) \;&=\; \lim_{x \to 4} 2(4x + 13) \\ &=\; 2 \cdot \lim_{x \to 4}(4x + 13) \\ &=\; 2 \cdot 29 \;=\; 58 \end{aligned}$$

3.3.2 Example 2

The limit of a square of a function can be shown to be equal to the square of the limit using the *Product Law* of limits:

$$\lim_{x \to a}[f(x)]^2 = L^2$$

Proof. The square in question can be rewritten as follows:

$$\lim_{x \to a}[f(x)]^2 = \lim_{x \to a}[f(x) \cdot f(x)] = \lim_{x \to a} f(x) \cdot \lim_{x \to a} f(x)$$

The *Product Law* of limits, as outlined above, can be used to prove the following

$$\begin{aligned} \lim_{x \to a}[f(x)]^2 &= \left[\lim_{x \to a} f(x)\right]^2 \\ &= \lim_{x \to a} f(x) \cdot \lim_{x \to a} f(x) \\ &= L \cdot L \\ &= L^2 \end{aligned}$$

■

Through the repeated use of the *Product Law*, this property of limits can be further generalised to show that

$$\lim_{x \to a}[f(x)]^n = \left[\lim_{x \to a} f(x)\right]^n = L^n$$

where n is a positive integer.

Use of this Property

Let $f(x) = 4x + 13$. As proved using the $\varepsilon - \delta$ definition of a limit in example 2.3.1, we know

$$\lim_{x \to 4} f(x) = 29$$

Therefore, using the property of a limit that $\lim_{x \to a}[f(x)]^n = L^n$, where n is a positive integer, it is true that

$$\begin{aligned} \lim_{x \to 4}[f(x)]^2 &= \lim_{x \to 4}(4x + 13)^2 \\ &= \left[\lim_{x \to 4}(4x + 13)\right]^2 \\ &= 29^2 = 841 \end{aligned}$$

3.3.3 Example 3

The limit of a quotient of functions can be shown to be equal the quotient of the limit using the *Product Law* of limits, provided that the limit of the function in the denominator is not zero.

$$\lim_{x\to a}\frac{f(x)}{g(x)}=\frac{L}{M}\qquad \text{if } \lim_{x\to a}g(x)\neq 0$$

The quotient in question can be rewritten as a product as follows:

$$\lim_{x\to a}\left[f(x)\cdot\frac{1}{g(x)}\right]=L\cdot\frac{1}{M}\qquad \text{if } \lim_{x\to a}g(x)\neq 0$$

In order to use the *Product Law* to prove this property of limits it must first be shown that

$$\lim_{x\to a}\frac{1}{g(x)}=\frac{1}{M}\qquad \text{if } \lim_{x\to a}g(x)\neq 0$$

The *Product Law* could then easily be implemented; hence, proving this property.

Proof. First it must be shown that

$$\lim_{x\to a}\frac{1}{g(x)}=\frac{1}{M}$$

This means that for a given $\varepsilon>0$, a $\delta>0$ must be shown to exist, such that

$$\text{if}\qquad 0<|x-a|<\delta\qquad \text{then}\qquad \left|\frac{1}{g(x)}-\frac{1}{M}\right|<\varepsilon$$

By manipulating the expression above we obtain

$$\left|\frac{1}{g(x)}-\frac{1}{M}\right|\quad=\quad\left|\frac{g(x)-M}{Mg(x)}\right|$$

A x approaches a, we know that the numerator of this expression approaches 0. However, it must be shown that the denominator of this expression does not approach 0. Since, $\lim_{x\to a}g(x)=M$, there exists a $\delta_1>0$, such that

$$\text{if}\qquad 0<|x-a|<\delta_1\qquad \text{then}\qquad |g(x)-M|<\frac{|M|}{2}$$

and therefore,

$$|M| \;=\; |M - g(x) + g(x)| \;\leq\; |M - g(x)| + |g(x)|^{\ddagger} \;<\; \frac{|M|}{2} + |g(x)|$$

This expression can be manipulated to show that

$$\text{if} \qquad 0 < |x - a| < \delta_1 \qquad \text{then} \qquad |g(x)| > \frac{|M|}{2}$$

Therefore, for the values of x defined by δ_1, the following is true:

$$\frac{1}{|Mg(x)|} \;=\; \frac{1}{|M| \cdot |g(x)|} \;\leq\; \frac{1}{|M|} \cdot \frac{2}{|M|} \;=\; \frac{2}{|M|^2}$$

Also, there exists a number $\delta_2 > 0$, such that

$$\text{if} \qquad 0 < |x - a| < \delta_2 \qquad \text{then} \qquad |g(x) - M| < \frac{|M|^2}{2}\varepsilon$$

Let $\delta = \min(\delta_1, \delta_2)$. This value of δ allows both of the statements above to be true. Therefore the following is also true:

$$\left|\frac{1}{g(x)} - \frac{1}{M}\right| \;=\; \left|\frac{g(x) - M}{Mg(x)}\right| \;<\; \frac{2}{|M|^2} \cdot \frac{|M|^2}{2}\varepsilon \;=\; \varepsilon$$

This proves that $\lim_{x \to a} \frac{1}{g(x)} = \frac{1}{M}$. The *Product Law* of limits can then be used to prove

$$\lim_{x \to a}\left[\frac{f(x)}{g(x)}\right] \;=\; \lim_{x \to a}\left[f(x) \cdot \frac{1}{g(x)}\right] \;=\; \lim_{x \to a} f(x) \cdot \lim_{x \to a} \frac{1}{g(x)} \;=\; L \cdot \frac{1}{M} \;=\; \frac{L}{M}$$

■

Use of this Property

Let $f(x) = 4x - 13$ and $g(x) = x^2$. As proved using the $\varepsilon - \delta$ definition of a limit in Examples 2.3.1 and 2.3.2, we know

$$\lim_{x \to 4} f(x) \;=\; 29 \qquad \text{and} \qquad \lim_{x \to 4} g(x) \;=\; 16$$

[‡]Triangle Inequality

Therefore, using the property of limits that the limit of a quotient of functions is equal to the quotient of the limits of the functions, as x approaches a given value a, it is true that

$$\begin{aligned}\lim_{x\to 4}\left[\frac{f(x)}{g(x)}\right] &= \lim_{x\to 4}\left[\frac{4x+13}{x^2}\right] \\ &= \frac{\lim_{x\to 4}(4x+13)}{\lim_{x\to 4}(x^2)} \\ &= \frac{29}{16}\end{aligned}$$

3.4 Conclusion

A limit of a function is a powerful concept and tool that is used throughout the discipline of Mathematical Analysis and underpins the foundation on which the principles of the various branches of mathematics within it are built. Calculus, real and complex analysis and measure theory are but a few areas of mathematics which depend of the use of the limit and the precise definition that defines it. The precise definition of a limit is often overlooked by non-mathematicians when using the mathematical tools which depend on the concept of a limit. However, a proper understanding of it can lead to a clearer and more fundamental insight into the mathematical problems that are commonly dealt with.

MA180 Group Project

Limits - Proving from the epsilon delta definition

Polina Antonova
Adam Burke
David Callaghan
Monirul Choudhury
David Cullen

Tutor - Donal O'Regan

October 2020

1 Project Question

What does Examples of the Property mean?

We were asked to construct examples assuming nothing about limits. Example give was to prove the property

$$\lim_{x\to a}[f(x)g(x)] = \lim_{x\to a} f(x)][\lim_{x\to a} g(x) \tag{1}$$

Prove from the Epsilon Delta definition.

2 Unique Property

Consider the following two inequalities: 5–3 < 3 and 5–4 < 3. We may note that the preceding inequalities follow the general format of the epsilon side of the delta-epsilon definition. Note from this that it also cannot be inferred directly from the epsilon inequality that $L_1 = L_2$. Naturally, therefore, we precede by contradiction. Intuitively we may investigate L_1–L_2, the distance between the two points, as we can imagine that as f(x) approaches either of the two limits from within this interval the distance between f(x) and the other limiting point grows. Investigating this further we find that L_1–L_2 is bounded above by 2ε by definition or $\varepsilon > (L_1–L_2)/2$. Then for the contradiction it suffices to impose an upper bound on ε of $(L_1–L_2)/2$. Note that there is nothing intrinsically special about our choice of 2ε – if L_1–L_2 is bounded above by 2ε it follows that L_1–L_2 is bounded above by Aε, where A is any real number greater than 2, motivating different upper bounds.

3 Proof

Proof. Suppose $L_2 = L_1| \Rightarrow |L_2 - L_1| > 0$
Suppose $\varepsilon < \frac{|L_2-L_1|}{2} \Rightarrow 2\varepsilon < |L_2 - L_1|$
Then
$2\varepsilon > |f(x) - L_1| + |f(x) - L_2|$
$= |f(x) - L_1| + |-f(x) + L_2|$
$\geq |f(x) - f(x) + |L_2 - L_1| = |L_2 - L_1| > 0$

But $2\varepsilon < |L_2 - L_1|$
Contradiction

$\therefore L_1 = L_2$ □

4 Addition Property

Preceding normally with the triangle inequality we find that $[f(x)+g(x)-(L_1+L_2)]$ is bounded above by 2ε. In this case, 2ε serves the same purpose as ε in the sense that it includes all the real numbers except 0. Noting this, we precede as follows: for every epsilon we choose we simply choose a delta such that f(x) $-L_1$ and g(x) $-L_2$ are less than $\varepsilon/2$. To satisfy both we choose the minimum of (δ_1, δ_2).

5 Proof

Proof. By assumption

For $0 < |x-1| < \delta_1 \Rightarrow |f(x) - L_1| < \varepsilon$
$0 < |x-1| < \delta_1 \Rightarrow -\varepsilon < |g(x) - L_1| < \varepsilon$

Then choose $\delta = \min(\delta_1, \delta_2)$ such that

$|f(x) - L_1| < \frac{\varepsilon}{2}$
$|g(x) - L_2| < \frac{\varepsilon}{2}$

$\Rightarrow |(f(x)+g(x)) - (L_1+L_2)|$
$= |f(x)+g(x) - L_1 - L_2|$
$= |(f(x) - L_1) + (g(x) - L_2|$
$= |(f(x) - L_1) + (g(x) - L_2|$
$= |(f(x) - L_1) + (g(x) - L_2| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2}$

$\therefore$ For $\delta = \min(\delta_1, \delta_2)$

$\Rightarrow |(f(x)+g(x) - (L_1+L_2)| < \varepsilon$

Or that

$\lim_{x \to >c}[f(x)+g(x)] = L_1 + L_2$ $\square$

6 Linear Equation

$$\lim_{x \to 2} 4x - 12 = -4 \tag{2}$$

Proof.

$= f(x) - L| < \varepsilon$ First find a value for delta.

$= |4x - 8| < \varepsilon$ Sub in known values.

$= |4||x - 2| < \varepsilon$ Factor.

$= |x - 2| < \frac{\varepsilon}{4}$

$=$ Since $\varepsilon > 0$ and $|x - 2| < \delta$ Now prove

$= |x - 2| < \frac{\varepsilon}{4} \Rightarrow |4||x - 2| < |4|\frac{\varepsilon}{4}$ Get the inverse.

$= |4x - 8| < \varepsilon$ Rewrite.

$= |f(x) + 4| < \varepsilon$

$\therefore \lim_{x \to 2} 4x - 12 = -4$ $\square$

7 Quadratic Equation

$$\lim_{x \to 1} 4x^2 + 3x + 7 = 14 \tag{3}$$

Proof.

$$\begin{aligned}
&= f(x) - 14 < \varepsilon \\
&\Longrightarrow |4x^2 + 3x - 7| < \varepsilon \\
&= |(4x + 7)(x - 1)| < \varepsilon \\
&\Longrightarrow |x - 1| < \frac{\varepsilon}{(4x + 7)}
\end{aligned}$$

Since x is approaching 1 :

$$\begin{aligned}
&= 0 < x < \delta \\
&\Longrightarrow 0 < |(4x) < 8 \\
&= 7 < |(4x + 7)| < 15 \\
&= \frac{1}{15} < \frac{1}{(4x + 7)} < \frac{1}{7} \\
&= \frac{\epsilon}{15} < \frac{\varepsilon}{|4x + 7|}
\end{aligned}$$

Therefore $\delta \leq \frac{\varepsilon}{15}$

$$\begin{aligned}
&= |(x - 1)| < 6 \\
&\Longrightarrow |(x - 1)| < \frac{\varepsilon}{15} \\
&= |(x - 1)| < \frac{\epsilon}{(4x + 7} \\
&= |(x - 1)(4x + 7)| < |(4x + 7)| < \frac{\varepsilon}{(4x + 7)}
\end{aligned}$$

$$\begin{aligned}
&\Longrightarrow \therefore |(4x^2 + 3x - 7)| < \varepsilon \\
&= |f(x) - 14| < \varepsilon
\end{aligned}$$

$\therefore \lim_{x \to 1}(4x^2 + 3x + 7) = 14$ $\square$

8 Cubic Polynomial

$$\lim_{x \to 1} x^3 + 5x = 6 \tag{4}$$

Proof.

$= f(x) - L| < \varepsilon$

$= |x^3 + 5x - 6| < \varepsilon$ Sub in values.

$= |(x - 1)(x^2 + x + 6)| < \varepsilon$ Factorise.

$\Longrightarrow |x - 1| < x^2 + x + 6$

= Since x is approaching $1, 0 < x < 2$

$= 0 < x < 2 \Rightarrow 0 < x^2 < 4$ Square each value.

$= 0 < x^2 + x < 6$ Add $0 < x < 2 (0 + 0 < x^2 + x < 4 + 2)$

$= 6 < x^2 + x + 6 < 12$ Add 6 to each value.

$\Longrightarrow \frac{1}{12} < \frac{1}{|x^2 + x + 6|} < \frac{1}{6}$ Get inverse of each value.

$\Longrightarrow \frac{\varepsilon}{12} < \frac{\varepsilon}{|x^2 + x + 6|}$ Multiply by ε.

= Since $|x - 1| < 5[$

$= |x - 1| < \frac{\epsilon}{12}$

$\Longrightarrow |x - 1| < \frac{\varepsilon}{|x^2 + x + 6|}$

$= |x - 1||x^2 + x + 6| < |x^2 + x + 6| < \frac{\varepsilon}{x^2 + x + 6}$

$= |x^3 + 5x - 6| < \varepsilon$ Simplify.

$\Longrightarrow |(fx) - 6| < \varepsilon$ Definition.

□

9 Cubic function

$$\lim_{x \to 2} x^3 = 8 \tag{5}$$

Proof.

$$\begin{aligned}
&= 0 < |x-2| < \delta \Rightarrow ||x^3 - 8| = |x^3 - 2^3| \\
&= |x^3 - 2^3| = |x-2| - |x^2 + 2x + 4| \\
\text{Sub in } < \delta \text{ for } |x-2| &=< \delta \cdot |x^2 + 2x + 4| \\
&= 0 < |x-2| < \delta \\
&= -\delta < |x-2| < \delta \\
&= 2 - 8 < x < 2 + \delta \\
\text{Let } \delta &= 1 \\
&= 1 < x < 3 \\
&= \delta \text{ can be} \leq 1 \\
&=< \delta \cdot |x^2 + 2x + 4| \\
&=< \delta \cdot 19 < \varepsilon \\
\text{When } \delta &= \frac{\varepsilon}{19} \\
&=\therefore \delta \text{ can be} \leq \frac{\varepsilon}{19}
\end{aligned}$$

$$\text{Let } \varepsilon > 0. \text{ Choose } \delta = \min\left(1, \frac{\varepsilon}{19}\right)$$

Then for all x with $0 < |x-2| < \delta$

$$\begin{aligned}
&= |x^3 - 8| = |x-2||x^2 + 2x + 4| \\
&=< \delta \cdot (9 + 6 + 4) \\
&= \delta \cdot 19
\end{aligned}$$

$\therefore \lim_{x \to 2} x^3 = 8$ $\square$

Maths Project

a.forde28@nuigalway.ie, e.forde16@nuigalway.ie, a.donnelly18@nuigalway.ie

November 2020

Names: Aaron Forde, Evan Forde and Austin Donnelly
Tutor: donal.oregan@nuigalway.ie

1 Introduction

Our Project was to Discuss the $\epsilon - \delta$ definition for the $\lim_{x \to a} f(x)$ and prove using the definition that if, $\lim_{x \to a} f(x) = L$ and $\lim_{x \to a} g(x) = M$ then $\lim_{x \to a}[f(x) + g(x)] = L + M$ and to find examples of the property.

We first used Weierstrass' definition of a Limit that tells us, Let **f** be a function defined on some open interval that contains the number **u**, except possibly at **u** itself. Then we say that the **limit of f(x) as x approaches u is L**, and we write $\lim_{x \to a} f(x) = L$ if for every number ϵ ¿ 0 there is a number δ ¿ 0 such that: if 0¡—x-a—¡δ then —f(x)-L—¡ϵ

2 Proof

$\lim_{x \to a} f = L$ ..... $lim_{x \to a} g = M$
$\lim_{x \to a}(f + g)(x) = L + M$
ϵ ¿ 0. $\delta_1 > 0 for all values of x$
—x-a—¡δ_1,,,, $|f(x) - L| < \epsilon/2$
ϵ¿0,$\delta_2 > 0 for all values of x$
—x-a—¡δ then —(f+g)(x)-(L+M)—¡ϵ
take δ = minimum (δ_1,δ_2)
we assume
—f(x)-L— ¡$\epsilon/2$ and —g(x)-M— ¡ $\epsilon/2$
are true
—f(x)-L+g(x)-M— is less than or equal to —f(x)-L—+—g(x)-M—¡ $\epsilon/2$ + $\epsilon/2$
using
—a+b— = —a—+—b—
=—f(x) +g(x) - L - M—
=—f(x)+g(x)-(L+M)— ¡ ϵ
same as
—x-a—¡ δ goes to —(f+g)(x)-(L+M)— ¡ ϵ

Q.E.D

3 Examples Of The Properties

Take for example:

$\lim_{x\to 2} x = 2$

$\lim_{x\to 2} 2x = 4$

$\lim_{x\to 2}[x + 2x] = 6$
$\lim_{x\to 2}[3x] = 6$

This is true for all values

4 Conclusion

As seen above $\lim_{x\to a}[f(x)+g(x)] = L+M$ using the $\epsilon-\delta$ definition of a limit.

Thus we can say for all values "x" that are added together that go to the same limit "a" can be added together.

MA180 Project
Workshop tutor: Donal O Regan

November 5, 2020

by Niamh O Toole, Olivia Philo, Tadhg O Donnell, Eoghan O Domhnaill

1 Project Question

Discuss the $\epsilon - \delta$ definition for $\lim_{x \to a} f(x)$
Prove using the defintion that if $\lim_{x \to a} f(x) = L$ and α is a real number then $\lim_{x \to a}[\alpha f(x)] = \alpha L$

2 $\epsilon - \delta$ definition

Definition: $\lim_{x \to a} f(x) = L$ means that for every $\epsilon > 0$ there exists a $\delta > 0$, such that for all x, $0 < |x - a| < \delta$ implies $|f(x) - L| < \epsilon$
In other words, given an ϵ close to L, a δ can be found whose x is within δ of a. Then f(x) will be within ϵ of L.
i.e Take any x in the range (a-δ, a+δ), f(x) will be within the range (L-ϵ, L+ϵ).
Limits are functions that approach a certain input. So for any distance around the limit of a certain value, say L, the range for each value within that range can be shown, meaning it is closer to L than ϵ. This is useful for finding change in speed or velocity as time approaches 0, without dividng by 0.

3 Proof of Property

Prove $\lim_{x\to a}[\alpha f(x)] = \alpha L$ where $\lim_{x\to a} f(x) = L$ and α is a real number. Use the Constant Multiple Law which states that the limit of a constant times a function is the constant times the limit of the function.
Proof: Consider $\lim_{x\to a}[f(x)g(x)] = \lim_{x\to a} f(x).\lim_{x\to a} g(x)$
Let α=g(x)
Thus: $\lim_{x\to a}[\alpha.f(x)] = \lim_{x\to a} \alpha.\lim_{x\to a} f(x) = \alpha.\lim_{x\to a} f(x)$
However: $\lim_{x\to a} f(x) = L$
So: $\alpha.\lim_{x\to a} f(x) = \alpha.L$

4 Examples of the Property

1.
$\lim_{x\to 1}[-3x^3]$ = -3.$\lim_{x\to 1} x^3$ = -3(1) = -3
2.
$\lim_{x\to -3}[4x + 2] = \lim_{x\to -3}[4x] + \lim_{x\to -3} 2 = 4.\ \lim_{x\to -3} x + \lim_{x\to -3} 2 =$ 4(-3)+2 = -10
3.
$\lim_{x\to 5} 3(x - 2) = 3.\lim_{x\to 5} x - 2 = 3.\lim_{x\to 5} x - \lim_{x\to 5} -2 = 3(5 - 2) = 9$

Project 1

Aislinn Reidy,Ben Somers,Daniel Smyth,Jenny Roe

(Tutor:Donal 0'Regan)

Question: Discuss the $\epsilon - \delta$ definition for $\lim_{x\to a} f(x)$ and prove using the definition that if $f(x) \leq g(x) \leq h(x)$ for $0 < |x-a| < \rho$ (here $\rho > 0$) and $\lim_{x\to a} f(x) = L = \lim_{x\to a} h(x)$ then $\lim_{x\to a} g(x) = L$.

1 The $\epsilon - \delta$ definition for $\lim_{x\to a} f(x)$

In a looser definition of a limit, we say that by making x sufficiently close to a, but not equal to a ,we can make the function f(x) very close to the limit L but not at L.Bringing x closer to a, then brings f(x) closer again to the limit, without ever reaching the limit.In very basic terms, as f(x) approaches L, x approaches a. The rigorous definition of a limit explains the reasoning behind this idea a bit more. We know from our knowledge of limits that the distance from x to a is $|x-a|$, likewise the distance from f(x) to L is $|f(x)-L|$.Hence if we take ϵ to be a small specified distance from the limit, then $|f(x) - L < \epsilon|$ if $|x-a| < \delta$ but $\neq$ a. If we then take $0 < |x-a| < \epsilon$, we can always find an appropriate δ, by equating it to a fraction of ϵ.

For example: If we are given a function $[\lim_{x\to 1} \frac{3x(x-1)}{x-1} = 3]$ and are told $\epsilon < 0$ then we can find a $\delta < 0$ by the following method:

Taking, $0 < |x-1| < \delta$

The distance between the function and the limit is:$|\frac{3x(x-1)}{x-1} - 3| < \epsilon$
This simplifies down to,

$|3x-3| < \epsilon$
$|3(x-1)| < \epsilon$
$|3||x-1| < \epsilon$
$|x-1| < \frac{\epsilon}{3}$

We can now use the number $\frac{\epsilon}{3}$ as our δ value.

2 Proof of $f(x) \leq g(x) \leq h(x)$ (The sandwich theorem)

We must find a $\delta > 0$ *such that* $|g(x) - L| < \epsilon$ *when* $0 < |x - a| < \delta$.
Proof:
Since $\lim_{x \to a} f(x) = L$,this means that according to our definition of a limit, there exists $\delta_1 > 0$ such that
$|f(x) - L| < \epsilon$ **for** $0 < |x - a| < \delta_1$
Thus,
$-\epsilon < f(x) - L < \epsilon$ **for** $0 < |x - a| < \delta_1$
$L - \epsilon < f(x) < L + \epsilon$ **for** $0 < |x - a| < \delta_1$
Likewise, since $\lim_{x \to a} h(x) = L$, a $\delta_2 > 0$ also exists in which,
$L - \epsilon < h(x) < L + \epsilon$ **for** $0 < |x - a| < \delta_2$
Since $f(x) \leq g(x) \leq h(x)$ for x values in an interval containing a, there exists some $\delta_3 > 0$ such that,
$f(x) \leq g(x) \leq h(x)$ **for** $0 < |x - a| < \delta_3$
We then choose $\delta = min(\delta_1, \delta_2, \delta_3)$
We now have,
$L - \epsilon < f(x) \leq g(x) \leq h(x) L + \epsilon$ **for all** $0 < |x - a| < \delta$
Therefore,
$-\epsilon < g(x) - L < \epsilon$ **for** $0 < |x - a| < \delta$
ie.$|g(x) - L| < \epsilon$ **for all** $0 < |x - a| < \delta$
Hence, by using the definition of limits we have proved that $\lim_{x \to a} g(x) = L$

Example 1
Show that $\lim_{x \to 0} x^2 Sin\frac{1}{x} = 0$
Using our knowledge of Sine functions, We know that we can say the sine of any number lies between -1 and 1, therefore:
$-1 \leq Sin\frac{1}{x} \leq 1$
Multiplying both sides by x^2 we get
$-x^2 \leq x^2 Sin\frac{1}{x} \leq x^2$
We know that the $\lim_{x \to 0} (x^2) = 0$ and that the $\lim_{x \to 0}(-x^2) = 0$
Therefore if we decide that,
$f(x) = -x^2$,
$g(x) = x^2 Sin\frac{1}{x}$
$h(x) = x^2$
According to the Sandwich theorem we get $\lim_{x \to 0} x^2 Sin\frac{1}{x} = 0$

Example 2
If we are told three functions follow $f(x) \leq g(x) \leq h(x)$ and are also told that x is close to 2
If we know $f(x) = -\frac{-1}{3}x^3 + x^2 - \frac{7}{3}$ and $h(x) = \cos(\frac{\pi}{2}x)$
We can work out the limit of the third function g(x)
First we find $\lim_{x \to 2} f(x)$
$\lim_{x \to 2} f(x) = \lim_{x \to 2}(\frac{-1}{3}x^3 + x^2 - \frac{7}{3})$
$(\frac{-1}{3}(2)^3 + (2)^2 - \frac{7}{3})$

$= -1$
Now we find $\lim_{x \to 2} h(x)$
$\lim_{x \to 2} h(x) = \lim_{x \to 2} \cos(\frac{\pi}{2} x)$
$= \cos(\frac{\pi}{2}(2))$
$= -1$
Since we have shown that the limit of f(x) and h(x) are the same,according to the Sandwich theorem we can guarantee that $\lim_{x \to 2} g(x) = -1$

References:
Calculus Early Transcendentals -James Stewart

Maths Project: Group 1
ϵ-δ definition

Aidan O'Beirn, Chloe Lawlor, Miriam Kennedy, Cian Sweeney, Jonny O'Connor

October 2020

1 Contents

2 Epsilon-Delta Proof

$$\lim_{x \to a} f(x)$$

For every

$$\epsilon > 0$$

there exists a

$$\delta > 0$$

such that for every

$$x$$

the expression

$$0 < |x - c| < \delta$$

this implies

$$|f(x) - L| < \epsilon$$

2.0.1 Explanation of the proof

The phrase "for every $\epsilon < 0$ " signifies that one does not control the value of epsilon, the proof must work for all values of epsilon.

The phrase "there exists a $\delta > 0$" signifies that the proof must give the value of delta thus confirming the existence of it.

The phrase "such that for ever x" signifies that we cannot restrict the value of x any further than the next restriction provides.

The phrase the expression "$0 < |x - c| < \delta$" is the start of a series of algebra steps which concludes with the final statement. The expression "$|x - c| < \delta$" means that x will be close to c More specifically, x will be no more than nor equal to δ units from c.

The key to the proof is finding the value of δ. In order to find δ one typically begins with $|f(x) - L| < \epsilon$ which is the final statement. From the final statement one works back until the form $|x - c| < \delta$ is reached.

2.0.2 Examples

Prove using δ and ϵ that:

$$\lim_{x \to -4}(5x - 6) = -26$$

We must find the value of δ before we can start the proof

Step 1 : We begin from the final statement and work backwards

$$|f(x) - L| < \epsilon$$

Step 2: We substitute in our values of $f(x)$ and L

$$|(5x - 6) - (-26)| < \epsilon$$

$$|(5x - 6) + 26| < \epsilon$$

Step 3 : We simplify inside of the absolute value, we are aiming to obtain the form $|x - c| < \delta$

$$|5x + 20| < \epsilon$$

$$|5(x + 4)| < \epsilon$$

$$|5||x + 4| < \epsilon$$

$$|x + 4| < \frac{\epsilon}{5}$$

Step 4: We now have the form $|x - c| < \delta$ (in our case $|x - (-c)|$). Recall that we are evaluating a limit as x approaches -4 therefore x must be equal to -4. Thus delta must be equal to or smaller than ϵ divided by 5.

Now we are ready to write out proof.

Suppose

$$\epsilon > 0$$

This is always the first line of the proof. It signifies that our argument will work for every epsilon

Define

$$\delta = \frac{\epsilon}{5}$$

Since the definition of the limit claims a delta exists we use the value found in our preliminary work above as the value of delta

Since

$$\epsilon > 0$$

then we also have

$$\delta > 0$$

Now for every x the expression $0 < |x - c| < \delta$ implies $|x + 4| < \frac{\epsilon}{5}$

This is simply just the words from the next part of the definition

$$|x + 4| < \frac{\epsilon}{5}$$

Here we replaced the value of c and δ with values specific to our problem.

$$|5x + 20| < \epsilon$$

Here we begin to work in reverse order to our preliminary work

$$|(5x - 6) - (-26)| < \epsilon$$

Here we break the expression into the original function and the limit value
Therefore

$$\lim_{x \to -4} f(5x - 6) = -26$$

We have obtained our final result while meeting all the requirements of the definition of the limit Q.E.D

3 Properties

(1)

$$\lim_{x \to a}[cf(x) = cK$$

(2)

$$\lim_{x\to a}[f(x) \pm g(x)] = \lim_{x\to a} f(x) \pm \lim_{x\to a} g(x) = K \pm L$$

(3)

$$\lim_{x\to a}[f(x)g(x)] = \lim_{x\to a} f(x) \lim_{x\to a} g(x) = KL$$

(4)

$$\lim_{x\to a}[f(x)]^n = [\lim_{x\to a} f(x)]^n = K^n \; n \geq 2, \; n \in i$$

(5)

$$\lim_{x\to a} c = c$$

3.1 Proof of 5

To prove:

$$\lim_{x\to a} c = c$$

$$f(x) = c$$

Let

$$\epsilon > 0$$

(Epsilon has to be greater than zero as f(x) is equal to c)
and show we can find

$$\delta > 0$$

so whenever

$$0 <\mid x - a \mid< \delta$$

because we defined

$$f(x) = c$$

$$\mid f(x) - c \mid< \epsilon$$

(The modulus of f(x)-c has to be zero as f(x) is c)

so choose

$$\delta > 0$$

to equal any number, then

$$\mid f(x) - c \mid=\mid c - c \mid= 0 < \epsilon$$

3.1.1 Example

To show that $|f(x) - c| < \epsilon$
We assume that
$$f(x) = c$$

And we end up with
$$|f(x) - c| = |c - c| = 0 < \epsilon$$

For example, let's assume
$$c = 5,$$

This will give us the following equation
$$|5 - 5| = |5 - 5| = 0 < \epsilon$$

3.2 Proof of 1

There are several ways to prove this part. If you accept 3 And 7 then all you need to do is let g(x) = c and then this is a direct result of 3 and 7. However, we'd like to do a more rigorous mathematical proof. So here is that proof. First, note that if c = 0 then cf(x) = 0

$$\lim_{x \to a} 0f(x) = \lim_{x \to a} = 0 = 0f(x)$$

The limit evaluation is a special case of 7 (with c = 0) which we just proved Therefore we know 1 is true for c = 0 and so we can assume that c $\neq$ 0 for the remainder of this proof.
Let $\epsilon > 0$ then because $\lim_{x \to a} f(x) = K$ by the definition of the limit there is a $\delta > 0$ such that,

$$|f(x) - K| < \frac{\epsilon}{|c|} whenever 0 < |x - a| < \delta$$

Now choose $\delta = \delta 1$ and we need to show that

$$|cf(x) - cK| < \epsilon whenever 0 < |x - a| < \delta$$

and we"l be done. So, assume that $0 < |x - a| < \delta$ and then,

$$|cf(x) - cK| = |c||f(x) - K| < |c|\frac{\epsilon}{|c|} = \epsilon$$

3.2.1 Example

To show that
$$|cf(x) - K| = c|f(x) - K| < |c|\frac{\epsilon}{|c|}$$

Let's assume that c=5

$$|5f(x) - K| = 5|f(x) - K| < |5|\frac{\epsilon}{|5|}$$

$$\frac{|5|\epsilon}{|5|} = \epsilon$$

3.3 Proof of 2

In limits there is something called triangle inequality which is necessary for this proof. The triangle inequality says that,

$$|a+b| \leq |a| + |b|$$

This proof will be done in two parts. First we need to prove $\lim_{x\to\ a}[f(x)+g(x)] = K+L$ Let $\epsilon > 0$ then because $\lim_{x\to\ a} f(x) = K$ and $\lim_{x\to\ a} g(x) = L$ there is a $\delta 1 > 0$ and a $\delta 2 > 0$ such that,

$$|f(x) - K < \frac{\epsilon}{2} whenever 0 < |x-a| < \delta 1$$

$$|g(x) - L < \frac{\epsilon}{2} whenever 0 < |x-a| < \delta 2$$

Now choose $\delta = \min(\delta 1, \delta 2)$. We have to now show that,

$$|f(x) + g(x) - (K-L)| < \epsilon whenever 0 < |x-a| < \delta$$

Now we assume that 0 < —x-a— < δ. We can then have,

$$|f(x) + g(x) - (K+L) = |(f(x) - K) + (g(x) - L)|$$

$$\geq |f(x) - k| + |g(x) - L|$$

by the triangle inequality

$$< \frac{\epsilon}{2} + \frac{\epsilon}{2}$$
$$= \epsilon$$

In the next step we used our choice of δ that we also have 0 < x-a < $\delta 1$ and 0 < x-a < $\delta 2$ and so we can use the initial statements in our proof. Next, we prove that $\lim_{x\to\ a}[f(x)-g(x)] = K-L$. The sum above could also be used for the sum of two functions. But we have already proven this so we can now take advantage of what we have proven in proof one.

$$\lim_{x\to\ a}[f(x) - g(x)] = \lim_{x\to\ a}[f(x) + (-1)g(x)]$$

$$= \lim_{x\to\ a} f(x) + \lim_{x\to\ a}(-1)g(x)$$

by the first part of proof 2

$$\lim_{x\to\ a} f(x) + (-1)\lim_{x\to\ a} g(x)$$

by proof 1

$$K + (-1)L$$
$$K - L$$

3.3.1 Example

For example subbing in 10 for x

$$\lim_{x\to\ 5} f(10) = 15, \lim_{x\to\ a} g(10) = 18$$

$$f(10) - 15 < \frac{\epsilon}{2}, 0 < 10 - 5 < \delta 1$$

$$g(10) - 15 < \frac{\epsilon}{2}, 0 < 10 - 5 < \delta 2$$

$$f(10) + g(10) - (15 + 18) < \epsilon, 0 < 10 - 5 < \delta$$

$$(f(10) - g(10)) + (g(10) - 18)$$

$$\leq f(10) - 15 + g(10) - 18$$

$$< \frac{\epsilon}{2} + \frac{\epsilon}{2}$$

$$\epsilon$$

3.4 Proof of 3

To Prove

$$\lim_{x \to a}[f(x)g(x)] = \lim_{x \to a} f(x) \lim_{x \to a} g(x) = LM$$

First note that because $\lim_{x \to a} f(x) = K$ and $\lim_{x \to a} g(x) = L$ .We can use the properties from 2 and 5 to prove the following two properties

$\lim_{x \to a}[f(x) - K] = lim_{x \to a} f(x) - \lim_{x \to a} K = K - K = 0$
$\lim_{x \to a}[g(x) - L] = lim_{x \to a} g(x) - \lim_{x \to a} L = L - L = 0$
$Let \epsilon > 0$
From proof 1. So then we have
$\delta_1 > 0$,
$\delta_2 > 0$
Such that

$$| (f(x) - K) - 0 | < \sqrt{\epsilon} \; when \; 0 < | x - a | < \delta_1$$

and

$$| (g(x) - L) - 0 | < \sqrt{\epsilon}$$

when

$$0 < | x - a | < \delta_2$$

Choose $\delta = \min \delta_1 , \delta_2$ if $0 < | x - a | < \delta$
Then we have,

$$| [f(x) - K][g(x) - L] - 0 | = | f(x) - K | \, | g(x) - L | < \sqrt{\epsilon}\sqrt{\epsilon} = \epsilon$$

So we've proved

$$\lim_{x \to a}[f(x) - K][g(x) - L] = 0$$

This is not the final proof but is needed later on

We start by expanding

$$[f(x) - K][g(x) - L] = f(x)g(x) - Lf(x) - Kg(x) + KL$$

Rearrange the equation for f(x)g(x)

$$f(x)g(x) = [[f(x) - K][g(x) - L] + Lf(x) + Kg(x) - KL]$$

$$\lim_{x \to a} f(x)g(x) = \lim_{x \to a}[[f(x) - K][g(x) - L] + Lf(x) + Kg(x) - KL]$$

$$\lim_{x \to a} f(x)g(x) = \lim_{x \to a}[f(x) - K][g(x) - L] + \lim_{x \to a} Lf(x) + \lim_{x \to a} Kg(x) - \lim_{x \to a} KL$$

As proved earlier

$$\lim_{x \to a} f(x)g(x) = \lim_{x \to a}[f(x)K][g(x) - L] = 0$$

So

$$\lim_{x \to a} f(x)g(x) = 0 + \lim_{x \to a} Lf(x) + \lim_{x \to a} Kg(x) - \lim_{x \to a} KL$$

$$\lim_{x \to a} f(x)g(x) = LK + KL - KL$$

$$\lim_{x \to a} f(x)g(x) == LK$$

3.4.1 Example

For example we'll say the
$\lim_{x \to 2}$
and we have
$f(x) = (x^2 + 3x)$ and $g(x) = (5x^2 - 7x)$
So to prove,
$\lim_{x \to 2}[(x^2 + 3x)(5x^2 - 7)] = \lim_{x \to 2}(x^2 + 3x) lim_{x \to 2}(5x^2 - 7x) = KL$
From proof
$\lim_{x \to 2}(x^2 + 3x) = 10 = K$
$\lim_{x \to 2}(5x^2 - 7x) = 6 = L$

We expand
$[(x^2 + 3x) - 10][(5x^2 - 7x) - 6] = (x^2 + 3x)(5x^2 - 7x) - 6(x^2 + 3x) - 10(5x^2 - 7x) + (6)(10)$
Then rearrange
$(x^2 + 3x)(5x^2 - 7x) = [[(x^2 + 3x) - 10][(5x^2 - 7x) - 6] + 6(x^2 + 3x) + 10(5x^2 - 7x) - (6)(10)]$

$\lim_{x \to 2}(x^2 + 3x)(5x^2 - 7x) = \lim_{x\ to\ 2}[[(x^2 + 3x) - 10][(5x^2 - 7x) - 6] + 6(x^2 + 3x) + 10(5x^2 - 7x) - (6)(10)]$

$\lim_{x\to\ 2}(x^2+3x)(5x^2-7x) = \lim_{x\ to\ 2}[[(x^2+3x)-10][(5x^2-7x)-6] + \lim_{x\to\ 2} 6(x^2+3x) + \lim_{x\to\ 2} 10(5x^2-7x) - \lim_{x\to\ 2}(6)(10)]$

From proof we know $\lim_{x\ to\ 2}[[(x^2+3x)-10][(5x^2-7x)-6]$ goes to zero.

$\lim_{x\to\ 2}(x^2+3x)(5x^2-7x) = 0 + \lim_{x\to\ 2} 6(x^2+3x) + \lim_{x\to\ 2} 10(5x^2-7x) - \lim_{x\to\ 2}(6)(10)]$

$\lim_{x\to\ 2}(x^2+3x)(5x^2-7x) = 60 + 60 - 60$

$\lim_{x\to\ 2}(2^2+3(2))(5(2)^2-7(2)) = 0 + \lim_{x\to\ 2} 6(2^2+3(5)) + \lim_{x\to\ 2} 10(5(2)^2-7(2)) - \lim_{x\to\ 2}(6)(10)]$

$60 = 60 + 60 - 60$
$60 = 60$

3.5 Proof of 4

We're going to prove Property 4 for n (an integer exponent) To prove:

$$\lim_{x\to a}[f(x)]^n = [\lim_{x\to a} f(x)]^n = K^n \; n \geq 2, \; n \in i$$

For n=2 we have nothing more than special case of property 3

$$\lim_{x\to a}[f(x)]^2 = \lim_{x\to a} f(x)f(x) = \lim_{x\to a} f(x) \lim_{x\to a} f(x) = KK = K^2$$

(In this line we multiply the limit by itsself "expanding" the limit which will give us (K)(K))

So 5 is true for n=2. Now assume 5 is true for n-1 or

$$\lim_{x\to a}[f(x)]^n = \lim_{x\to a}(([f(x)]^(n-1))(f(x)))$$

(Now we prove that it is the same for any value of n)

3.5.1 Example

Let

$$f(x) = 3x + 5$$

Let

$$n = 3$$

Let

$$\lim_{x\to 1}$$

As

$$\lim_{x\to 1}[f(x)]^3 = \lim_{x\to 1} f(x)f(x)f(x)$$

=

$$\lim_{x\to 1}[3x+5]^3 = \lim_{x\to 1}(3x+5)(3x+5)(3x+5)$$

=

$$(\lim_{x\to 1}(3x+5))(\lim_{x\to 1}(3x+5))(\lim_{x\to 1}(3x+5))$$

=

$$(8)(8)(8) = 8^3 = 512$$

As

$$\lim_{x\to 1}[f(x)]^3 = \lim_{x\to 1}[f(x)]^2 f(x)$$

=

$$\lim_{x\to 1}[3x+5]^3 = \lim_{x\to 1}(3x+5)^2(3x+5)$$

=

$$\lim_{x\to 1}[3x+5]^3 = \lim_{x\to 1}(3x+5)^2 + \lim_{x\to 1}(3x+5)$$

=

$$(8^2)(8)$$

=

$$8^3 = 512$$

4 Refrences

http://www.milefoot.com/math/calculus/limits/GenericLimitLawProofs04.htm
https://math.libretexts.org/Bookshelves/Calculus/Book
https://tutorial.math.lamar.edu/classes/calci/limitproofs.aspx
http://www.milefoot.com/math/calculus/limits/DeltaEpsilonProofs03.htm

Limits Project

Caimin Keavney, Elson Ling, Jack Kelly, Joshua McGowan

Workshop Tutor: Donal O'Regan
30/10/2020

1 Project

Project: Discuss the $\epsilon - \delta$ definition for $\lim_{x \to a} f(x)$ and use the definition to prove that if $\lim_{x \to a} f(x) = L$ and $L \neq 0$ then $\lim_{x \to a} \frac{1}{f(x)} = \frac{1}{L}$

Include some examples of the property.

2 The Cauchy Definition for Limit

The number L is called the limit of the function f(x) as $x \to a$, if and only if for every $\epsilon > 0$ there exists $\delta > 0$ such that $|f(x) - L| < 0$

Whenever

$0 < |x - a| < \delta$

This is also known as the Cauchy definition for limit.

3 Alternative Definition for Limit

In simpler terms, as f(x) gets closer and closer to a specific value L as x approaches a from the right, then we can say that the limit of f(x) as x approaches a from the right is L.

Similarly, if f(x) gets closer and closer to a specific value L as x approaches a from the left, then we can say that the limit of f(x)as x approaches a from the left is L.

If the limit of f(x) as x approaches a is the same from both the right and left, then we can say that the limit of f(x) as x approaches a is L.

Otherwise (if the limit of f(x) as x approaches a doesn't approach a specific value from the right and left), we say the limit doesn't exist.

4 Proof of Property

For every $\epsilon > 0$ there exists $\delta > 0$ such that for all x,

$|x - a| > \delta$ implies that $|f(x) - L| < \epsilon$

We say $\lim_{x \to a} f(x) = L$

Because $\lim_{x \to a} f(x) = L$ there is a delta, $\delta_1 > 0$ such that

$|f(x) - L| < \frac{|L|}{2}$ whenever $0 < |x - 2| < \delta_1$

Assuming $0 < |x - a| < \delta_1$, we have

$|L| = |L - f(x) + f(x)|$ adding zero to L(f(x)-f(x)=0)
$\leq |L - f(x)| + |f(x)|$
$= |f(x) - L| + |f(x)|$
$< \frac{|L|}{2} + |f(x)|$ assuming that $0 < |x - a| < \delta_1$

Rearranging this gives
$|L| \leq \frac{|L|}{2} + |f(x)| \rightarrow \frac{|L|}{2} < |f(x)| \rightarrow \frac{1}{f(x)} < \frac{2}{|L|}$

Now, there is also a $\delta_2 < 0$ such that,
$|f(x) - L| < \frac{|L|^2}{2}\epsilon$ whenever $0 < |x - 2| < \delta_2$

Choose $\delta = min[\delta_1, \delta_2]$. If $0 < |x - a| < \delta$ we have,

$|\frac{1}{f(x)} - \frac{1}{|L|}| = |\frac{L - f(x)}{Lf(x)}|$ put in single fraction

$= \frac{1}{|Lf(x)|}|L - f(x)|$ rearranging

$= \frac{1}{|L|} * \frac{1}{|f(x)|} * |f(x) - L|$

$< \frac{1}{|L|} * \frac{2}{|L|} * |f(x) - L|$

$< \frac{2}{|L|^2} * \frac{|L|^2}{2}\epsilon$

$= \epsilon$

Q.E.D.

5 Examples of Property

Example 1: Consider the function $f(x) = 3$ where a=5

$\lim_{x \to 5} f(x) = 3$
$\lim_{x \to 5} \frac{1}{f(x)} = \frac{1}{3}$

Example 2: Consider the function f(x)=x+5 where a=5

$\lim_{x \to 5} f(x) = (5) + 5 = 10$
$\lim_{x \to 5} \frac{1}{f(x)} = \frac{1}{(5)+5} = \frac{1}{10}$

Example 3: Consider the function $f(x) = x^2 + 4x - 7$ where a=5

$\lim_{x \to 5} f(x) = (5)^2 + 4(5) - 7 = 25 + 20 - 7 = 38$
$\lim_{x \to 5} \frac{1}{f(x)} = \frac{1}{(5)^2+4(5)-7} = \frac{1}{25+20-7} = \frac{1}{38}$

Example 4: Consider the function $f(x) = \frac{x^2+4x-7}{2x^2-6x+1}$ where a=5

$\lim_{x\to 5} f(x) = \frac{(5)^2+4(5)-7}{2(5)^2-6(5)+1} = \frac{25+20-7}{50-30+1} = \frac{38}{21}$

$\lim_{x\to 5} \frac{1}{f(x)} = \frac{1}{\frac{x^2+4x-7}{2x^2-6x+1}} = \frac{1}{\frac{38}{21}} = \frac{21}{38}$

An Evaluation of the Epsilon-Delta Definition of a Limit

David Murphy, Jessica Murphy, Matthew Murphy

Workshop Lecturer: Donal O'Regan, November 6th, 2020

Introduction to the Epsilon-Delta Definition of a Limit:

In calculus, the $\epsilon - \delta$ definition of a limit is an algebraically precise formulation of evaluating the limit of a function. Informally, the definition states that a limit L of a function at a point a exists no matter how a is approached, the values returned by the function will always approach L. In this project we will be discussing the following: 1. Defining the Epsilon-Delta Definition of a Limit, 2. Proving a Property of the Epsilon-Delta Definition of a Limit, 3. Analyzing Conclusions Provided from the Proven Property in Section 2.

1. Defining the Epsilon-Delta Definition of Limits:

The Formal Definition of Epsilon-Delta Limits:

Let $f(x)$ be a function defined on an open interval a ($f(a)$ need not be defined). We say that the limit of $f(x)$ as x approaches a is L i.e.,

$$\lim_{x \to a} f(x) = L$$

If for every $\epsilon > 0$ there exists $\delta > 0$ such that for all x:

$$0 < |x - a| < \delta \Rightarrow |f(x) - L| < \epsilon$$

Let's discuss this.

Informal Discussion of Epsilon-Delta definition of a limit:

What this means intitally is that, when x approaches a from either side, it is equal to L. One helpful interpretation of this definition is visually with an exchange between two parties, *Alice* and *Bob*.

Consider *Alice* gives *Bob* any distance from L i.e. ϵ, *Bob* can always specify a distance around a i.e. δ. In this example, *Alice* gives *Bob* an epsilon as close as she wants to that limit value, and *Bob* can get *Alice* as close as she wants to that limit point by giving her a range around the point in which x is approaching a. As long as *Bob* picks an x value that is within this range around a, *Alice* can guarantee that f(x) will be within the range you specify, as long as $x \neq a$.

Alice gives *Bob* any Epsilon, in a range around L, greater than 0, given

$$\epsilon > 0,$$

Bob will give a delta, which is in a range around a. As long as the distance between x and a is

(i) greater than 0

(ii) and less than δ

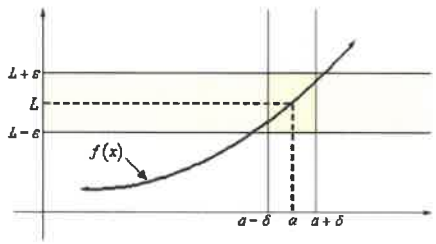
there is a guarantee that the function and the limit point L is going to be less than the number ϵ that was given.

i.e.

$$\lim_{x \to a} f(x) = L,$$

given $\epsilon > 0$

$$0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon$$



2. Proving a Property of the Epsilon-Delta definition of a Limit:

$$\lim_{x \to 4} g(x) = 2x + 5 = 13$$

$$\lim_{x \to 13} f(x) = x + 13, L = 16$$

$$|g(x) - L| < \epsilon$$

$$|(2x + 5) - 13| < \epsilon$$

$$|2x - 8| < \epsilon$$

$$|2(x - 4)| < \epsilon$$

$$|x - 4| < \epsilon/2$$

We know, from definition

$$|x - a| < \delta$$

thus,

$$|x - 4| < \delta$$

so, $\delta = \epsilon/2$

Proof:

$$\epsilon > 0$$

$$\delta = \epsilon/2,$$

as shown above. Since,

$$\epsilon > 0, \delta > 0,$$

For every x, $0 < |x - a| < \delta$,

$$x - 4 < \epsilon/2$$

$$(2x - 8) - 13 < \epsilon$$

Therefore,

$$\lim_{x \to 4} 2x + 5 = 13$$

Similarly,

$$|f(x) - L| < \epsilon$$

$$|x + 3 - 16| < \epsilon$$

$$|x - 13| < \epsilon$$

We know from definition,

$$|x - a| < \delta$$

$$|x - 13| < \delta$$

Thus,

$$\delta = \epsilon$$

Proof:

$$\epsilon > 0$$

$$\delta = \epsilon,$$

as shown above.

Thus,

$$\delta > 0$$

Now for every x, $0 < |x - a| < \delta$,

$$|x - 13| < \delta$$

$$|x - 13| < \epsilon$$

$$|(x + 3) - 16| < \epsilon$$

Therefore,

$$\lim_{x \to 13}(x + 3) = 16$$

Using the above proofs,

$$\lim_{x \to 4} f(g(x))(2x + 5) + 3 = 16$$

$$|f(g(x)) - L|$$

$$|((2x + 5 + 3) - 16| < \epsilon$$

$$|(2x + 8) - 16| < \epsilon$$

$$|2x - 8| < \epsilon$$

$$|2(x - 4)| < \epsilon$$

$$|x - 4| < \epsilon/2$$

From definition

$$|x - a| < \delta$$

$$|x - 4| < \delta$$

$$\delta = \epsilon/2$$

Proof:

$$\epsilon > 0$$

$$\delta = \epsilon/2,$$

as shown above.
Since $\epsilon > 0, \delta > 0$ for every $x, 0 < |x - a| < \delta$

$$|x - 4| < \delta$$

$$|x - 4| < \epsilon/2$$

$$|2x - 8| < \epsilon$$

$$|((2x + 5) + 3) - 16| < \epsilon$$

Therefore,

$$\lim_{x \to 4}(2x + 5) + 3 = 16$$

Thus, when

$$\lim_{x \to a} g(x) = L, \lim_{x \to L} f(x) = f(L)$$

3. Analyzing Conclusions Provided from the Proven Property in Section 2:

This final part of the project will serve to demonstrate how the property above can be utilized in a given example, assuming all conditions are met, to draw certain conclusions.

Given the functions $g(x) = x^2$ and $f(x) = x$, one can determine:

$$\lim_{x \to 2} f(g(x)) = f(4)$$

We know this because,

$$\lim_{x \to 2} g(x) = 4$$

One can then evaluate the limit of f(x) as it approaches this value 4, considered now as L, to find that

$$\lim_{x \to 4} f(x) = 4$$

and also find $f(4) = 4$, showing that

$$\lim_{x \to 4} f(x) = f(L)$$

Therefore,

$$\lim_{x \to 2} f(g(x)) = 4$$

$$f(\lim_{x \to 2} g(x)) = 4$$

$$4 = f(4)$$

Q.E.D

The property above is possible to be used because both $g(x) = x^2$ and $f(x) = x$ are defined at all points. In a situation where the limit of $f(x)$ at a point differs from the value of the function, one can conclude the property becomes unusable, due to all conditions not being met.

Given the functions $g(x) = x^2$ and $f(x)$, where $f(x) =$

$$\begin{cases} x, & x > 4 \\ 3, & x = 4 \\ x, & x < 4 \end{cases}$$

one cannot determine that

$$\lim_{x \to 2} f(g(x)) = f(4)$$

We know this because,

$$\lim_{x \to 2} g(x) = 4$$

However, when one then evaluates this value L for

$$\lim_{x \to 4} f(x)$$

the limit value is 4, while $f(4) = 3$ as defined by the piecewise function.

Therefore,

$$\lim_{x \to 4} f(x) \neq f(4),$$

and the property's conditions are no longer met.

Q.E.D

Honours Maths Project 1

Adam Mullins, Michael McNally, Lochlann Morcom, Liam Moran, Diarmaid Munroe
-Tutor: Donal O'Regan

November 6, 2020

• Question

Discuss the epsilon-delta definition

For:

$$\lim_{x \to a} f(x) \textit{ and prove using the definition}$$

That:

$$\lim_{x \to a} \left(\frac{f(x)}{g(x)} \right) = \left(\frac{\lim_{x \to a} f(x)}{\lim_{x \to a} g(x)} \right)$$

Finally, constant examples that display the above property.

• Introduction

The epsilon - delta definition for

$$\lim_{x \to a} f(x) = L \textit{ States that,}$$

Given:

$$\epsilon > 0, \textit{ there exists a } \delta > 0$$

Such that if:

$$(0 < |x - a|) < \delta$$

Then:

$$|f(x) - L| < \epsilon$$

This definition also applies to:

$$\lim_{x \to a} g(x) = M$$

If, for an epsilon, there exists a delta that renders the above statement true, then the limit is correct.

- **Proof**

Given that:

$$\lim_{x \to a} f(x) = L$$

$$\lim_{x \to a} g(x) = M, \textit{ and } M \neq 0 \textit{ then,}$$

using the epsilon - delta definition, for any $\epsilon > 0$, *There exists a* $\delta > 0$, *such that if* :

$$(0 < |x - a| < \delta), \textit{ Then } |\frac{f(x)}{g(x)} - \frac{L}{M}| < \epsilon.$$

Given that:

$$\lim_{x \to a} g(x) = M \textit{ and that } M \neq 0$$

Then:

$$\lim_{x \to a} \frac{1}{g(x)} = \frac{1}{M}$$

We will use this, in combination with the Product Law of Limits, to prove the Quotient Law of Limits.

If

$$\lim_{x \to a} g(x) = M$$

then:

$$|g(x)| \to M \textit{ as } x \to a.$$

Since:

$$M > 0 \textit{ and } M \neq 0,$$

We can say that:

$$\frac{|M|}{2} < |M|.$$

Then, also:

$$\frac{|M|}{2} \leq |g(x)|.$$

$$\lim_{x \to a} g(x) = M.$$

Then, for any:

$$\epsilon > 0, \textit{ there exists a } \delta > 0 \textit{ such that if}$$

$$(0 < |x - a| < \delta), \textit{ then } |g(x) - M| < \epsilon.$$

$$\textit{Let } \epsilon = \epsilon\, |M| \frac{|m|}{2}.$$

Then, as in the above definition

$$|g(x) - M| < \epsilon |M| \frac{|M|}{2} \textit{ for } 0 < |x - a| < \delta.$$

Also,

$$|M - g(x)| < \epsilon |M| \frac{|M|}{2} \textit{ for } 0 < |x - a| < \delta$$

(because absolute value expressions are commutative).

$$\textit{So, for any } \epsilon > 0, \textit{ there exists a } \delta > 0$$

such that

$$|M - g(x)| < \epsilon\, |M| \frac{|M|}{2} \textit{ for } 0 < |x - a| < \delta$$

AND

$$\frac{|M|}{2} \leq |g(x)| \textit{ for } 0 < |x - a| < \delta.$$

So, take:

$$\left|\frac{1}{g(x)} - \frac{1}{M}\right|$$

$$= \left|\frac{M - g(x)}{M \cdot g(x)}\right| \textit{ (subtraction)}$$

$$= \frac{|M - g(x)|}{|M||g(x)|}$$

(the absolute value of a product is equal to the product of the absolute values)

$$Then,\ for\ any\ \epsilon > 0,\ there\ exists\ a\ \delta > 0$$

such that

$$\frac{|M|}{2} \leq |g(x)|\ for\ 0 < |x - a| < \delta.$$

Therefore

$$\frac{1}{g(x)} \leq \frac{1}{\frac{|M|}{2}}\ for\ 0 < |x - a| < \delta.$$

Therefore

$$|\frac{1}{g(x)} - \frac{1}{m}|$$

$$= \frac{|M - g(x)|}{|M||g(x)|} \leq \frac{|M - g(x)|}{|M|\frac{|M|}{2}}\ for\ 0 < |x - a| < \delta.$$

$$So,\ for\ any\ \ \epsilon > 0, there\ exists\ a\delta > 0$$

such that:

$$|\frac{1}{g(x)} - \frac{1}{m}| \leq \frac{|M - g(x)|}{|M|\frac{|M|}{2}}\ for\ 0 < |x - a| < \delta.$$

But, we found earlier that

$$|M - g(x)| < \epsilon|M|\frac{|M|}{2}\ for\ 0 < |x - a| < \delta.$$

Therefore

$$|\frac{1}{g(x)} - \frac{1}{m}| \leq \frac{|M - g(x)|}{|M|\frac{|M|}{2}} < \frac{\epsilon|M|\frac{|M|}{2}}{|M|\frac{|M|}{2}}$$

$$for\ 0 < |x \to a| < \delta.$$

Then, we can say that,

$$for\ any\ \epsilon > 0,\ there\ exists\ a\ \delta\ > 0\ such\ that$$

$$|\frac{1}{g(x)} - \frac{1}{M}| < \epsilon\ for\ 0 < |x \to a| < \delta$$

Therefore

$$\lim_{x \to a} \frac{1}{g(x)} = \frac{1}{M}$$

So, given that

$$\lim_{x \to a} f(x) = L\ and\ \lim_{x \to a} g(x) = M\ \ and\ M \neq 0,$$

using the Products Law of Limits:

$$\lim_{x \to a} \left(\frac{f(x)}{g(x)} \right) = \lim_{x \to a} \left(f(x) \cdot \left(\frac{1}{g(x)} \right) \right)$$

$$= L \cdot \frac{1}{M} = \frac{L}{M}$$

Therefore

$$\lim_{x \to a} \frac{f(x)}{g(x)} = \frac{\lim_{x \to a} f(x)}{\lim_{x \to a} g(x)}$$

$$QED$$

- **Examples**

Ex (1)

$$\lim_{x\to 4} \frac{x-1}{x^2-5x+6} = \frac{3}{2}$$
$$\frac{\lim_{x\to 4}(x-1)}{\lim_{x\to 4}(x^-5x+6)} = \frac{3}{2}$$

Therefore,

$$\lim_{x\to 4}\left(\frac{x-1}{x^2-5x+6}\right) = \frac{\lim_{x\to 4}(x-1)}{\lim_{x\to 4}(x^2-5x+6)}$$

Ex (2)

$$\lim_{x\to 3}\left(\frac{x}{x-2}\right) = 3$$
$$\frac{\lim_{x\to 3}(x)}{\lim_{x\to 3}(x-2)} = 3$$

Therefore,

$$\lim_{x\to 3}\left(\frac{x}{x-2}\right) = \frac{\lim_{x\to 3}(x)}{\lim_{x\to 3}(x-2)}$$

Ex (3)

$$\lim_{x\to 1}\left(\frac{cos\ x}{sin\ x}\right) = 57.23$$
$$\frac{\lim_{x\to 1}(cos\ x)}{\lim_{x\to 1}(sin\ x)} = 57.23$$

Therefore

$$\lim_{x\to 1}\left(\frac{cos\ x}{sin\ x}\right) = \frac{\lim_{x\to 1}(cos\ x)}{\lim_{x\to 1}(sin\ x)}$$

Ex (4)

$$\lim_{x\to 2}\left(\frac{x^2-5x+7}{x^2+7x-3}\right) = \frac{1}{15}$$
$$\frac{\lim_{x\to 2}(x^2-5x+7)}{\lim_{x\to 2}(x^2+7x-3)} = \frac{1}{15}$$

Therefore,

$$\lim_{x\to 2}\left(\frac{x^2-5x+7}{x^2+7x-3}\right) = \frac{\lim_{x\to 2}(x^2-5x+7)}{\lim_{x\to 2}(x^2+7x-3)}$$

Ex (5)

$$\lim_{x \to 1.5} \left(\frac{2x}{4x} \right) = \frac{3}{6} = \frac{1}{2}$$

$$\frac{\lim_{x \to 1.5}(2x)}{\lim_{x \to 1.5}(4x)} = \frac{3}{6} = \frac{1}{2}$$

Therefore,

$$\lim_{x \to 1.5} \left(\frac{2x}{4x} \right) = \frac{\lim_{x \to 1.5}(2x)}{\lim_{x \to 1.5}(4x)}$$

Ciarán Campbell, Julia Kompanowska, Tony o' Hanluain, Alison o' Sullivan
Workshop Lecturer: Michael McGettrick

CiaránCampbellMaths1stGroupProject

Ciarán Campbell

November 2020

1 Introduction

x = C O M P U T I N G ,f(x) = space X F 5 D 4 G O Z mod 37
A=10, B=11,..., Z=35, space=36
G $\rightarrow$ $Z, 16$ $\rightarrow$ 35
N $\rightarrow$ $O, 23$ $\rightarrow$ 24
16 α + β = 35
23α + β = 24
$-7\alpha \equiv 11$, $\alpha \equiv (-11)(7)^{-}1$
$7^{-}1 \equiv 16 \mod 37$, $\alpha \equiv -11 * 16 \equiv -176 \equiv 9 \mod 37$
$\beta \rightarrow 2$
f(x) $\rightarrow 9x + 2$

2 Question 1

Calculate f(lF) and f(lL) where f(lF) is first letter of name and f(lL) is last letter of first name
$f(lF) \rightarrow f(C) \rightarrow f(12)$, $f(lL) \rightarrow f(N) \rightarrow f(23)$
$12 * 9 + 2 \rightarrow 110 \equiv 36 \mod 37 \rightarrow space$
12*23+2 $\rightarrow$ 278 $\equiv$ 19 mod 37 $\rightarrow$ J
$F(C) \rightarrow space, F(N) \rightarrow J$

3 Question 2

Calculate the sum of lF and lL for each member in group. Find f(x) of that value.
Ciarán $\rightarrow C + N, Julia \rightarrow J + A, Tony \rightarrow T + Y, Alison \rightarrow A + N$
C+N+J+A+T+Y+A+N $\equiv 12 + 23 + 19 + 10 + 29 + 34 + 10 + 23 \equiv 110 \equiv 36$ mod 37, 36 $\rightarrow$ *space*

4 Question 3

g(x) is inverse of f(x), calculate g(sum of lL for all members)
sum of lL $\equiv$ 23 + 10 + 34 + 23 $\equiv$ 16 mod 37, find g(16)

g(x)		$\rightarrow$(x-2)/9$\equiv$(x-2)$9^{-}1$
$9^{-}1$	$\equiv$	$33 mod 37$
$g(x)$		$\rightarrow$33(x-2)$\equiv$33x-66$\equiv$33x+8

$g(16) \rightarrow 33(16)+8 \equiv 18 \bmod 37$, $18 \rightarrow I$

Workshop 5

Orla Conlon, Daniel Haines, Charlie O'Connor, Angie Scully
Tutor: Michael Mc Gettrick

October 2020

1 Question 1

Each person in your group should calculate $f(l_F)$ and $f(l_L)$ where l_F is the First letter of your first name and l_L is the Last letter of your first name.

First Names: $f(x) = (9x + 2)$ **mod** 37

1. Orla Conlon:
$$f(l_F) = (9 \times 24) + 2 \equiv 33 \bmod 37$$
2. Daniel Haines:
$$f(l_F) = (9 \times 13) + 2 \equiv 8 \bmod 37$$
3. Charlie O'Connor:
$$f(l_F) = (9 \times 12) + 2 \equiv 36 \bmod 37$$
4. Angie Scully:
$$f(l_F) = (9 \times 10) + 2 \equiv 18 \bmod 37$$

Last Names:

1. Orla Conlon:
$$f(l_L) = (9 \times 12) + 2 \equiv 36 \bmod 37$$
2. Daniel Haines:
$$f(l_L) = (9 \times 17) + 2 \equiv 7 \bmod 37$$
3. Charlie O'Connor:
$$f(l_L) = (9 \times 24) + 2 \equiv 33 \bmod 37$$
4. Angie Scully:
$$f(l_L) = (9 \times 28) + 2 \equiv 32 \bmod 37$$

2 Question 2

If there are n people in your group, and l_1F is the first letter in the first name of the first person, l_2F is the first letter in the first name of the second person, etc, calculate:

$$f(\sum_{i=1}^{n}(l_iF + L_iF))$$

where the letters are added modulo 37, as in the sample OKUSON question
Answer:

$$(\sum_{i=1}^{4}(l_iF + L_iF)) \equiv 18 \textbf{ mod } 37$$

$$f(x) = (9 \times x) + 2$$

$$f(18) = (9 \times 18) + 2 \equiv 16 \textbf{ mod } 37$$

This evaluates to the letter G

3 Question 3

Calculate

$$g(\sum_{i=1}^{n}(l_iL))$$

where g is the inverse function to f (i.e.$g(f(x)) = x$)
Answer:

$$(\sum_{i=1}^{4}(l_iL)) = 34$$

$$g(x) = (33 \times x + 8)$$

$$g(34) = (33 \times 34) + 8 \equiv 20 \textbf{ mod } 37$$

This evaluates to the letter K

Maths Project Group 3

Rían deBairéad, Mark Tobin, Emily Hayes and Eoghan Tinney

October - November 2020

Question 1

Each person in your group should calculate $f(l_F)$ and $f(l_L)$ where l_F is the **F**irst letter of your first name and l_L is the **L**ast letter of your first name.

$$f : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, x \mapsto \alpha x + \beta$$

To Calculate

First and last letters of our first names

$$\begin{array}{ll} R \mapsto ? & N \mapsto ? \\ M \mapsto ? & K \mapsto ? \\ E \mapsto ? & Y \mapsto ? \\ E \mapsto ? & N \mapsto ? \end{array}$$

Given
_XF5D4GOZ $\mapsto$ COMPUTING

Solution 1

$$G \mapsto G\alpha + \beta = Z$$
$$N \mapsto N\alpha + \beta = O$$

$$\text{Where :} \quad G = 16, \quad Z = 35, \quad N = 23, \quad O = 24$$

Calculating β

$$16\alpha + \beta = 35$$
$$\underline{23\alpha + \beta = 24}$$

$$368\alpha + 23\beta = 805$$
$$\underline{-368\alpha - 16\beta = -384}$$

$$7\beta = 421$$

So

$$\beta \equiv (7^{-1})(421) \mod 37$$
$$\beta \equiv (7^{-1})(14) \mod 37$$

Using the Euclidean Algorithm

$$37 = (5)(7) + 2$$
$$\underline{7 = (3)(2) + 1}$$
$$1 = 7 - (3(37 - 5(7))$$
$$1 = 16 - ((3)(37) - (2)(16))$$
$$1 = \cancel{(-3)(37)} + 7(16)$$
$$= 7(16)$$

So

$$7^{-1} \mod 37 \equiv 16 \mod 37$$
$$\beta \equiv (16)(421) \mod 37$$
$$\beta \equiv 224 \mod 37$$
$$\beta \equiv 2 \mod 37$$

Now calculating α

$$\begin{aligned}
&16\alpha + (\beta) = 35 \\
&16\alpha + (2) = 35 \\
&16\alpha = 33 \\
&\alpha = (16^{-1})(33) \mod 37
\end{aligned}$$

Using the Euclidean Algorithm

$$\begin{aligned}
&37 = (2)(16) + 5 \\
&\underline{16 = (3)(5) + 1} \\
&1 = 16 - (3)(5) \\
&1 = 16 - (3)(37 - (2)(16)) \\
&1 = (7)(16) - \cancel{(3)(37)} \\
&1 \equiv 16(7) \mod 37
\end{aligned}$$

$$\begin{aligned}
&\alpha \equiv (7)(33) \mod 37 \\
&\alpha \equiv 9
\end{aligned}$$

Therefore

$$\alpha = 9, \quad \beta = 2$$

Enciphering

Enciphering using the function $f_{(E)}$

$$\begin{gathered}
f_{(E)}(x) \equiv (x)(\alpha) + (\beta) \mod 37 \\
E = (9, 2)
\end{gathered}$$

$$
\begin{aligned}
R &= (27)(\alpha) + \beta \\
&= (27)(9) + 2 \\
&= 245 \\
&\equiv 23 \mod 37 \\
R &\mapsto N
\end{aligned} \tag{1}
$$

$$
\begin{aligned}
N &= (23)(\alpha) + \beta \\
&= (23)(9) + 2 \\
&= 209 \\
&\equiv 24 \mod 37 \\
N &\mapsto O
\end{aligned} \tag{2}
$$

$$
\begin{aligned}
M &= (22)(\alpha) + \beta \\
&= (22)(9) + 2 \\
&= 200 \\
&\equiv 15 \mod 37 \\
M &\mapsto F
\end{aligned} \tag{3}
$$

$$
\begin{aligned}
K &= (20)(\alpha) + \beta \\
&= (20)(9) + 2 \\
&= 182 \\
&\equiv 15 \mod 37 \\
K &\mapsto Y
\end{aligned} \tag{4}
$$

$$
\begin{aligned}
E &= (14)(\alpha) + \beta \\
&= (14)(9) + 2 \\
&= 128 \\
&\equiv 17 \mod 37 \\
E &\mapsto H
\end{aligned} \tag{5}
$$

$$
\begin{aligned}
Y &= (34)(\alpha) + \beta \\
&= (34)(9) + 2 \\
&= 308 \\
&\equiv 12 \mod 37 \\
Y &\mapsto C
\end{aligned} \tag{6}
$$

$$
\begin{aligned}
E &= (14)(\alpha) + \beta \\
&= (14)(9) + 2 \\
&= 128 \\
&\equiv 17 \mod 37 \\
E &\mapsto H
\end{aligned} \tag{7}
$$

$$
\begin{aligned}
N &= (23)(\alpha) + \beta \\
&= (23)(9) + 2 \\
&= 209 \\
&\equiv 24 \mod 37 \\
N &\mapsto O
\end{aligned} \tag{8}
$$

Enciphered first and last letters of our first names

$$
\begin{aligned}
R &\mapsto N \ (1) & \qquad E &\mapsto H \ (5) \\
N &\mapsto O \ (2) & \qquad Y &\mapsto C \ (6) \\
M &\mapsto F \ (3) & \qquad E &\mapsto H \ (7) \\
K &\mapsto Y \ (4) & \qquad N &\mapsto O \ (8)
\end{aligned}
$$

Question 2

"If there are n people in your group, and l_{1F} is the first letter in the first name of the first person, l_{2F} is the first letter in the first name of the second person, etc, calculate

$$f(\sum_{i=1}^{n}(l_{iF} + l_{iL})$$

where the letters are added modulo 37."

Solution 2

$$\begin{aligned} f(\sum_{i=1}^{n}(l_{iF} + l_{iL}) &= f(\sum_{i=1}^{4}((M+K)+(R+N)+(E+Y)+(E+N)) \\ &= (22 \mod 37) + (20 \mod 37) + (27 \mod 37) + (23 \mod 37) \\ &+ (14 \mod 37) + (34 \mod 37) + (14 \mod 37) + (23 \mod 37) \\ &= (5 \mod 37) + (13 \mod 37) + (11 \mod 37) + (0 \mod 37) \\ &\equiv 29 \mod 37 \end{aligned}$$

$$\begin{aligned} & f(29 \mod 37) \\ &= (29)(9) + 2 \\ &\equiv 4 \mod 37 \\ &= 4 \end{aligned}$$

Question 3

" Calculate

$$g(\sum_{i=1}^{n}(l_{iL})$$

where g is the inverse function to f (i.e. $g(f(x)) = x$)."

Solution 3

$$g(\sum_{i=1}^{n}(l_{iL}) = (f_{(E)})^{-1}$$

$$f_{(E)})^{-1} \equiv 9^{-1}(y-2) \mod 37$$

Calculate

$$9^{-1} \mod 37$$

$$\begin{aligned}
&\underline{37 = 4(9) + 1} \\
&1 = 37 - 4(9) \\
&= -4 \\
&\equiv 33 \mod 37 \\
&\therefore y \mapsto 9^{-1} \\
&(y-2) \mod 37 = 33(y-2) \\
&= 33y + 8 \\
&D = (33, 8)
\end{aligned}$$

Now using the summation;

$$g(\sum_{i=1}^{n}(l_{iL})$$

$$g(\sum_{i=1}^{4}(K+N+Y+N)$$

$$g(\sum_{i=1}^{4}(20+23+34+23)$$

$$\begin{aligned}
&= 100 \\
&= 26 \mod 37 \\
&26 \mapsto 33(26) + 8 \\
&= 866 \\
&= 15 \mod 37 \\
&\equiv F
\end{aligned}$$

Group Project 1

Luke McManus Doyle, Robin Pfeiffer, Erica Madden, Danielle Flannery

October 2020

Tutor: Dr M. Mc Gettrick

Question

The following cipher text was produced using an affine enciphering function

$$f : Z_{37} \rightarrow Z_{37}, x \rightarrow \alpha x + \beta$$

on single letter message units over the 37-letter alphabet

0,1,2,...9,A=10,B=11,...Z=35,-=36

where the underscore represents a blank
COMPUTING in the plaintext corresponds to _XF5D4GOZ in the cyphertext

1 Calculating the Enciphering Key

$$f(n) \longmapsto \alpha * n + \beta$$

$$f(G) = Z \longmapsto \alpha * 16 + \beta = 35 \tag{1}$$

$$f(N) = O \longmapsto \alpha * 23 + \beta = 24 \tag{2}$$

From equations (1) and (2) we solve for α and β

$$23 * \alpha + \beta = 24 \tag{3}$$

$$-16 * \alpha - \beta = -35 \tag{4}$$

equations (3) + (4) give : $7 * \alpha = -11 \Rightarrow 7 * \alpha = 26 \pmod{37}$

$$\alpha = 26 * 7^{-}1 = 26 * 16 = 9 \tag{5}$$

$$\beta = 24 - 23 * \alpha = 24 - 23 * 9 = 2 \tag{6}$$

Therefore, $\underline{E_k = (9, 2)}$

2 Calculating the Deciphering Key

$$f(E) = x \mapsto x * \alpha + \beta$$

Therefore,

$$f(D) = x \mapsto \frac{x - \beta}{\alpha}$$

from the enciphering key we get

$$f(D) = x \mapsto \frac{x - 2}{9} = 9^{-1}(x - 2)$$

$$9^{-1} \pmod{37} \equiv 33$$

$$f(D) = 33(x - 2) \equiv 33(x + 35) \pmod{37}$$

$$f(D) = x \mapsto 33x + 8 \mod 37$$

Therefore, $\underline{D_K = (33, 8)}$

Question 1

Each person in your group should calculate $f(l_F)$ and $f(l_L)$ where l_F is the first letter of your first name and l_L is the last letter of your first name

Erica Madden:

$$f(E) \mapsto f(14) = 9 * 14 + 2 \equiv 17 \pmod{37} = H$$
$$f(A) \mapsto f(10) = 9 * 10 + 2 \equiv 18 \pmod{37} = I$$

Danielle Flannery:

$$f(D) \mapsto f(13) = 9 * 13 + 2 \equiv 8 \pmod{37} = 8$$
$$f(E) \mapsto f(14) = 9 * 14 + 2 \equiv 17 \pmod{37} = H$$

Luke McManus Doyle:

$$f(L) \mapsto f(21) = 9 * 21 + 2 \equiv 6 \pmod{37} = 6$$
$$f(E) \mapsto f(14) = 9 * 14 + 2 \equiv 17 \pmod{37} = H$$

Robin Pfeiffer:

$$f(R) \mapsto f(27) = 9 * 27 + 2 \equiv 23 \pmod{37} = N$$
$$f(N) \mapsto f(23) = 9 * 23 + 2 \equiv 24 \pmod{37} = O$$

Question 2

If there are n people in your group, and l_1F is the first letter in the first name of the first person, l_2F is the first letter in the first name of the second person, etc, calculate $f\left(\sum_{i=0}^{n}(l_{iF} + l_{iL})\right)$

Where the letters are added modulo 37.

$$l_{1F} + l_{1L} = 14 + 10 \equiv 24 \pmod{37} \tag{7}$$
$$l_{2F} + l_{2L} = 13 + 14 \equiv 27 \pmod{37} \tag{8}$$
$$l_{3F} + l_{3L} = 21 + 14 \equiv 35 \pmod{37} \tag{9}$$
$$l_{4F} + l_{4L} = 27 + 23 \equiv 13 \pmod{37} \tag{10}$$

$$\sum_{i=1}^{n}(l_{iF} + l_{iL}) = \text{eqn}(7) + \text{eqn}(8) + \text{eqn}(9) + \text{eqn}(10) \equiv 25 \pmod{37}$$

$$f(\sum_{i=1}^{n}(l_{iF} + l_{iL})) = f(25) = 9 * 25 + 2 = 227 \equiv \underline{5 \pmod{37}}$$

Question 3

Calculate

$$g\left(\sum_{i=1}^{n}(l_{iL})\right)$$

where g is the inverse function to f (i.e. $g(f(x)) = x$)

Last letter of each name:

Erica $\rightarrow$ A = 10
Danielle $\rightarrow$ E = 14
Luke $\rightarrow$ E = 14
Robin $\rightarrow$ N = 23

$$\sum_{i=1}^{n}(l_{iL}) = 10 + 14 + 14 + 23 = 61 \equiv 24 \pmod{37}$$

Using our deciphering function: $D_K = (33, 8)$
$33 * 24 + 8 = 800 \equiv 23 \pmod{37} = \underline{N}$

Group Project 5 Michael McGettrick

Sean Murphy, Eli Sheedy, Rian Duggan, Katherine Mannion

6th November 2020

The cipher text was produced using an affine enciphering function

$$f : x \to \alpha x + \beta \tag{1}$$

on single letter message units over a 37-letter alphabet

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A = 10, B = 11, ..., Z = 35, \_ = 36 \tag{2}$$

where the following plain text corresponds to following ciphertext
C O M P U T I N G
_ X F S D 4 G O Z
C = 12 O = 24
_ = 36 X = 33

1 Question 1

Calculate $f(l_F)$ and $f(l_L)$ where l_F is the first letter of your first name and l_L is the last letter of your first name

1.1 Enciphering function

$24\alpha + \beta \bmod 37 = 33$
$-12\alpha + \beta \bmod 37 = 36$
$12\alpha \bmod 37 = -3$
$\alpha = 9$
$9x + \beta \bmod 37 = 36$
$9(12) + \beta \bmod 37 = 36$
$\beta = 2$

1.2 Rian

$f : x \to 9x + 2 \bmod 37$
$f : x \to 9(R) + 2 \bmod 37$
$f : x \to 9(27) + 2 \bmod 37$
$f : x \to 245 \bmod 37$

$f : x \to 23 \implies N$

$f : x \to 9x + 2 \bmod 37$
$f : x \to 9(N) + 2 \bmod 37$
$f : x \to 9(23) + 2 \bmod 37$
$f : x \to 209 \bmod 37$
$f : x \to 24 \implies O$

1.3 Eli

$f : x \to 9x + 2 \bmod 37$
$f : x \to 9(E) + 2 \bmod 37$
$f : x \to 9(14) + 2 \bmod 37$
$f : x \to 128 \bmod 37$
$f : x \to 17 \implies H$

$f : x \to 9x + 2 \bmod 37$
$f : x \to 9(I) + 2 \bmod 37$
$f : x \to 9(18) + 2 \bmod 37$
$f : x \to 164 \bmod 37$
$f : x \to 16 \implies G$

1.4 Katherine

$f : x \to 9(K) + 2 \bmod 37$
$f : x \to 9(20) + 2 \bmod 37$
$f : x \to 182 \bmod 37$
$f : x \to 34 \implies Y$

$f : x \to 9(E) + 2 \bmod 37$
$f : x \to 9(14) + 2 \bmod 37$
$f : x \to 128 \bmod 37$
$f : x \to 17 \implies H$

1.5 Sean

$f : x \to 9(S) + 2 \bmod 37$
$f : x \to 9(28) + 2 \bmod 37$
$f : x \to 254 \bmod 37$
$f : x \to 32 \implies W$

$f : x \to 9(N) + 2 \bmod 37$
$f : x \to 9(23) + 2 \bmod 37$
$f : x \to 209 \bmod 37$
$f : x \to 24 \implies O$

2 Question 2

Where l_{1_F} is the first letter in the first name of the first person, l_{2_F} is the first letter in the first name of the second person, etc.

Calculate

$$f(\sum_{i=1}^{4} (l_{i_F} + l_{i_L})) \tag{3}$$

$f(\sum_{i=1}^{4} ((K+E)+(E+I)+(S+N)+(R+N)))$
$f(\sum_{i=1}^{4} ((20+14)+(14+18)+(28+23)+(27+23)))$
$f(\sum_{i=1}^{4} ((34)+(32)+(51)+(50)))$
$f(167 \bmod 37)$
$f(19)$
$f : x \to 9(19) + 2 \bmod 37$
$f : x \to 173 \bmod 37$
$f : x \to 25 \implies P$

3 Question 3

Where g is the inverse function to f

$36\alpha + \beta \bmod 37 = 12$
$-33\alpha - \beta \bmod 37 = -24$
$3\alpha \bmod 37 = -12$
$\alpha = 33$

$33x + \beta \bmod 37 = 12$
$33(36) + \beta \bmod 37 = 12$
$1188 + \beta \bmod 37 = 12$
$\beta = 8$
$g : X \to 33x + 8 \bmod 37$

Calculate

$$g(\sum_{i=1}^{4} (l_{i_L})) \tag{4}$$

$g(\sum_{i=1}^{4} (l_{i_L}))$
$g(\sum_{i=1}^{4} (E+I+N+N))$
$g(\sum_{i=1}^{4} (14+18+23+23))$
$g(78 \bmod 37)$
$g(4)$

$g : x \to 33(4) + 8 \bmod 37$
$g : x \to 33(4) + 8 \bmod 37$
$g : x \to 29 \implies T$

Workshop Project 1

Eleanor Egan, Josua Hanrahan, Sean Janson, Maciej Stec
Tutor: Michael Mc Gettrick

November 2020

1 Question

5	The following cipher text was produced using an affine enciphering function $$f: \mathbb{Z}_{37} \to \mathbb{Z}_{37}, x \mapsto \alpha x + \beta$$ on single letter message units over the 37-letter alphabet $$0,1,2,...,9,A = 10,B = 11,...,Z = 35,\_ = 36$$ where underscore represents a blank. The enciphering program (with changed enciphering key) can be downloaded from: `http://hamilton.nuigalway.ie/teachingWeb/CSalgebra/cryptosystemSingle37.c` The last nine characters of plain text are: COMPUTING Determine the **second word** of the original plain text and carefully enter it as your answer. The answer is upper/lower-case sensitive
	47HU4NIZG_UFI47HFI4G_GIOUI6IOU4DNGOZU VIWU47HUQI47HNUXQUFX8HNOU_XF5D4GOZ ———————

Figure 1: This is a question from our first Okuson Worksheet

From this we were required to:

1. Encrypt the first letters(l_F) and last letters(l_L) of our first names mod 37(according to the 37 letter alphabet shown above)
2. Find the sum of the first letters
$$\sum_{i=1}^{n}(l_{iF})$$
And the sum of the last letters
$$\sum_{i=1}^{n}(l_{iL})$$

Then use that to find

$$\sum_{i=1}^{n}(l_{iF} + l_{iL}) \pmod{37}$$

3. Finally we had to create an inverse function that could decipher

$$\sum_{i=1}^{n}(l_i L) \pmod{37}$$

2 Solution

The question gives us the enciphering function $y = \alpha x + \beta$ The question tells us that an input of C(12) outputs Underscore(36)
We also know that an input of O(24) gives us an output of X(33)

2.1 Solving the Simultaneous Equations

$$12\alpha + \beta = 36$$
$$24\alpha + \beta = 33$$

$$+24\alpha + \beta = +33$$
$$-12\alpha - \beta = -36$$

$$12\alpha = -3$$
$$\alpha = 12^{-1} * -3 \pmod{37}$$

Using the Euclidean Algorithm
$$\alpha = 34 * -3 \pmod{37}$$
$$\alpha = 9$$

Subbing in let's you workout that
$$\beta = 2 \pmod{37}$$

Finally, we are left with the equation
$$Y = 9X + 2$$

2.2 Encrypting Letters

We are required to find the encrypted first and last letters of each of our first names.

For Example, the encrypted version of 'E'(Which corresponds to number14), would be $9 * 14 + 2 = 128$, which mod 37 is 17, which corresponds to the letter 'H'
Using this we can find out that:

- E = 17 = H
- R = 23 = N
- J = 25 = P
- A = 18 = I
- S = 32 = W
- N = 24 = O
- M = 15 = F
- J = 25 = P

This completes the first part of the question

2.3 Summation

The next part of the question asks us to find the sum of all the first and last letters of our first names.
Adding up the first letters of our first names gives

$$E + J + S + M$$
$$17 + 25 + 32 + 15 = 15 \pmod{37}$$

Adding up the last letters of our first names gives

$$R + A + N + J$$
$$23 + 18 + 24 + 25 = 16 \pmod{37}$$

Finally, if we sum those two numbers we get

$$15 + 16 = 31 \pmod{37} = V$$

This completes the second part of the question

2.4 Decryption

The last part of the question asks us to create a deciphering function which we then must use to decipher the sum of the last letters of our first name.
We can find our deciphering function by finding the inverse of our enciphering

function.
Recall that our enciphering function is

$$Y = 9X + 2$$

Inverting this gives us

$$X = (Y - 2) * 9^{-1}$$

We can use the Euclidean Algorithm again to find that the inverse of 9 mod 37 is 33.
Expanding the brackets now gives us

$$X = 33Y + 8 \pmod{(37)}$$

Finally, we can swap X and Y to give us

$$Y = 33X + 8$$

We know from earlier that the sum of the last letters from our first names is 16. We can now use our deciphering function to find out what the deciphered version of that is

$$Y = 33(16) + 8 \pmod{37}$$

$$Y = 18 \text{ Which equals I}$$

And that is the final answer to the final part of the question.

MA180 Project

Dmytro Lyubka, Megan O'Connor, Conor Kinnarney

Dr. M. Mc Gettrick

October 2020

1 Introduction

The following cipher text was produced using an affine enciphering function

$$f : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, x \mapsto \alpha x + \beta,$$

on single letter message units over the 37-letter alphabet

$$0, 1, 2, ..., 9, A - 10, B = 11, ..., Z = 35, \_ = 36,$$

where underscore represents a blank.
The last nine characters of the plain text are: COMPUTING.

```
47HU4NIZG_UFI47HFI4G_GIOUI6IOU4DNGOZUVIWU47HUQI47HNUXQUFX8HNOU_XF5D4GOZ
```

2 Evaluating the Cipher Keys

In order to proceed with the problems at hand, we must first obtain the cipher key which was used to encipher the plain text message.

We are told that a 37-letter alphabet was used to encipher the plain text message.

Alphabet Character → Integer Conversion			
0 → 0	A → 10	K → 20	U → 30
1 → 1	B → 11	L → 21	V → 31
2 → 2	C → 12	M → 22	W → 32
3 → 3	D → 13	N → 23	X → 33
4 → 4	E → 14	O → 24	Y → 34
5 → 5	F → 15	P → 25	Z → 35
6 → 6	G → 16	Q → 26	_ → 36
7 → 7	H → 17	R → 27	
8 → 8	I → 18	S → 28	
9 → 9	J → 19	T → 29	

This table can be used to efficiently convert any given alphabet character found in the plain/cipher into its corresponding integer, which will then be used in future encipher/deciphering functions.

We happen to know that the final 9 plain text characters and their corresponding cipher text characters are:

$$COMPUTING \to \_XF5D4GOZ,$$

and that an enciphering function of the form $\alpha x + \beta$ was used.

Thus, we know that $f_E(N) = O$ and $f_E(G) = Z$, or using integers in the place of letters:

$$f_E(23) \equiv 24 \mod 37 \tag{1}$$
$$23\alpha + \beta \equiv 24 \mod 37, \tag{2}$$

and

$$f_E(16) \equiv 35 \mod 37 \tag{3}$$
$$16\alpha + \beta \equiv 35 \mod 37. \tag{4}$$

We can rewrite (4) into the following:

$$\beta \equiv 35 - 16\alpha \mod 37, \tag{5}$$

and substitute this equation for β into (2).

$$23\alpha + 35 - 16\alpha \equiv 24 \mod 37 \tag{6}$$
$$7\alpha \equiv -11 \mod 37 \tag{7}$$
$$\alpha \equiv -11 \cdot 7^{-1} \mod 37. \tag{8}$$

To find 7^{-1} we use the Euclidean algorithm:

$$37 = 5 \cdot 7 + 2 \tag{9}$$
$$7 = 3 \cdot 2 + 1 \tag{10}$$

alongside Bézout's Identity

$$1 = 7 - 3 \cdot 2 \tag{11}$$
$$= 7 - 3(37 - 5 \cdot 7) \tag{12}$$
$$= 16 \cdot 7 - 3 \cdot 37, \tag{13}$$

to deduce that

$$7 \times 16 \equiv 1 \mod 37 \tag{14}$$
$$\Rightarrow 7^{-1} \equiv 16 \mod 37. \tag{15}$$

With this information, from equation (8) we find:

$$\alpha \equiv -11 \times 16 \equiv -176 \mod 37 \tag{16}$$
$$\alpha \equiv 9 \mod 37. \tag{17}$$

Now, in order to evaluate β, we use α in equation (5):

$$\beta \equiv 35 - 16\alpha \mod 37 \tag{18}$$
$$\beta \equiv 35 - 16(9) \mod 37 \tag{19}$$
$$\beta \equiv 2 \mod 37. \tag{20}$$

Following our calculations, we know that the enciphering key is $E = (9, 2)$.
The deciphering key can now be easily obtained by the following:

$$\alpha x + \beta \equiv y \mod 37 \tag{21}$$
$$x \equiv (y - \beta) \cdot \alpha^{-1} \mod 37. \tag{22}$$

Using our newfound values from the enciphering key, we get:

$$x \equiv (y - 2) \cdot 9^{-1} \mod 37 \tag{23}$$
$$x \equiv 33(y - 2) \mod 37 \tag{24}$$
$$x \equiv 33y - 66 \mod 37 \tag{25}$$
$$x \equiv 33y + 8 \mod 37. \tag{26}$$

And so, the deciphering key is $D = (33, 8)$.
For ease of access, we will manifest our obtained cipher keys into enciphering and deciphering functions of the form $\alpha x + \beta$.

$$f_E(x) : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, n \mapsto 9x + 2$$
$$f_D(x) : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, n \mapsto 33x + 8.$$

3 The Problems Themselves

3.1 Problem 1

> Each person in your group should calculate $f(l_F)$ and $f(l_L)$ where l_F is the **F**irst letter of your *first name* and l_L is the **L**ast letter of your *first name*.

Our group consists of three members - DMYTRO, MEGAN, and CONOR. We can employ our enciphering function $f_E(x)$ to the relevant characters in the first names of our group members.

D**MYTR**O

In this case, "D" and "O" will be fed into the enciphering function, or more specifically, their corresponding integers.

$$D \to 13 \tag{27}$$
$$f_E(D) \equiv 9(13) + 2 \mod 37 \tag{28}$$
$$\equiv 9 \mod 37, \tag{29}$$

$$O \to 24 \tag{30}$$
$$f_E(O) \equiv 9(24) + 2 \mod 37 \tag{31}$$
$$\equiv 33 \mod 37. \tag{32}$$

An identical process can be applied to the group's second member,

$$\underline{\boldsymbol{M}}EGA\underline{\boldsymbol{N}}$$

$$M \to 22 \tag{33}$$
$$f_E(M) \equiv 9(22) + 2 \mod 37 \tag{34}$$
$$\equiv 15 \mod 37, \tag{35}$$

$$N \to 23 \tag{36}$$
$$f_E(N) \equiv 9(23) + 2 \mod 37 \tag{37}$$
$$\equiv 24 \mod 37. \tag{38}$$

And finally to the group's third member.

$$\underline{\boldsymbol{C}}ONO\underline{\boldsymbol{R}}$$

$$C \to 12 \tag{39}$$
$$f_E(C) \equiv 9(12) + 2 \mod 37 \tag{40}$$
$$\equiv 36 \mod 37, \tag{41}$$

$$R \to 27 \tag{42}$$
$$f_E(R) \equiv 9(27) + 2 \mod 37 \tag{43}$$
$$\equiv 23 \mod 37. \tag{44}$$

Thus, we have the following table, with each column containing the required letter conversions.

DMYTRO	MEGAN	CONOR
D $\to$ 9	M $\to$ 15	C $\to$ 36
O $\to$ 33	N $\to$ 24	R $\to$ 23

3.2 Problem 2

> If there are n people in your group, and l_{1F} is the first letter in the first name of the first person, l_{2F} is the first letter in the first name of the second person, etc, calculate
>
> $$f\left(\sum_{i=1}^{n}(l_{iF}+l_{iL})\right)$$
>
> where the letters are added modulo 37, as in the sample OKUNSON question.

This next problem features a summation used as the input for the enciphering function, which we have been referring to as f_E. We will first evaluate the summation, prior to bringing it subject to f_E. Using the group member names - DMYTRO, MEGAN, and CONOR - we find that:

$$\sum_{i=1}^{n}(l_{iF}+l_{iL}) \mod 37 \tag{45}$$

$$(D+O)+(M+N)+(C+R) \mod 37 \tag{46}$$

$$(13+24)+(22+23)+(12+27) \mod 37 \tag{47}$$

$$121 \equiv 10 \mod 37. \tag{48}$$

$$\tag{49}$$

Now that we have the result of our summation, we can use it as the input for our enciphering function f_E.

$$f_E(n) : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, n \mapsto 9n+2 \tag{50}$$

$$f_E(10) \equiv 9(10)+2 \mod 37 \tag{51}$$

$$\equiv 18 \mod 37 \tag{52}$$

$$18 \to I. \tag{53}$$

Thus, our resulting evaluation is:

$$f\left(\sum_{i=1}^{n}(l_{iF}+l_{iL})\right) \equiv 18 \equiv I. \tag{54}$$

3.3 Problem 3

Calculate

$$g\left(\sum_{i=1}^{n}(l_{iL})\right) \tag{55}$$

where g is the inverse function to f (i.e. $g(f(x)) = x$).

Our final problem requires an understanding inverse functions and their properties. Put into intuitive terms, it is a function which "reverses" the process of another, returning the original input. Although not explicitly mentioned previously, we have actually already obtained the inverse of our affine enciphering function, under the concept of a "deciphering function" which reverses the process of the enciphering function, i.e. it converts the enciphered text back into plain text.

In order to make this clear, we will illustrate how our two previously obtained functions work.

$$f_E(x) : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, n \mapsto 9x + 2 \tag{56}$$
$$f_D(x) : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, n \mapsto 33x + 8. \tag{57}$$

f_E is the function which transforms the plain text message into its enciphered counterpart. Theoretically, the inverse of this function would be one which transforms the output of the enciphering function back into the original plain text message unit. i.e.

$$f_E^{-1}(f_E(x)) = x \mod 37, \tag{58}$$

or in more convenient notation:

$$f_E^{-1} \circ f_E(x) \mod 37, \tag{59}$$

where f_E^{-1} is the inverse function of f_E.
This is merely a concise, mathematically aesthetic variation of our cumbersome equation (58), meaning "use the output of $f_E(x)$ as the input for f_E^{-1}.

Now let's use our $f_E(x)$ function as the input for $f_D(x)$, and observe what our generic result will be.

$$f_D \circ f_E \mod 37 \tag{60}$$
$$\equiv f_D(9x + 2) \mod 37 \tag{61}$$
$$\equiv 33(9x + 2) + 8 \mod 37 \tag{62}$$
$$\equiv 297x + 74 \mod 37 \tag{63}$$
$$\equiv x \mod 37. \tag{64}$$

This proves that f_D the inverse of f_E, as bringing the output of $f_E(x)$ subject to f_D results in our original input x. With that observation in mind, we can proceed to solving problem 3.

Similar to how we tackled problem 2, we will first evaluate the required summation using our group member names - DMYTRO, MEGAN, and CONOR - before feeding the resulting output into our deciphering function f_D (which we established to be the inverse of the the enciphering function f_E).

$$\sum_{i=1}^{n}(l_{iL}) \equiv O + N + R \mod 37 \tag{65}$$

$$\equiv 24 + 23 + 27 \mod 37 \tag{66}$$

$$\equiv 0 \mod 37. \tag{67}$$

Now that we have the result of the given summation, we can use it as the input for our deciphering function f_D.

$$f_D(n) : \mathbb{Z}_{37} \to \mathbb{Z}_{37}, n \mapsto 33n + 8 \tag{68}$$

$$f_D(0) \equiv 33(0) + 8 \mod 37 \tag{69}$$

$$\equiv 8 \mod 37. \tag{70}$$

Thus, our final evaluation is:

$$g\left(\sum_{i=1}^{n}(l_{iL})\right) \equiv 8 \mod 37, \tag{71}$$

where $g = f_E^{-1} = f_D$.

Maths Group Project 1

Jack Reidy, Tom McGuinness, Saran O'Hora

October 2020

Question

The following cipher text was produced using an affine enciphering function

$$f : Z_{37} \to Z_{37}, x \to \alpha x + \beta$$

on single letter message units over the 37-letter alphabet:

$$0, 1, 2, ..., 9, A = 10, B = 11, ..., Z = 35, \_ = 36.$$

Where the underscore represents a blank. The enciphering program (with changed enciphering key) can be downloaded from:

http://hamilton.nuigalway.ie/teachingWeb/CSalgebra/cryptosystemSingle37.c

The last nine characters of plain text are: COMPUTING

Determine the **second word** of the original plain text and carefully enter it as your answer. The answer is upper/lower-case sensitive

47HU4NIZG_UFI47HFI4GGIOUI6IOU4DNGOZUVIWU47HUQI47HNUXQUFX8HNOU_XF5D4GOZ

1.

Each person in your group should calculate $f(l_f)$ and $f(l_L)$ where (l_F) is the First letter of your first name and (l_L) is the Last letter of your first name.

2.

If there are n people in your group, and (l_{1F}) is the first letter in the first name of the first person, (l_{2F}) is the first letter in the first name of the second person,etc, calculate

$$f(\sum_{i=1}^{n}(l_{iF} + l_{iL}))$$

where the letters are added modulo 37, as in the sample OKUSON question.

3.

Calculate

$$g(\sum_{i=1}^{n}(l_{iL}))$$

where g is the inverse function to f (i.e. g(f(x)) $\equiv x$).

Answers

$$\text{x} \rightarrow \alpha x + \beta$$

$$\text{f(T)} \equiv 4$$
$$\text{F(P)} \equiv 5$$

$$\alpha(29) + \beta \equiv 4$$
$$\alpha(25) + \beta \equiv 5$$

$$29\alpha - 25\alpha \equiv 4 - 5 \equiv -1 \equiv 36$$
$$\equiv 4\alpha \equiv 36 \rightarrow \alpha \equiv 9$$

$$(9)(25) + \beta \equiv 5 \equiv 225 + \beta \equiv 3 + \beta$$
$$5 \equiv \beta + 3 \rightarrow \beta \equiv 2$$

$$\alpha x + \beta \equiv 9x + 2$$
$$\text{x} \equiv ? \rightarrow \alpha x \equiv y - \beta$$

$$\alpha \equiv (\alpha^{-1})(y - \beta) \rightarrow X \equiv (\alpha^{-1})(y - \beta)$$
$$\equiv (9^{-1})(y - 2) \rightarrow (9^{-1})(y + 35)$$

$$\text{GCD(9,37)}$$
$$37 \equiv (9)(4) + 1$$
$$1 \equiv 37 - (9)(4)$$
$$\equiv -(9)(4) \rightarrow (9)(-4)$$
$$\equiv 9(33) \rightarrow 9^{-1} \equiv 33$$

$$\text{Inverse: x} \equiv 33(y + 35)$$
$$33\text{y} + 1155 \equiv 33y + 8$$

Question 1.

$$\text{f(x)} \equiv 9(x) + 2$$

Name: Jack
First Letter, $\text{f}(\text{l}_F) \equiv J \equiv 19$
$9(19) + 2 \equiv 173, \text{mod}37$
$\text{f}(\text{l}_f) \equiv 25 \rightarrow P$

Last Letter , $\text{f}(\text{l}_L) \equiv K \equiv 20$
$9(20) + 2 \equiv 182, \text{mod}37$
$\text{f}(\text{l}_L) \equiv 34 \rightarrow Y$

Name: Tom
First Letter, $\text{f}(\text{l}_F) \equiv T \equiv 29$
$9(29) + 2 \equiv 263, \text{mod}37$
$\text{f}(\text{l}_f) \equiv 4 \rightarrow 4$

Last Letter, $\text{f}(\text{l}_L) \equiv M \equiv 22$
$9(22) + 2 \equiv 200, \text{mod}37$
$\text{f}(\text{l}_L) \equiv 15 \rightarrow F$

Name: Saran
First Letter, $\text{f}(\text{l}_F) \equiv S \equiv 28$
$9(28) + 2 \equiv 254, mod37$
$\text{f}(\text{l}_f) \equiv 32 \rightarrow W$

Last Letter, $\text{f}(\text{l}_L) \equiv N \equiv 23$
$9(23) + 2 \equiv 209, \text{mod}37$
$\text{f}(\text{l}_L) \equiv 24 \rightarrow O$

Quesion 2.

$$f(\sum_{i=1}^{n}(l_{iF} + l_{iL}))$$

Jack: $\mathrm{f}(\mathrm{l}_{1F}) \equiv 25, f(l_{1L}) \equiv 34$
Tom: $\mathrm{f}(\mathrm{l}_{2F}) \equiv 4, f(l_{2L}) \equiv 15$
Saran: $\mathrm{f}(\mathrm{l}_{3F}) \equiv 32, f(l_{3L}) \equiv 24$
$\mathrm{n} \equiv 3$

$$f(\sum_{i=3}^{3}(l_{1F} + l_{1L}) + (l_{2F} + l_{2L}) + (l_{3F} + l_{3L}))$$

$$f(\sum_{i=3}^{3}(25 + 34) + (4 + 15) + (32 + 24))$$

$$f(\sum_{i=3}^{3}(59) + (19) + (56))$$

$$f(\sum_{i=3}^{3}(134)$$

$134, \bmod 37 \equiv 23 f(23) \equiv 9(23) + 2 \rightarrow 207 + 2$
$\mathrm{f}(23) \equiv 209 \rightarrow 209, \mathrm{mod} 37 \equiv 24, \rightarrow O$

Question 3.

g(x)$\equiv 33y + 8$

$$g(\sum_{i=1}^{n}(l_{iL}))$$

$$g(\sum_{i=1}^{3}(l_{1L}) + (l_{2L}) + (l_{3L}))$$

$$g(\sum_{i=1}^{3}(34) + (15) + (24))$$

$$g(\sum_{i=1}^{3}(73))$$

73, mod $37 \equiv 36$
g(36) $\equiv 33(36) + 8 \rightarrow 1188 + 8$
g(36) $\equiv 1196 \rightarrow 1196, \text{mod} 37 \equiv 12, \rightarrow C$

Euclidean's Algorithm

Helena Canny, Ellie Diamond, Ayla de Barra and Dean Ivers

Workshop tutor - Kirsten Pfeiffer

October 2020

Learning outcome

1) What is a modulus?
2) What is a multiplicative inverse?
3) What is the Euclidean Algorithm?
4) How do we put them together?

1 Modulus

1.1 Definition

The modulo (or "modulus" or "mod") is the remainder after dividing one number by another.

1.2 Example

A simple addition equation usually looks like the following:

$7 + 8 = 15$

However the equation

$7 + 8 = 3$

is also correct, on a 12 hour clock. This is because there is 12 hours on a 12 hour clock. Therefore

$15 - 12 = 3$

so as 3 is our remainder, we can then rewrite the equation as

$7 + 8 \equiv 3 mod 12$

same concept can be used for subtraction and multiplication

$7 - 8 = -1$ but on a 12 hour clock, -1 when subtracted from 12 gives us 11.

$7 - 8 \equiv 11 mod 12$

$7x8 = 56$

we can then divide 56 by 12, and we get a remainder 8

$7x8 \equiv 8 mod 12$

2 Multiplicative Inverse

2.1 Definition

A multiplicative inverse of a number is what you would multiply that number by to get one. In other words when you multiply a number by it's multiplicative inverse you end up with the number one. Another name for the multiplicative inverse is the reciprocal of a number.

2.2 Example

A simple example of this is when we are looking for the multiplicative inverse of 10. This means we are looking for the number we can multiply 10 by to obtain the number one.

$$10x = 1$$

We multiply 10 by one divided by itself we end up with 1. Therefore:

$$x = \frac{1}{10}$$

This means the multiplicative inverse of 10 is $\frac{1}{10}$. Which can also written as 10^{-1}.

2.3 How do we find this when using the modulus clock?

We can transfer our learning of the multiplicative inverse in numbers to using the multiplicative inverse in modulus. We are still looking for the number that when multiplied by another number will equal one.

For example: $7^{-1} = 2 \bmod 13$

This is because:

$7 \times 2 = 1 \bmod 13$ as

$7 \times 2 = 14$ which is 1 mod 13.

However, it is key to remember that there are numbers that do not have an inverse in certain modulus clocks as the number you are trying to find the inverse of and the modulus must be coprime.

For example:

$4^{-1} \bmod 12$ does exist as 4 and 12 are not coprime.

To find the inverse of bigger numbers on a modulus clock we can use the Euclidean Algorithm.

3 The Euclidean Algorithm

3.1 Definition

Euclidean's Algorithm (or Euclid's algorithm) is used to find the greatest common divisor (GCD) of two large integers. The GCD of 2 numbers is the largest number that divides into them both with no remainder.

3.2 Method

For this algorithm to work we may need to rewrite numbers to make them easier to work with. It would be very difficult to calculate the GCD of big numbers like 234 or 247 without first making them smaller.

For example: 234 can be written as 18x13 and 247 can be written as 19x13, in this case the GCD of these two integers is 13 as that is the greatest number that can divide into them evenly.

3.3 What do we do if the GCD of two numbers is 1?

This is where our algorithm really comes into play. We can not divide these numbers by any number other than themselves and 1 without leaving a remainder, this means these numbers are prime. Since their GCD is 1 we can call these numbers coprime.

Even though we can not divide and get whole numbers we still need to rewrite these numbers as we did before we will just have to add the remainder to our equation.

For example: The GCD of 23 and 167 is 1, (in these examples "." is used to represent the fact that we are multiplying) so we rewrite these numbers as shown,

$$167 = 7.23 + 6 \tag{1}$$

Meaning 23 goes into 167 seven full times with 6 as its remainder. We continue writing like this until our remainder is 1 as 1 is the GCD of our two numbers. Your equation should look like this by the end of our calculation,

$$167 = 7 \cdot 23 + 6 \tag{2}$$
$$23 = 3 \cdot 6 + 5 \tag{3}$$
$$6 = 1 \cdot 5 + 1 \tag{4}$$

This is what you need to know about Euclidean's algorithm before finding the inverse of a bigger number on a modulus clock.

4 Putting them all together

4.1 How are they linked?

The Modulus, The Multiplicative Inverse and Euclidean's algorithm can be linked as the modular inverse of a number refers to the modular multiplicative inverse. For any integer a such that (a,p)=1 there exists another integer b such that ab=(mod p). The integer b is called the multiplicative inverse of a, which is denoted as $b(a^{-}1)$

4.2 Where do we need to use all three concepts?

We need to use all three concepts when we are asked for the Multiplicative Inverse of a certain number (modulus another number). (ie.$(x^{-}1)$ mod y)

4.3 Example.

Find the Multiplicative Inverse of 3 (modulus 26)

In order to solve this problem we need to use Euclidean's Algorithm as demonstrated in Section 3.

$26 = 8x3 + 2$
$3 = 1x2 + 1$

Backwards Substitution

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1(26 - 8 \cdot 3)$
$1 = 3 - 1 \cdot 26 + 8 \cdot 3$
$1 = 9 \cdot 3 - 1 \cdot 26$
$9 \cdot 3 = 1 \cdot 26 = 1(mod 26)$

Therefore 9 is the multiplicative inverse of 3 (mod 26)

Maths tutorial project MA180.

•

Group 2: Laura Fannon, Paddy Gannon, Sinéad Gorham, Patrick Lynch Michelle O'Connor.

•

Project 1: How we would motivate and explain a question from the homework sheet to a group of Leaving Cert students. We explained question 3 from Graham Ellis' homework sheet 2.

•

Tutor name: Dr. Kirsten Pfeiffer.

•

Title of question (Q3, homework sheet 2): Fill in the blank in the following ISBN. 0-912843-0_1. $/Prove\ that\ the\ ISBN\ 0-912843-07-1\ is\ true?$

1 Introduction to Modular/Clock Arithmetic.

Are the following two equations correct?

$$8+5=13 \tag{1}$$

$$8+5=1 \tag{2}$$

Let us think.....
From the beginning of your education,you have been taught to not question that the equation (1) is correct and equation (2) is incorrect, which in some cases is not wrong. If Kate buys 8 shoes and has 5 pairs already, she now has 13 pairs of shoes not one but what if we were to change the context of the problem? Would our answer change? Would 8+5=1 ever be correct?

Let's say we are working on a 12-hour clock and to support her shoe addiction, Kate must work 5 hours starting from 8 am. Then she would finish at 1pm.
Therefore:

$$8+5=1 \qquad on\ \ a\ \ 12-hour\ \ clock \tag{3}$$

is as correct as

$$8+5=13 \tag{4}$$

This new number system illustrated in (3) is called Modular/Clock arithmetic.In clock arithmetic, we focus on the remainders of a sum after being divided by a fixed integer called a *"modulus"*.

For example:

$$15 \div 8 = 1 \ \ remainder \ \ \mathbf{7} \tag{5}$$

In modular arithmetic we notate this as:

$$15 \ \ mod \ \ 8 \equiv \ \ \mathbf{7} \tag{6}$$

and say that:

$$15 \ \ is \ \ congruent \ \ to \ \ 7 \ \ modulo \ \ 8 \tag{7}$$

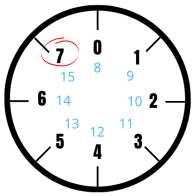


Figure 1: The above statement can be illustrated on an 8 hour clock as shown.

So a general definition of this, where a and b are integers, and m is a natural number:

$$a \equiv b \ mod \ m, \ \ \ where \ m \ divides \ evenly \ into \ (a - b). \tag{8}$$

1.1 Performing Arithmetic Operations with Moduli

1.1.1 Addition and subtraction.

As shown in a previous example, addition on a clock is quite simple.
Examples:

$$8 + 1 \equiv 9 \ \ mod \ 10 \tag{9}$$

$$8 + 20 \equiv 4 \ \ mod \ 24 \tag{10}$$

$$26 + 15 \equiv 17 \ \ mod \ 24 \tag{11}$$

Note: As, in clock arithmetic, we our working with a restricted range of numbers, we have to be careful of negative values as they are not shown on a clock. Let us try to understand negative values on a clock by changing this equation:

$$5 + 6 \equiv 0 \ \ mod \ 11 \tag{12}$$

into:

$$-5 \equiv 6 \ \ mod \ 11 \tag{13}$$

As -5 is not a value on an 11-hour clock, we immediately see that equation (13) differs from our previous examples.We do not know the value of -5 mod 11 but we can say that:

$$5 + (-5) \equiv 0 \mod 11 \tag{14}$$

So when we analyse this, we note that -5 mod 11 must be a natural number that when added with 5 on an 11 hour clock gives 0 as the answer. Hence, proving equation (13) to be correct.
Now with this knowledge,we can evaluate the following equations.

$$9 - 3 \equiv 6 \mod 12 \tag{15}$$

$$8 + 3 \equiv -1 \mod 12 \tag{16}$$

$$22 - 26 \equiv 20 \mod 24 \tag{17}$$

1.1.2 Multiplication and Division

Multiplication in modular arithmetic is not complicated as it follows the normal procedure.

$$3 \times 7 \equiv 11 \mod 10 \tag{18}$$

$$2 \times (-10) \equiv 4 \mod 24 \tag{19}$$

While to understand division on a clock, we must first recognise:

$$12 \div 5 = 12 \times 5^{-1} \tag{20}$$

5^{-1} is called the multiplicative inverse and to find this inverse on a clock, we recognise that when the multiplicative inverse of 5, is multiplied by 5 the answer must be 1. For example:
What $is\ 5^{-1}\ on\ a\ 24-hour\ clock$?
$After\ some\ experimentation,\ we\ notice\ that:$

$$5 \times 5 = 25 \equiv 1 \mod 24 \tag{21}$$

So the multiplicative inverse of 5 on a 24 hour clock must be 5.

Now that we have been introduced to this new system called Modular arithmetic and can understood its arithmetic operations, we now must question how we will use this in the question at hand.

1.2 What is an ISBN?

Do you recognise this image above and if so, where have you seen it before?

This is an International Standard Book Number (ISBN). An **ISBN** is a code used to identify products for sale online e.g. a book for sale on amazon. When creating an ISBN, modular arithmetic is used,in particular mod 11. When given the first 10 digits with the last digit is kept secret as a security check, we can use this fact to find the missing digit or prove this ISBN is correct.

2 Solving the Question

Prove that the International Book Sellers Number (ISBN) 0-912843-07-1 is true?.

To prove whether this ISBN is true, when it is applied to a modular clock of 11, it should be congruent to 0.

- We begin by *multiplying all the digits in the ISBN individually* by the *order they appear* i.e 0 would be multiplied by 1 as its the first number in the ISBN number sequence, 9 would be multiplied by 2 as its the second number in the sequence, 1 would be multiplied by 3 s its the third number in the sequence and so on:

  $(0.1) + (9.2) + (1.3) + (2.4) + (8.5) + (4.6) + (3.7) + (0.8) + (7.9) + (1.10) \bmod 11$

- We then work out what is being multiplied in the brackets in our equation while keeping the number we arrive at in brackets:

  $(0) + (18) + (3) + (8) + (40) + (24) + (21) + (0) + (63) + (10) \bmod 11.$

- Then we apply our modulus clock of 11 to the results that we arrived to in our brackets from the previous step of multiplying:

  $0 + 7 + 3 + 8 + 7 + 2 + 10 + 0 + 8 + 10 \bmod 11.$

- After completing this we then add all our integers together to have just one integer mod 11 i.e. x mod 11:

  $55 \bmod 11$

- Finally we apply our modulus clock of 11 to our accumulated integer and once the congruent number is 0, then we know that the ISBN is true:

  $55 \equiv 0 mod 11$

- As our congruent integer we arrive to is 0, we can rightfully say that the ISBN 0-912843-07-1 is true.

3 Misconceptions

The Modular arithmetic has many uses in our lives, but in order to be able to properly preform it we must understand the common mistakes and misconceptions.

1. Ensuring all calculations are made to the correct mod and including the mod in your answer.

2. When calculating the mod ensure to take the remainder as your answer. **Example:** $12 mod 10$ To calculate this we divide 12 by the mod12 $12/10 = 1r2$ As the remainder is 2 we can then say that 12 is congruent to 2 on a 10 hour clock ie. $12 = 2 mod 10$

3. When working with negative numbers we must remember that negative numbers cannot be shown on a clock. **Example:** -3 does not exist of a 14 hour clock. To calculate this we can work backwards on the clock ie. $14 - 3$ by doing this we find the answer to be 11

4. When dealing with the multiplicative inverse ensure your answer is congruent to 1 using the given mod. **Example:** $7^{-1} mod 10$

To complete this example we must find out what multiplied by 7 gives you 1 on a 10 hour clock. This can be done by trial and error. We will then see that $7x3 = 21$ When we put this on a 10 hour clock we get $1 mod 10$. Therefore $7^{-1} = 3 mod 10$

4 Applications

The Modular arithmetic has many uses

1. It can be used to encipher and decipher codes.

2. It is used for ISBN numbers (identification numbers for books) **Example:** 978-3-16-148410-0

3. It is used in bar codes to create a unique 12 digit identification code for products.

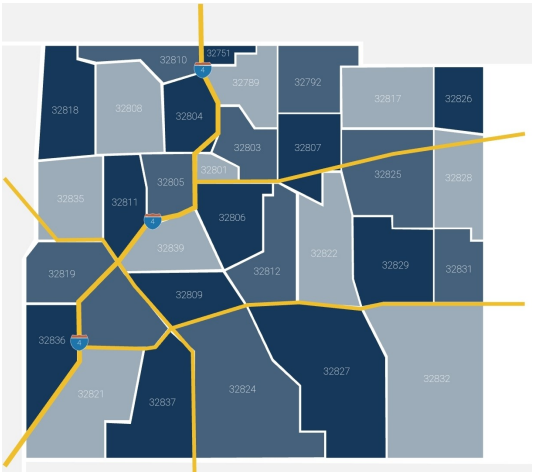


Figure 2: Map of Orlando postal codes created by the elementary number system

4. It is also used to create postal codes to locate individual addresses. **Example:**32801 thru 32837 are the postal codes from Orlando Florida.

5 Conclusion

To finish up I would just like to acknowledge the importance of understanding modular arithmetic in daily life, not just as a part of our mathematical knowledge. Let's take the ISBN number as an example. The final digit in an ISBN number is called a safety check digit. This digit allows a publisher to see if an error has been made when an order is placed for a book or in fact if the order is correct.
As previously stated, there are numerous other uses and applications of modular arithmetic and the elementary number system in daily life, one being the calculation of unique postal codes. Every single address requires a unique postal code for purchasing goods online and even just a regular post.
Thus, from our discussions while answering this question, we have been introduced to a whole new side of mathematics, which is not only fascinating but ultimately an essential element of everyday life that before this, we simply did not notice.

Group Project

Brendan Penny, Glenn Carolan, Zach Nolan, Zoe Arthurs

October 2020

1 Introduction

Number theory, sometimes known as "arithmetic", studies the properties of the integers: ...-3,-2,-1,0,1,2,3... Although the integers are familiar, and their properties might therefore seem simple, it is instead a very deep subject.

2 Basic Arithmetic

We're going to begin with basic arithmetic:

- 5+10=15
- 22+19=41
- 8 x 7=56

3 Modulo

This is very easy to understand, however when we introduce modulo it does get more complicated. We'll do some examples around the basis of a 24 hour clock, thus our modulo being 24(as there is 24 hours in a day).

3.1 Examples:

- 10+16=26 — 26=2am mod 24
- 5+13=18 — 18=18 (6pm) mod 24
- 9 x 4= 36 — 36=12pm mod 24

Now lets take it as weeks. Our modulo thus being 7(as there is 7 days in a week). Example: Today is Wednesday. In 54 days it will be Friday.

- 3+54=57 — 57= 5 mod 7

4 Question

Now we pose our question. Calculate **7 x 8 mod 12**. Your answer should be an integer in the range [0,1,..10,11]

5 How To Motivate Your Students

5.1 Make It Interesting For The Students

It can be easy for students to lose interest if there is nothing of interest for them. This could be done by allowing them to take part in the lesson. For example ask the students questions to involve them instead of an autocratic style of teaching.

5.2 Let the Information being thought be Obtainable for all Students

An average class size is between 21-30 students and not all students will have the same competency of maths. With this in mind you must deliver a lesson that has all students in mind. For example, you may introduce a new topic slower than you might teach your lessons on the topic in later classes. As well you might use class time to help students that may be struggling.

5.3 Make The Lesson Relatable

Some students can find it hard to listen in class even at the best of times so makinging it as enjoyable and relatable as possible is extremely important to motivating students. For example using the idea of clocks to describe a lesson on modules. Clocks are something all students should be able to read and will find it much easier to learn it that way than any other.

5.4 Keep the Students Confident in their Ability

Students can find themselves losing confidence in their ability when they get questions wrong and especially when a new topic is being introduced. To keep your students motivated you might give them a lighter or easier work load, praise them for their work and encourage hard work over the right answer.

Project 1

Clodagh Kennan,Danielle Quinn, Kiera White
Kirsten Pfeiffer

November 6, 2020

Explain what is meant by -7 x 8 mod 12 and how to calculate it.

1 Introduction

We would first define modular arithmetic before explaining thoroughly what it means and the method used.

Modular arithmetic can also be referred to as clock arithmetic and is denoted as mod N.

As we already know, arithmetic is the processes of addition,subtraction, multiplication and division.

Modular arithmetic is arithmetic done with a count that resets itself to zero every time a certain whole number N has been reached.
Note: N is always greater than one.
Taking a clock for example, this would be mod 12. 12 is our whole number N and every time we reach a multiple of 12 it changes to 0.

When left with a remainder, that remainder is our answer. For example, with 25 mod 12, we reach 12 twice at 12,24. This leaves us with a remainder of 1.

Therefore

$$25 mod 12 \equiv 1$$

1.1 Including real life applications

We would then explain why we need modular arithmetic in real life.

It is used to verify the ISBN number on a book by which helps to give the book a unique identification, acting like a barcode.

The 10-digit number is found on the back of the book and must satisfy the equation

$$x1 + 2x2 + 3x3 + \ ... + 10x10 \equiv 0 mod 11$$

This method is essential to libraries and book stores.

1.2 Easy example

For example 10+11= 9 on a 12-hour clock which we write as $10+11 \equiv 9 mod 12$

1.3 Further understanding

To further the students understanding we would now get them to discuss examples of modular arithmetic with time and see if they can think of any other real life examples, the months of the year for example. It is also used in IBANs in the bank and ISBNs in bookshops. If the students were still struggling to understand this concept we would use physical clocks to further their understanding.

2 Progressing towards the question

Before starting the question above we will work through an easier example

$$7 \times 8 \equiv 6 mod 10$$

We know this because

$$7 \times 8 = 56$$

On a 10 hour clock all multiples of 10 are 0 e.g, 10,20,30,40,50. We are left with a remainder of 6 and therefore

$$7x8 \equiv 6 mod 10$$

3 -7 x 8 mod 12

Now we will move on to a more complex equation

$$-7x8 mod 12$$

- We know that
$$-7x8 = -56.$$
- As -56 is a negative number we will we will go up to the closest multiple of 12.

(We would now ask the students to think about the multiples of 12 and give us a suitable answer.)

- The multiples of 12 are

$$12, 24, 36, 48, 60, 72.$$

- We will use 60 in our equation.
- We use 60 because you must ALWAYS go up to the higher number when working with negatives in modular arithmetic. This is so we are not left with another negative in our answer
- To find our final answer we use

$$60 - 56 = 4$$

- Therefore,

$$-7x8 = 4mod12.$$

4 Conclusion of the lesson

To conclude the lesson we would go through a variety of other examples to give a full understanding of the concept.

To ensure that the students understand the concept we would get them to give us answers to equations and to also let them work through examples in groups and individually.

MA-185 Project, Group 5

Anthony Jordan, Cliodhna Carey, Elijah Alliowe, Matthew Fahey, Micheál Durkin

November 2020

Workshop Tutor Kirsten Pfeiffer

1 Introduction to Modular Arithmetic and ISBN

Picture a 12-hour clock, something we are all familiar with and use every day. But how does a clock relate in any way to algebra? As we all know on a traditional clock face there are 12 numbers. 12 o'clock is the number 0, 1 o'clock is number 1, 2 o'clock is number 2 and so on up to 11 o'clock is number 11.
We know how to add numbers on a clock. If it is now 6 o'clock, in 8 hours' time it will be 2 o'clock. 6 add 8 is equal to 2 on a 12-hour clock, but why? Well on a 12-hour clock the number 12 is equal to 0. Every time a clock passes 12 o'clock it returns to zero therefore every multiple of 12 when calculated on a 12-hour clock is equal to zero. Another example could be 12 add 5 on a 12 hour clock is equal to 5, because as we now know all multiples of 12 on a 12 hour clock are equal to 0. We use the following notation to denote this, 5+12=5 mod 12.

Now that we understand the concept of clock arithmetic, we will go on to talk about the ISBN. ISBN stands for the International Standards Book Number, a number found on the back cover of books used to identify them. But how does this relate in any way to clocks? We will start by explaining how the ISBN works. Each ISBN is a 10-digit number. Whenever a book is ordered online, and the ISBN is entered, the book seller conducts a calculation. This calculation involves taking the first number of the 10-digit ISBN and multiplying it by 1, adding this to the second number multiplied by 2, adding this to the third multiplied by 3 and so on.

For example, if we had an ISBN

$$X_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}$$

The calculation would be as follows

$$X_1 + 2X_2 + 3X_3 + 4X_4 + 5X_5 + 6X_6 + 7X_7 + 8X_8 + 9X_9 + 10X_{10}$$

This is where the idea of clocks comes in to play. The number produced from the calculation above is then calculated on an 11-hour clock. The number

produced from any ISBN using the calculation above will equal 0 on an 11-hour clock. Or to put it differently,

$$1X_1 + 2X_2 + 3X_3 + 4X_4 + 5X_5 + 6X_6 + 7X_7 + 8X_8 + 9X_9 + 10X_{10} = 0 mod 11$$

If the number does not equal zero when calculated it is clear to the book seller the there has been an error made when typing in the ISBN.
Written by Cliodhna Carey

2 What is Modular Arithmetic

From the introduction you have heard of modular arithmetic and how it is used in ISBN.
But before we can see how modular arithmetic is being used in ISBN, we must first learn what it is and how it works.

You may be surprised to learn that everybody uses modular arithmetic everyday, and that we all understand its use.
You might be wondering 'Well how is this possible, as I'm only just hearing this term being used now'.
This reading will attempt to show you that you have used modular arithmetic before.

First off, I will ask you to calculate these 2 equations.

$$8 + 4 = x$$

and

$$9 + 6 = y$$

seems pretty easy, right?

Well, what if I were to say instead of my results being

$$8 + 4 = 12$$

and

$$9 + 6 = 15$$

I found that my results were very different.

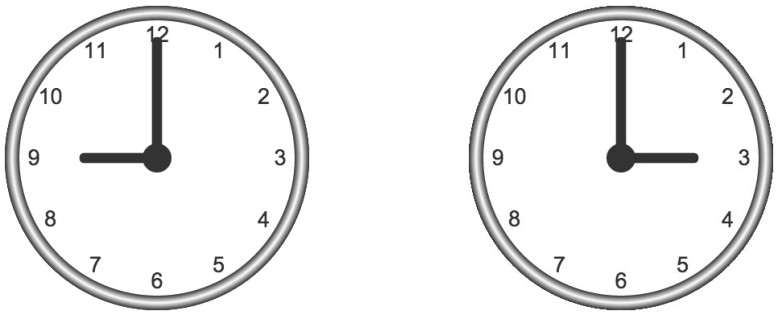
$$8 + 4 = 0$$

and

$$9 + 6 = 3$$

This seems a bit strange or just simply untrue, or maybe that I'm using some trick, maybe that I made my character for $3 = 15$.

This equation is true but only in certain exceptions, and we use one such exception every day.



(a) 9 o 'clock (b) 3 o'clock

Figure 1: 6 hours after 9 o'clock is 3 o'clock

You may have already guessed it but if it is 9 o'clock we know that 6 hours later will be 3 o'clock. [1]

So how can we avoid confusion as to which equation we want to use $9+6 = 15$ or $9 + 6 = 3$.

We write $9 + 3 = 3$, the equation that represents the hours on a clock as $9 + 6 \equiv 3 mod 12$.

We use $mod 12$ in this equation because we are working with a clock that has 12 hours on it. We also use $\equiv$ instead of $=$.

Now that that you understand what is meant by modular arithmetic we can see its use in another everyday example such as... the days of the week.

Figure 2: Caption1

If we label each day to a distinct integer for example Monday=1, Tuesday=2....Sunday=7.
We use mod 7, this is because there are 7 days in a week and after the 7th day the cycle repeats. We can see the usefulness of modular arithmetic in this everyday example.
If we needed to know what day of the week a particular day was in a certain amount of days.
For example we know that today is Tuesday and we need to know what day it will be after exactly 150 days.

Well, we can write. $2 + 150 = 152$.
Then we can divide 152 by 7 and get a remainder.

$$\frac{152}{7} = 21r5$$

.
The remainder of this is 5.
Because the remainder is 5 we know that 152 days after Tuesday (your current day), it will be a Friday.
Friday is 5 on this clock.

Now for many of you, this may be the first time since national school having used a remainder in a fraction.
There's no need to worry, there are different methods of understanding modular arithmetic.

Alternatively another way of thinking about the problem is that you can subtract 7 from 152 until you are left with the 5. $152 - 7(21) = 5$

One more efficient method, especially in regards to working with larger numbers is to divide 152 by 7, then you minus the whole number (if there is any) from your result and multiply the remainder by 7.

$$\frac{152}{7} = 21.\dot{7}14285\dot{5}$$

$$21.\dot{7}14285\dot{5} - 21 = 0.\dot{7}14285\dot{5}$$

$$7 * 0.\dot{7}14285\dot{5} = 5$$

Of course you could also write $21.\dot{7}14285\dot{5}$ as $21\frac{5}{7}$

The reason why the division method works is because 7 goes into 152 21 times and has $\frac{5}{7}$ of 7 left over and of course $\frac{5}{7}$ of 7 is 5.

$$\frac{5}{7} * 7 = 5$$

3 Applications of Modular Arithmetic

We have discussed its use as hours on the clock and days of the week but it also works....

- Months of the year
- Encryption and in code making
- RSA encryption, form of encryption used on the internet
- IBAN numbers for banking
- Used in Music, as notes repeat after 12 semi-tones in Western music's equal temperament, the notes of the keys on a piano.
- Bar-codes
- ISBN

ISBN is the number on the back of all purchasable books and it is used to identify the particular book. We will now discuss this topic more.
Written by Anthony Jordan.

4 What is ISBN

The International Standard Book Number, the ISBN, is a practical application of modular arithmetic which is used every single day by booksellers, libraries and universities, to establish and identify one title or edition of a title from one specific publisher.

It is a 10-digit number found on the back of books used to identify them. Whenever a book is ordered online, and the ISBN is entered, the book seller conducts a calculation. This calculation involves taking the first number of the 10-digit ISBN, with the final digit being a safety check against any errors made, and multiplying it by 1, adding this to the second number multiplied by 2, adding this to the third multiplied by 3 and so on. As seen in our introduction, if we were to have an ISBN:

$$X_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}$$

the calculation would be as follows:

$$X_1 + 2X_2 + 3X_3 + 4X_4 + 5X_5 + 6X_6 + 7X_7 + 8X_8 + 9X_9 + 10X_{10}.$$

The sum of these numbers will then be taken and put on an 11-hour clock. This will always be equal to 0 on an 11-hour clock, for a correct ISBN. If the number does not equal zero when calculated it is clear to the book seller that there has been an error made when typing in the ISBN.
Written by Micheál Durkin

5 Example of ISBN

Any book is identified by its ISBN. For older books this is a string of ten digits.

$$3 - 540 - 9429Y - 7$$

is the number for a hypothetical book we will call "The best book ever". The final digit is a safety digit. The second last number, Y, in the ISBN is unknown. Recall that the formula for ISBN can be written as:

$$X_1 + 2X_2 + 3X_3 + 4X_4 + 5X_5 + 6X_6 + 7X_7 + 8X_8 + 9X_9 + 10X_{10}.$$

I will now determine Y using this formula.

$$(1)(3)+(2)(5)+(3)(4)+(4)(0)+(5)(9)+(6)(4)+(7)(2)+(8)(9)+(9)(Y)+(10)(7) = 0 mod 11$$

$$3 + 10 + 12 + 0 + 45 + 24 + 14 + 72 + 9Y + 70 = 0 mod 11$$

$$3 + 10 + 1 + 0 + 1 + 2 + 2 + 6 + Y + 4 = 0 mod 11$$

$$29 + Y = 0 mod 11$$

$$7 + Y = 0 mod 11$$

$$11 - 7 = 4$$

$$Y = 4$$

Written by Ellijah Alliowe

6 Conclusion

We have now seen a practical use of modular arithmetic, the International Standard Book Number (ISBN), which is used every single day by booksellers, libraries and universities, to establish and identify one title or edition of a title from one specific publisher. This is achieved by using 10 digits, with the final digit being a safety check against any possible mistakes made. Multiplying the first digit by 1, the second digit by 2 and so on, until the final digit multiplied by 10, you then add these numbers together. If the sum of these numbers is equal to 0 on an 11-hour clock, the ISBN is correct. This means that each time your sum reaches a multiple of 11, this number will be counted as a zero and the following proceeding number will count up from 1 until again reaching 11 – for example, the number 23 will be equal to 1 on an 11-hour clock. With this in mind, we can now use this idea to calculate what a missing digit in an ISBN is, as seen in the example above where we have the ISBN:

$$3 - 540 - 9429Y - 7$$

In which case we found that:

$$Y = 4$$

This was achieved using modular arithmetic, along with the knowledge that the sum of the 10 digits in an ISBN, when multiplied by the number of their order in the ISBN, must be equal to 0 on an 11-hour clock. In conclusion, this is one of many applications of modular arithmetic which is used every single day, and one that should be very easy to calculate for most maths students, with the use of the correct process, as outlined above.
Written by Matthew Fahey

References

[1] Ellis,G (2020) $MA180Mathematics$: $Lecture1$[Lecture], MA180, MA185, MA190 Mathematics. NUI Galway. 28 September.

[2] images taken from Google Images

Clock arithmetic

Nicole Fortune-Lydon,
Imogen Hards,
Padraig Horgan,
James Webb
Workshop tutor- Dr. Kirsten Pfeiffer

November 2020

1 Introduction

In mathematics, modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value, called the modulus. The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in his book Disquisitiones Arithmeticae, published in 1801.The basics of modular artimetic has similar operation to that of standard artimetic such as addition, subtraction, multilplcation and division which we will explain below.

2.Addition in modular arithmetic-

11+4=? mod 12

The best way to understand addition within modular arithmetic is to think of the face of a clock

The numbers go from 1 to 12 but when it goes to '13 o'clock', it actually goes back around to 1 o'clock again

Think of how a 24 hour clock works. 13 becomes 1, 14 becomes 2 and so on

On a 12 hour clock what do we get if it is 11 o'clock and add 4 hours. 3 right?

You might not know it but you are doing modular arithmetic here, you are doing the mentioned sum

We add 11 and 4 which gives us 15 and then 12 goes into 15 1 time remainder 3

Thus 11+4=3 mod 12

(It is worth mentioning that 12 behaves as 0 here)

3.Subtraction in modular arithmetic-

2-11=? mod 12

To start, the key difference between standard arithmetic and modular arithmetic is that in the latter there is a certain range of values the answer can only be equal to, such as on a 12 hour clock the hours can only be between 1 and 12

What is 11 hours before 2 o'clock?

Standard arithmetic says 2-11=-9

But -9 isn't on a 12 hour clock

If we think about it all we must do is 12-9=3 and 3 is on the clock so it is the correct answer

Thus 2-11=3 mod 12

4.Multiplication in modular arithmetic-

5x13= ? mod 16

One way to understand this equation is to note that it refers to an maths equation on a 16 hour clock, and on that clock there are only 16 numbers (0,1,2,.....,15)

For instance we cant let 5x13=65 be the answer in this context as 65 does not appear on a 16 hour clock

What we do is see how many times 16 goes into 65 and the remainder is our answer mod 16

65 divided by 16 is equal to 4 remainder 1, therefore, 65=1 mod 16 Thus 5x13=1 mod 16

5.Calculating an inverse number in clock arithmetic-

$9^{-}1 = ?mod11$

What we are trying to calculate here is the inverse of 9 on an 11 hour clock

In order to do that we need to see what number you have to multiply by 9 to get 1 on an 11 hour clock

In this case the number is 5 because 5x9=45 and 11 goes into 45 4 times leaving a remainder of 1

6.Problem sheet 1- question 3:

Fill in the blank in the following ISBN 3-540-9429$_{-7}$

Step 1 Split all of the numbers up labeling our blank as X 3+5+4+0+9+4+2+9+X+7

Step 2 Start by multiplying the first number by 1 and then the second number by 2 all the way up to the last number which is the tenth number by 10. All book codes are calculated mod 11(or on an 11 hour clock) therefore the answer is equal to 0 mod 11 (the answer must be a multiple of 11). E.g: (3x1)+(5x2)+(4x3)+(0x4)+(9x5)+(4x6)+(2x7)+(9x8)+(Xx9)+(7x10)= 0 mod 11

Step 3 Solve the equation keeping in mind the rules of modular arithmetic. 250+9X= 0 mod 11 (250= 8 mod 11, because 11 goes into 250 22 times remainder 8) 8+9X= 0 mod 11 9X= -8 (which is equal to 3 mod 11 because 11-8=3) 9X=3 mod 11 X= 3/9 mod 11 (which can be written as $(3)(9^{-}1)mod11)X = (3)(9^{-}1)mod11(9^{-}1 = 5mod11)X = (3)(5)mod11X = 15mod11(15isequalto4onan11hourclock)X = 4mod11FinalanswerX = 4$

Modular Arithmetic for Leaving Certificate Students

Alex Gordon, Ronan Kenny, Ryan Shannon

Daniel O'Flanagan, Oran O'Reilly

Tutor: Kirsten Pfeiffer

November 2020

1 Explanation of Modular Arithmetic

Modular arithmetic (also known as 'clock arithmetic') is a form of integer arithmetic in which all integers that have the same remainder when divided by a given natural number (called the 'modulus') are considered equivalent. The reason modular arithmetic can sometimes be known as clock arithmetic is because it applies directly to reading time/clocks.

Example It is now 9 o clock, what time will it be in 8 hours ?

Solution We are calculating

$$9 + 8 \mod 12$$

First, perform the calculation

$$9 + 8 = 17$$

Then subtract the modulus

$$17 - 12 = 5$$

$$\Rightarrow 9 + 8 = 5 \mod 12$$

Therefore, in 8 hours it will be 5 o'clock.

Modular arithmetic can also be used in other scenarios as well. For example it can be used for calculating the day of the week (mod 7), how many weeks are left in the year (mod 52) and how many days are left in a year (mod 365 or mod 366).

Example Today is Thursday, what day will it be in 54 days time?

Solution We are calculating days of the week ($mod 7$). We can ascribe the days numerical values with Monday=1, Tuesday = 2...Saturday = 6, Sunday = 0.

In this system, Thursday would be day 4. Thus we are calculating:

$$4 + 54 \mod 7$$

Again, we begin with the normal calculation

$$4 + 54 = 58$$

Then we apply the modulus, using multiples of 7 to reduce the total.

$$7 * 8 = 56$$

is the closest value to 58 and also less than 58.

$$58 - 56 = 2 => 4 + 54 = 2 \mod 7$$

Therefore in 54 days it will be Tuesday, since Tuesday is the second day.

It is important to note that all values in a modular calculation are, or are equivalent to, an integer in the range [0, modulus - 1]. So, the value of any number in $\mod n$ cannot be greater than $n - 1$, and must be an integer.

Negative Values Negative integers are also able to be calculated. For example:

Calculate:

$$3 - 8 \mod 6$$

We first calculate $3 - 8$ which is of course -5. Then, we 'add' this number to the modulus, to find a result of 1. Therefore:

$$3 - 8 = 1 \mod 6$$

2 Euclidean Algorithm

The Euclidean algorithm is an efficient way of finding the greatest common divisor of two integers, usually denoted as $\gcd(x, y)$, which is the greatest number that will divide two integers without leaving a remainder. It is used in modular arithmetic when we have a large number modulus. We can also use the output of the Euclidean algorithm to evaluate the inverse of a number in modular arithmetic.

What is an inverse? Before we explain everything else, it is important to know its relevance to modular arithmetic. The Euclidean algorithm is used to find the inverse of a number, $m \mod n$. But what is an inverse?

In regular scalar arithmetic, the inverse of a number is denoted by x^-1, and is usually written as $1/x$. For example, 7^-1 in standard arithmetic is $1/7$. Another way of phrasing this is that the inverse of a number is the number that, when multiplied by the original number, gives you a value of 1. In standard arithmetic, since there is only one instance of 1, it is simple enough to calculate for any integer. In modular arithmetic, however, this is not the case.

The issue with this in modular arithmetic is that we do not deal with fractions or decimals, only whole integers. Therefore, the inverse of a number must also be a whole number.

An easy example Calculate $2^-1 mod 5$.

$$\begin{aligned} 2 * x &= 1 \mod 5 \\ 2 * x &= \{1, 6, 11, 16, 21...\} \\ 2 * 3 &= 6 => \\ 3 &= 2^-1 \mod 5 \end{aligned}$$

We could also say, for example, that $2 * 8 = 16$, so why not use that? Well, $8 = 3 \mod 5$, so it is the same thing. When working in a modulus, you should reduce all numbers until they are less than the modulus, as we saw in an earlier section.

Example What is the gcd$(19, 26)$?

To begin, we write down the two numbers, 19 and 26. The system used in the algorithm is to first find the greatest number of times you can multiply the smaller number (19) and still be less than the greater number (26). Then, you write down the remainder after you do the calculation. On the next line, write down the smaller number in the place of the greater number (19 in place of 26) and the remainder in place of the smaller number (7 in place of 19) and repeat the process. In words, it seems complicated but it is in fact quite simple.

Demonstration

$$\begin{aligned} 26 &= 1 * 19 + 7 \\ 19 &= 2 * 7 + 5 \\ 7 &= 1 * 5 + 2 \\ 5 &= 2 * 2 + 1 \end{aligned}$$

(Note how the 7 changes position across lines 1, 2, and 3, and the 5 across lines 2, 3, and 4.)

Once the remainder is 1, we stop the algorithm as there are no further values.

Coprime If the $\gcd(x, y) = 1$, we say x and y are *coprime*.

As we can see from above, 19 and 26 are coprime. In modular arithmetic, a number can only have an inverse if it is coprime with the modulus. Therefore, we know that 19 has an inverse in modulus 26. But how do we calculate it?

Using Euclid to calculate the inverse To calculate the inverse, we need the lines from the Euclidean algorithm. Since the numbers are coprime, the last value is 1. We can rearrange the lines, starting from the last one, to have several lines that all equal 1. As we move up the lines, we find we have

$$19(x) + 26(y) = 1 \mod 26$$

in this instance. Of course, in other instances, the coefficients are different. This method relies on the idea that $26 * a \mod 26 = 0$ where a is any integer. Therefore, we have the last line of the calculation as

$$19(x) = 1 \mod 26$$

.

Demonstration

$$\begin{aligned} 1 &= 5 - 2 * 2 \\ &= 5 - 2 * (7 - 1 * 5) \\ &= 3 * 5 - 2 * 7 \\ &= 3 * (19 - 2 * 7) - 2 * 7 \\ &= 3 * 19 - 8 * 7 \\ &= 3 * 19 - 8 * (26 - 1 * 19) \\ &= 11 * 19 - 8 * 26 \mod 26 \end{aligned}$$

and since $26 * a = 0 \mod 26$, we now have

$$19 * 11 = 1 \mod 26$$

which can be written as

$$11 = 19^{-}1 \mod 26$$

This is how to find the inverse of a number in modular arithmetic. A number, m can only have an inverse $\mod n$ if m and n are *coprime*.

3 Affine Enciphering Functions

An affine enciphering function is a form of encryption. It is not overly secure, and so should only be used for mathematical and demonstrative purposes. Using

it for important security could be deemed reckless, as it is not overly difficult to decipher.

To use the affine enciphering function we need to be familiar with the alphabet being used. We commonly use a 37-letter alphabet. This is an alphabet commonly used in affine crypto-systems. It is based on the standard Latin alphabet, but it only uses capital letters and also includes numbers and an underscore to usually represent a 'blank' space. Other alphabets can include only letters (26), extra symbols (37+) or lowercase letters (52+).

The 37-letter alphabet that we will use in examples is as follows:

$$0, 1, 2..., 9, A = 10, B = 11, C = 12..., Z = 35, \_ = 36$$

Once you are familiar with the alphabet (in this instance, 37-letter), you can begin to use the affine enciphering systems.

Form of the Function An affine enciphering function over single letter message units is one of the form:

$$f_e(x) = \alpha x + \beta \mod n$$

where x is your input value and α and β are constants. The input, x must be an integer, which is determined by a corresponding value in your n-letter alphabet.

For example if we wanted to encipher the word 'HELLO' (we can only use capital letters) using a 37-letter alphabet and over single message units, we would do the following:

- Convert 'HELLO' to its corresponding numerical values
- Input those values into the enciphering function
- Take the outputs and change them into their corresponding values in the alphabet

First, we must have the defined enciphering function. Taking α to be, arbitrarily, 4, and β to be, arbitrarily, 7, we have the following function:

$$f_e(x) = 4x + 7 \mod 37$$

Now to convert our plain-text, 'HELLO', to cipher-text. 'HELLO' = 17/14/21/21/24
Applying the function to each of these we get:

$$\begin{aligned}
f_e(17) &= 4(17) + 7 \mod 37 = 75 \mod 37 = 1 \mod 37 \\
f_e(14) &= 4(14) + 7 \mod 37 = 63 \mod 37 = 26 \mod 37 \\
f_e(21) &= 4(21) + 7 \mod 37 = 91 \mod 37 = 17 \mod 37 \\
f_e(24) &= 4(24) + 7 \mod 37 = 103 \mod 37 = 29 \mod 37
\end{aligned}$$

So our output is 1/26/17/17/29.

Then, if we correspond these integers to their alphabetical pairs we produce the cipher-text: 1QHHT

That is how we use an affine function to encipher. But how do we decipher?

Deciphering the text As we know, the enciphering function is of the form:

$$f_e(x) = \alpha(x) + \beta \mod n$$

It may seem intuitive, then, that the deciphering function is actually just the inverse of the enciphering function, or f_e^-1.

This is found by rearranging to make x the subject of the function, as follows:

$$f_d(x) = \alpha^-1(x - \beta) \mod n$$

This involves calculating the inverse of $\alpha \mod n$, which is covered in a previous section, on the Euclidean algorithm. Once this is calculated, simplify the expression, reducing it until all terms are less than $n-1$. To decipher, simply substitute in your values (in integer form) and then correspond the outputs of the function.

4 Applying the concepts to the question

The question is as follows: 'The following cipher-text was produced using an affine enciphering function

$$f_e : Z_{37} => Z_{37}, x => \alpha x + \beta$$

on single letter message units over the 37-letter alphabet

$$0, 1, 2, ..., 9, A = 10, B = 11, ..., Z = 35, = 36$$

where underscore represents a blank.

The last nine characters of plain text are: COMPUTING. Determine the second word of the original plain-text.'

The cipher-text: 2G106I4E7Y04I2G14I2LSLI90II9027TL9B

0HIY02G106I2G1T0E604EX1T90SE4J72L9B

(Taken from Okuson Homework Sheets, Q5, Prof. Graham Ellis)

Solution To begin, we need to provide the reference values. Since we are working with single letter message units, we can take the values one at a time.

COMPUTING == SE4J72L9B

We can also take the previous character, 0, to be equivalent to a blank.

We must also ascribe each letter a numerical value, according to the table above.

For example, taking the last characters, we get

$$G = 16$$

and

$$B = 11.$$

The function above takes the input G, or 16, and outputs B, or 11. Similarly, it takes the input C, or 12, and outputs S, or 28. It is good to note that the 'blank' is 0 in this specific instance, as you can locate and determine the length of the second word of plain-text.

Simultaneous Equations As such, we can define the following simultaneous equations:

$$16 => \alpha(16) + \beta = 11 \mod 37 \tag{1}$$

$$12 => \alpha(12) + \beta = 28 \mod 37 \tag{2}$$

Solving the equations simultaneously, we get

$$\begin{aligned}(1) - (2) &= \alpha(16) - \alpha(12) + \beta - \beta = 11 - 28 \mod 37 \\ &= \alpha(4) = -17 \mod 37 \\ &= \alpha(4) = 20 \mod 37 \\ &= \alpha = 5 \mod 37\end{aligned}$$

We now have the value $\alpha = 5$, which we can substitute into either equation to evaluate β.

$$\begin{aligned}(5)(16) + \beta = 11 mod 37 &=> \beta = 11 \mod 37 - 80 \\ &=> \beta = -69 \mod 37 \\ &=> \beta = 5 \mod 37\end{aligned}$$

Changing from enciphering to deciphering function Now we have our values for α and β, we can construct the deciphering function. It is important to note that the deciphering function is always constructed as such:

$$f_e = \alpha(x) + \beta => f_d = \alpha^{-}1(x - \beta)$$

or

$$f_d = f_e^{-}1$$

where f_e and f_d are the enciphering and deciphering function respectively.

So, substituting in 5 for α and β, we get

$$f_e = 5(x) + 5 \mod 37$$

To find f_d, we apply the procedure above, specifically:

$$f_d = 5^{-}1(x - 5) \mod 37$$

To proceed, we have to evaluate $5^{-}1 \mod 37$

Evaluating the inverse As we see above, evaluating the inverse of a number in modular arithmetic requires Euclid's Algorithm. We must do the following operation:

$$37 = 7 * 5 + 2$$
$$5 = 2 * 2 + 1$$

Since the inverse of a number is that which when multiplied by the number produces one, we do the following:

$$1 = 5 - (2 * 2)$$

but since $2 = 37 - 5 * 7$, we can rewrite that as

$$\begin{aligned} & 1 \\ & = 5 - 2 * (37 - 7 * 5) \mod 37 \\ & = (15 * 5) - (2 * 37) \mod 37 \\ & => 5 * 14 = 1 \mod 37 \end{aligned}$$

Therefore, $5^{-}1 \mod 37 = 14$.

The Deciphering Function Now that we have $5^{-}1 \mod 37$, we can construct our deciphering function fully. Previously it was written as:

$$f_d = 5^{-}1(x - 5) \mod 37$$

Now that we know that $5^{-}1 \mod 37 = 14$, the function can be written as:

$$\begin{aligned} f_d = 14(x - 5) \mod 37 & \\ & = 14x - 70 \mod 37 \\ & = 14x - 33 \mod 37 \\ & = 14x + 4 \mod 37 \end{aligned}$$

(*For practicality, we change the -33 to a 4 as they are the same in mod*37*. However, in some cases where the negative value is sufficiently smaller than the positive, we can retain the negative value for ease of calculation.*)

Deciphering The Text Now that we have our deciphering function, deciphering the text is a simple matter of inputting values and corresponding the outputs to their values in the 37-letter alphabet. The question specifically asks to decipher the second word of the plain-text. Bearing in mind that a 0 in the cipher-text is a 'blank' or 'space' in plain-text, we can locate the second word. From there it is a mechanical process, but the following example will make it clear. I will also demonstrate how to check the value of the 'blank' key.

Demonstration of deciphering 6 is the first letter of the second word, so this will help to answer the question. $6 = 6$

$$\begin{aligned} f_d = 14x + 4 \mod 37 => f_d(6) &= 14 * 6 + 4 \mod 37 \\ &= 88 \mod 37 \\ &= 14 mod 37 \end{aligned}$$

14 in our 37-letter alphabet corresponds to 'F'. Therefore, the first letter is 'F'.

0 = Blank Blank = 36

$$\begin{aligned} f_e(36) &= 36(5) + 5 \mod 37 \\ &= 5(36 + 1) \mod 37 \\ &= 5 * (37) \mod 37 \\ &= 0 \mod 37 \end{aligned}$$

Thus any instance of 0 in the cipher-text represents a blank.

This is how you would approach answering a question of this nature. It ties in many of the key ideas seen in the other sections, and demonstrates the usefulness and applications of this area of mathematics.

Maths Project 1

Students: Greg Healy, Jeffrey Forde, Michael O'Malley, Matt Ruane
Workshop Group Tutor: Kirsten Pfeiffer

November 2020

1 Introduction

1.1 What is modular arithmetic?: The basics

$$\frac{A}{B} = Q, remainder, R$$

$$A = Dividend$$
$$B = Divisor$$
$$Q = Quotient$$
$$R = Remainder$$

- Here's an example of how to do some basic Modular Arithmetic!

$$\frac{13}{5} = 2Mod(remainder)3$$

- It helps to visualise this particular type of math, with the help of a clock!:

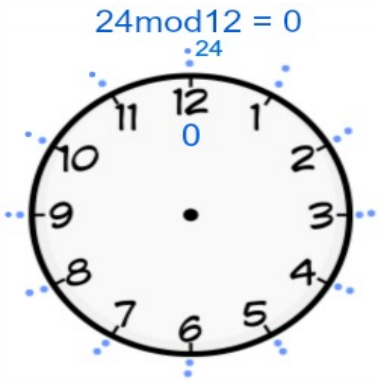


Figure 1: A picture speaks a thousand words!

1.2 Examples:

- Observe what happens when we increment numbers by one and then divide them by 3

$$\frac{0}{3} = 0$$

remainder 0

$$\frac{1}{3} = 0$$

remainder 1

$$\frac{2}{3} = 0$$

remainder 2

$$\frac{3}{3} = 1$$

remainder 0

$$\frac{4}{3} = 1$$

remainder 1

$$\frac{5}{3} = 1$$

remainder 2

$$\frac{6}{3} = 2$$

remainder 0

- The remainder start at 0 and increase by 1 each time until the number reaches one less than the number we are dividing. After that, the sequence repeats.
- By noticing this, we can visualise the modulo operator by using circles.
- We write 0 at the top of a circle and continuing clockwise integers 1,2,... up to one less than the modulus.
- For example, a clock with the 12 replaced by a 0 would be a circle for a modulus of 12.

1.3 Finding the inverse

- A number multiplied by its inverse is equal to 1. From basic Arithmetic, we know that:

  The inverse of a number A is

  $$\frac{1}{A}$$

  since

  $$A * \frac{1}{A} = 1$$

  All real numbers other than 0 have an inverse!

  Multiplying a number by $A^{-}1$ is the same as dividing by A

- How do we find the Modular Inverse? In modular Arithmetic, we do not have division as you are used to! However, we do have modular inverses.
- The modular inverse of A (mod C) is $A^{-^{1}}$

- Also:

$$(A * A^{-}1) = 1(modC)$$

or equivalently

$$(a^{-}1)modC = 1$$

- Only the numbers co-prime to C (Numbers that share no prime with C) have a modular inverse (mod C)‘

1.4 The Euclidean Algorithm

Step 1: Calculate A*B mod C for B values 0 through
3*0=0 (Mod 7)
3*1=3 (Mod 7)
3*2=6 (Mod 7)
3*3=9=2 (Mod 7)
3*4=12=5 (Mod 7)
3*5=15=1 (Mod 7)
(WE HAVE FOUND THE INVERSE)

Step 2: The modular inverse of A mod C is the B value that makes A*B mod C = 1 5 is the modular inverse of 3 mod 7 since 5*3 mod 7 = 1
Its not that hard, right?!

- Conclusion:

  If we have A mod B and we increase A by a multiple of B, we will end up in the same spot, i.e.

  For Example:

  $3 \bmod 10 = 3$
  $13 \bmod 10 = 3$
  $23 \bmod 10 = 3$
  $33 \bmod 10 = 3$

2 The history of enciphering

2.1 Nazi Ciphers

The infamous Nazi Enigma Machine is a famous encryption machine used by the German during the WW2 to transmit encrypted messages. An enigma machine allows for exactly
158,962,555,217,826,360,000

different ways to encode a message, which made it incredibly difficult for other nations to crack the German codes during the second world war. The Germans thought they had invented an unbreakable code. But the allies were determined to crack the code and win the war. If they could figure out how, they would gain invaluable intelligence that would save countless lives.

2.2 Alan Turing

Alan Turing, a mathematician and cryptographer from the 20th Century, who, along with other researchers, exploited a few weaknesses in the implementation of the enigma code and gains access to the German codebooks.
This allowed them to design a machine called a **Bombe Machine**, which helped to crack the most challenging versions of the Enigma. Some historians believe that the cracking of the Enigma code was the single most important victory by the allies.
Thanks to Alan Turing and his associates, the allies were able to decipher the Nazis codes using mathematics and modular arithmetic.

3 Modern applications of modular arithmetic

Modular arithmetic is rooted in the deepest of mathematics, where it is the cornerstone of number theory. But it also has many practical applications. It is used to calculate check sums for international standard book numbers(ISBNs) and bank identifiers(Iban numbers) and to spot errors in them. Modular arithmetic also acts as the backbone for public key cryptography systems, which are the life line of modern commerce.

Figure 2: Modular arithmetic allows banks to have unique and secure sorting system for bank accounts

Figure 3: It also allows book publishers to create unique identities for each publication, with built in authenticity verification

Without the deep understanding of modular arithmetic, modern commerce, for example, online shopping with the use of PayPal and end to end encryption, would simply flop. It is rooted in modern commerce and without it,it would feel like being in the dark ages

4 The problem

- We are given the following cipher text which was produced using an affine enciphering function:

$$f : Z_{37} \to Z_{37}, x \to \alpha x + \beta$$

- It is on single message units over a 37-letter alphabet.

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A = 10, B = 11 \ldots Z = 35, \_ = 36$$

- Where underscore represents a blank.
- The cipher text is as follows:

$$2G106I4E7Y04I2G14I2LSLI90119027TL9B0HIY$$
$$02G106I2G1T0E604EX1T0EX1T90SE4J72L9B$$

- We are given that the last nine characters of plain text are: COMPUTING
- We have to find the second word of the plain text.

5 Enciphering

5.1 What we found so far

- A 37-letter alphabet is used.
- An affine cryptosystem is used:

$$y \to \alpha x + \beta$$

- Given the last nine characters of plain text. Therefore, we can work out what letters they correspond to in the cipher text, as shown below:

$$SE4J72L9B$$
$$COMPUTING$$

5.2 What we need to find

- The enciphering key.

5.3 Finding the enciphering key

- We now sub in different values for x and y and solve them simultaneously.
- In this solution I have picked M and U as my variable y. Therefore, the corresponding x variables are 4 and 7.
- Subbing into the equation we get the following two equations:

$$C \to \alpha M + \beta = 4$$
$$U \to \alpha U + \beta = 7$$

- We now change M and U into their corresponding letters on the 37-letter alphabet and we get:

$$22\alpha + \beta = 4$$
$$30\alpha + \beta = 7$$

- Now we solve them:

$$\begin{aligned} 30\alpha + \beta &= 7 \\ -22\alpha - \beta &= 4 \\ 8\alpha &= 3 \\ \alpha &= 3(8)^{-}1 mod 37 \end{aligned}$$

Euclidean algorithm

- To simplify matters, we must use the euclidean algorithm to solve for 8^{-1}

$$\begin{aligned} 37 &= 4(8) + 5 \\ 8 &= 1(5) + 3 \\ 5 &= 1(3) + 2 \\ 3 &= 1(2) + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 1(2) \\ &= 3 - 1(5 - 1(3)) \\ &= 2(3) - 5 \\ &= 2(8 - 5) - 5 \\ &= 2(8) - 3(5) \\ &= 2(8) - 3(37 - 4(8)) \\ &= 14(8) - 3(37) \\ &= 14(8) - 3(0) \\ &= 14(8) \end{aligned}$$

- Now we must substitute 14 in for 8^{-1}

$$\begin{aligned} &14(3) mod 37 \\ &42 mod 37 \\ &5 mod 37 \end{aligned}$$

- Therefore: $\alpha = 5$
- Now we substitute 5 in for σ in one of the two original equations and solve for β:

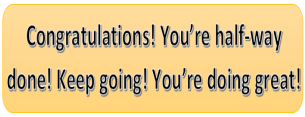
$$\begin{aligned} 30(5) + \beta &= 3 \\ 150 + \beta &= 3 \\ \beta &= -147 \\ \beta &= 5 \end{aligned}$$

- Therefore, the enciphering key is (5,5)

6 Deciphering

6.1 What we found so far

The enciphering function: $(5)x + 5$
The enciphering keys: $(5, 5)$



6.2 What we need to find

- The deciphering function: $ax + b$

6.3 Finding the deciphering function

- To find the deciphering function, it is helpful to think of the following analogy:

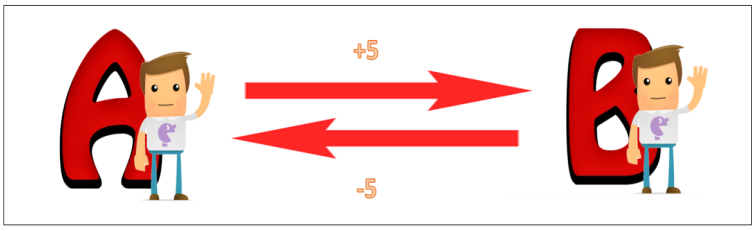


Figure 4: Jim had to take 5 steps forward to get from point A to point B. Therefore, Jim has to take 5 steps backward to get from point B to point A. Similarly:

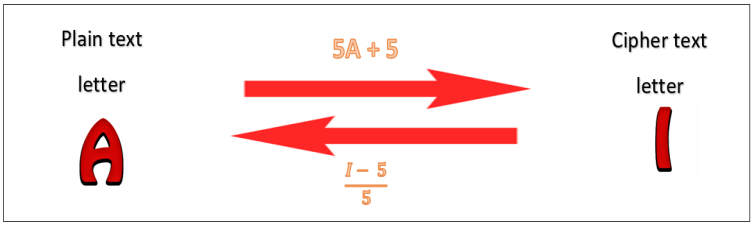


Figure 5: A had to multiply by 5 and add 5 to it's product to become I. Therefore, I has to subtract 5 and divide 5 into it's difference to become A.

Therefore:

$$x \xrightarrow{5x+5} \delta$$

$$x \xleftarrow{\frac{\delta-5}{5}} \delta$$

Euclidean algorithm

- To simplify matters, we must use the euclidean algorithm to solve for 5^{-1}

$$37 = 7 * 5 + 2$$
$$5 = 2 * 2 + 1$$

$$1 = 5 - (2 * 2)$$
$$1 = 5 - 2(37 - 7 * 5)$$
$$1 = 5 - 2(0 - 7 * 5)$$
$$1 = 15 * 5$$

$$5^{-1} = 15 mod 37$$

- Now we must substitute 15 in for 5^{-1}

$$15(x - 5)$$
$$15x - 75 mod 37$$
$$15x - 1 mod 37$$
$$15x + 36 mod 37$$

We now found the deciphering function, $15x + 36 mod 37$, and thereby, the deciphering keys $(15, 36)$

6.4 Reverting the cipher text back to plain text

- Follow the following steps on the table from left to right in order to unveil the hidden message that laid within the cipher text:

cipher text	cipher text value	$5(x) + 36$	sum ÷ 37	sum - (37 * quotient)	Plain text
2	2	66	1 + r	29	T
G	16	276	7 + r	17	H
1	1	51	1 + r	14	E
0	0	36	-	-	
6	6	126	3 + r	15	F
I	18	306	8 + r	10	A
4	4	96	2 + r	22	M
E	14	246	6 + r	24	O
7	7	141	3 + r	30	U
Y	34	546	14 + r	28	S
0	-	-	-	-	

Table 1: The deciphering process

- You have officially learned how to decipher a cipher text. Practice using the deciphering function by completing the rest of the message.