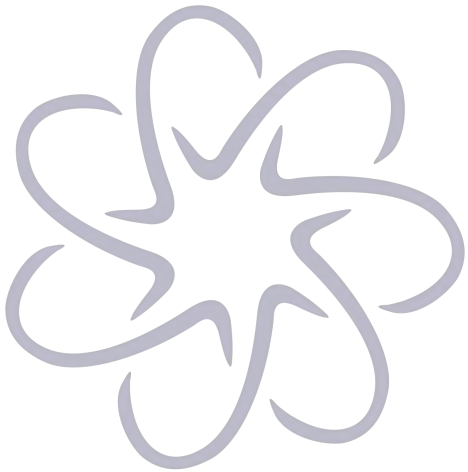
UNSW Mathematics Society Presents
MATH2400 Workshop



Presented by Jordan Russo and Gerald Huang

Overview I

Overview II

1. Integers and the Natural Numbers

Commutative ring

Let R be a non-empty set with addition $(+)$ and multiplication $(\cdot)$. Then R is a *commutative ring* if the following axioms hold, for all $a, b, c \in R$.

(I) (**Closure**) $a + b \in R$, $a \cdot b \in R$.

(II) (**Associativity**) $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(III) (**Distributivity**) $a \cdot (b + c) = a \cdot b + a \cdot c$.

(IV) (**Commutativity**) $a + b = b + a$, $a \cdot b = b \cdot a$.

(V) (**Additive identity**) There is an element $0 \in R$ such that $0 + a = a$ for all $a \in R$.

(VI) (**Additive inverse**) For every $a \in R$, there is an element $x \in R$ such that $a + x = 0$. We denote x as $-a$.

Field

A *field* $\mathbb{F}$ is a **commutative ring** with the multiplicative identity 1, where all non-zero elements have a *multiplicative inverse*.

To show that $\mathbb{F}$ is a field, we show:

$\mathbb{F}$ is a commutative ring,

$\mathbb{F}$ has the multiplicative identity 1,

Every non-zero element $a \in \mathbb{F}$, there is an element $b \in \mathbb{F}$ such that

$$a \cdot b = 1.$$

Field

(2018, Semester 2) Q1 i) c) and (2017, Semester 2) Q1 v)

Is $\mathbb{Z}_{15}$ a field?

We need to check to see whether every **non-zero** element in $\mathbb{Z}_{15}$ has a multiplicative inverse. We can do this by setting up a table, disregarding the 0 element.

$\times$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	**1**	2	3	4	5	6	7	8	9	10	11	12	13	14
2	2	4	6	8	10	12	14	**1**	3	5	7	9	11	13
3	3	6	9	12	0	3	6	9	12	0	3	6	9	12

Since $3 \neq 0$ and 3 does not have a multiplicative inverse, then $\mathbb{Z}_{15}$ is **NOT** a field.

Field

(2016, Semester 2) Q1 vii)

Show that $\mathbb{Z}_8$ is not a field.

You can show that the elements 2 and 4 have no multiplicative inverse.

$\times$	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
4	4	0	4	0	4	0	4

In fact, $\mathbb{Z}_p$ is a field if and only if p is prime! For example, $\mathbb{Z}_2$ is a field but $\mathbb{Z}_4$ is not!

An important result!

Let $\mathbb{F}$ be a field and suppose that $a, b \in \mathbb{F}$. If $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Divisibility

You've come cross divisibility in primary and high school; we're going to make it a bit more rigorous!

Let a and b be integers with $a \neq 0$. We say that $a \mid b$ if there exists an integer k such that $b = ka$. We say that a *divides* b.

Some special properties of divisibility:

(Reflexivity) $a \mid a$ for all $a \neq 0$.

(Anti-symmetry) If $a \mid b$ and $b \mid a$, then $b = \pm a$.

(Transitivity) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(Linear combination) If $a \mid b$ and $a \mid c$, then $a \mid kb + \ell c$ for any integers k, ℓ.

We prove the **anti-symmetry** property.

Divisibility

(2016, Semester 2) Q1 i)

Define what it means to say that for two integers a and b, a divides b. Prove that if $a \mid b$ and $b \mid a$, then $a = \pm b$.

We say that $a \mid b$ if there is an integer k such that

$$b = ka.$$

Using this definition, let k and m be integers such that

$$b = ka, \quad a = mb.$$

Then substituting one expression into another, we have

$$b = k(mb) = (km)b.$$

(2016, Semester 2) Q1 i)

Define what it means to say that for two integers a and b, a divides b. Prove that if $a \mid b$ and $b \mid a$, then $a = \pm b$.

Rewriting the expression we found gives us

$$b - (km)b = 0 \implies b(1 - km) = 0.$$

So either $b = 0$ or $km = 1$. If $b = 0$, then a is necessarily 0 and we are done. If $km = 1$, then either $k = m = 1$ or $k = m = -1$ since $k, m \in \mathbb{Z}$. This proves that $a = b$ for $k = m = 1$ or $a = -b$ for $k = m = -1$ which implies that $a = \pm b$.

(2019, Term 2) Q1 i)

Prove that if $a \mid b$ and $b \mid (a+c)$, then $a \mid c$.

Suppose that $a \mid b$ and $b \mid (a+c)$. Then there exist integers $k, m \in \mathbb{Z}$ such that

$$b = ka, \quad (a+c) = mb.$$

Substituting the expression of b gives

$$(a+c) = m(ka) = (mk)a \implies c = (mk)a - a = (mk-1)a.$$

Since $m, k \in \mathbb{Z}$, then $mk - 1 \in \mathbb{Z}$. Hence $a \mid c$.

Greatest common divisor

Suppose that d divides both a and b. We say that d is the **greatest common divisor** of a and b if and only if $c \leq d$ for all c where $c \mid a$ and $c \mid b$.

In other words, $d = \gcd(a, b)$ only when

$d \mid a$ and $d \mid b$,

If $c \mid a$ and $c \mid b$, then $c \leq d$.

Greatest common divisor

(2016, Semester 2) Q1 ii)

Let m be the product of all the **primes** between 10 and 20 and let n be the product of all the **integers** between 30 and 40 (inclusive). Find $\gcd(m, n)$.

We shall find the primes between 10 and 20 that appear in the prime factorisation of integers from 30 and 40. We see that

- 11 appears in the prime factorisation of 33: $33 = 11 \times 3$.
- 13 appears in the prime factorisation of 39: $39 = 13 \times 3$.
- 17 appears in the prime factorisation of 34: $34 = 17 \times 2$.
- 19 appears in the prime factorisation of 38: $38 = 19 \times 2$.

So $\gcd(m, n) = 11 \times 13 \times 17 \times 19$.

Greatest common divisor

(2017, Semester 2) Q1 i) d)

Find the greatest common divisor of 6^5 and 15^3.

Tip: Find the prime factorisation of both numbers!

We get

$$6 = 2 \times 3 \implies 6^5 = 2^5 \times 3^5,$$
$$15 = 3 \times 5 \implies 15^3 = 3^3 \times 5^3.$$

Then the greatest common divisor is the number that is common to both factorisations. Hence, $\gcd(6^5, 15^3) = 3^3 = 27$.

Greatest common divisor

Two integers, m and n, are said to be ***relatively prime*** if

$$\gcd(m, n) = 1.$$

Greatest common divisor

(2019, Term 2) Q1 i) c)

Show that $28^6 \cdot 6^5$ and $12^5 \cdot 15^3 \cdot 11 + 7$ are relatively prime.

***Tip**: Look at the prime factorisation of the left number and make a contradiction argument.*

For the sake of a contradiction, suppose that $28^6 \cdot 6^5$ and $12^5 \cdot 15^3 \cdot 11 + 7$ were **not** relatively prime. We look at the (unique) prime factors of $28^6 \cdot 6^5$. This is easy to compute and we have

$$28^6 \cdot 6^5 = \left(2^{12} \times 7^6\right) \cdot \left(2^5 \times 3^5\right) = 2^{17} \times 3^5 \times 7^6.$$

So at least one of $2, 3$ or 7 must appear in the right number.

It's easy to see that

$12^5 \cdot 15^3 \cdot 11$ does not share a common prime factor with 7.

So if a divides $12^5 \cdot 15^3 \cdot 11 + 7$, and it divides either $12^5 \cdot 15^3 \cdot 11$ or 7, then it must divide the other part as well. But

2 does not divide 7;

3 does not divide 7;

7 does not divide $12^5 \cdot 15^3 \cdot 11$.

So neither of these prime factors will appear in the prime factorisation of $12^5 \cdot 15^3 \cdot 11 + 7$ and thus, no combination of powers of 2, 3 or 7 can appear in the factorisation either. Thus, the greatest common divisor is 1.

The Euclidean Algorithm

The **Euclidean Algorithm** is a simple algorithm to find the greatest common divisor of two integers. You don't need to know the in's and out's of the algorithm, just know how to use it.

(General strategy)

- Write the bigger number as a quotient of the smaller number and a remainder.
- Repeat the process by writing the smaller number as a quotient of the original remainder and a new remainder.
- Repeat the previous steps until the remainder is 0.

Bézout's identity

The greatest common divisor can always be written as a linear combination of the two numbers.
Bézout's identity states:

Let m, n be integers (not both zero) and let $x, y \in \mathbb{Z}$. Then,

$$\gcd(m, n) = mx + ny.$$

However, if $c = mx + ny$, then c is **not(!!!)** necessarily $\gcd(m, n)$. In fact, if $c = mx + ny$, then $\gcd(m, n) \mid c$. If $c = 1$, then $\gcd(m, n) = 1$ since $\gcd(m, n) > 0$ and the only integers that divide 1 is ± 1.

Prime numbers

A **prime number** is a number $p > 1$ that is divisible by 1 and itself – so it has two factors exactly. As such, we typically do not declare 1 as a prime number.

(Strategies for questions regarding prime numbers)

- The only **even** prime p is $p = 2$. Every other prime is odd.
- For $p > 3$, p is congruent to 1 or 5 in mod 6.
- (**Fundamental Theorem of Arithmetic**) Any positive integer is a (unique up to reordering) factorisation of powers of primes.

For primes p and integers a, b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Prime numbers

(2021, Term 2 – Test 1) Q1 iii)

Find all prime numbers p such that $p+17$ is also a prime number.

- **Method 1**: If p is prime then $p \geq 2$ and importantly $p+17 > 3$. If $p+17$ is also prime then it must be an odd prime. Note that $p+17$ is odd if and only if p is even. But the only even prime is $p = 2$.
- **Method 2**: For a prime $p > 3$, p is congruent to either 1 or 5 in modulo 6. If $p \equiv 1 \pmod 6$, then write $p = 6k+1$ for some integer k. Then $p+17 = (6k+1)+17 = 6(k+3)$. This can never be prime since 6 is a composite factor. If $p \equiv 5 \pmod 6$, then write $p = 6m+5$ for some integer k. Then $p+17 = (6k+5)+17 = 2(3k+11)$. This is prime if and only if $3k+11 = 1$. But this implies that $k = -10/3$ which is not an integer. Thus, this can never happen. And so, no prime $p > 3$ works. It remains to check $p = 2$ and $p = 3$ and only $p = 2$ works.

Fundamental Theorem of Arithmetic

Every positive integer can be **uniquely** represented as a product of one or more primes.

We can extend this to negative integers by adding -1 into the product.

A harder question!!

(2021, Term 2 – Test 1) Q2 iii)

What is $\gcd(2n+1, 2n(n+1))$ for an integer n?

We show that

$$\gcd(2n+1, 2) = \gcd(2n+1, n) = \gcd(2n+1, n+1) = 1.$$

Since 2 is even and prime, then no odd number can divide 2, so $\gcd(2n+1, 2) = 1$. For $\gcd(2n+1, n)$, note that

$$\gcd(2n+1, n) = \gcd(2n+1-n, n) = \gcd(n+1, n) = 1.$$

For $\gcd(2n+1, n+1)$, note that

$$\gcd(2n+1, n+1) = \gcd(2n+1-(n+1), n+1) = \gcd(n, n+1) = 1.$$

(2021, Term 2 – Test 1) Q2 iii)

What is $\gcd(2n+1, 2n(n+1))$ for an integer n?

Hence, we see that

$$\begin{aligned}\gcd(2n+1, 2n(n+1)) &= \gcd(2n+1, n(n+1)) \\ &= \gcd(2n+1, n+1) \\ &= 1.\end{aligned}$$

2. Representation of Numbers

Base b representation

We can represent a number from base 10 to a number in base b. In base b, we can represent a number N as

$$N = \underbrace{a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + a_{n-2} \cdot b^{n-2} + \cdots + a_0 \cdot b^0}_{\text{integer part}} + \underbrace{a_{-1} \cdot b^{-1} + a_{-2} \cdot b^{-2} + \cdots + a_{-m} \cdot b^{-m}}_{\text{fractional part}}.$$

We can write this number as

$$N = (a_n a_{n-1} a_{n-2} \ldots a_0 . a_{-1} a_{-2} \ldots a_{-m})_b \,,$$

which is just a concatenation of *digits* in base b.

Converting from base m to base n

Base b Algorithm (integer)

Input: N, some number in base m.

Algorithm: Start by splitting the number into its integer and fractional part.

For the integer part,

(I) Set $a = \lfloor N \rfloor$ (the integer part of N).

(II)

$$\begin{aligned} a &= q_1 \cdot n + a_0, \\ q_1 &= q_2 \cdot n + a_1, \\ &\dots \\ q_k &= 0 \cdot n + a_k. \end{aligned}$$

Output: $a = (a_k a_{k-1} \dots a_1 a_0)_n$.

Converting from base m to base n

Base b Algorithm (fractional)

For the fractional part,

(I) Set $x = \{N\} = N - \lfloor N \rfloor$ (the fractional part of N).

(II) Find the highest power of m smaller than x. Then compute the remainder.

(III) Now take the remainder to be the new x and repeat steps (I) and (II).

(IV) Terminate when $x = 0$ or when you have seen x before in your calculations.

You will have an expression written in terms of power of m.

Converting from base m to base n

(General strategies for fractional parts)

If a/b is periodic in base 10 (like 1/3 and 2/3), then you should also expect it to periodic in other bases too. If this is the case:

- See if you can write the remainder as a multiple of your original number.
- This tells you what the period is in the expansion.

(2016, Semester 2) Q1 iv)

Write $\frac{1}{3}$ in base 2.

Applying the Euclidean algorithm, we see that (finding the highest powers of 2 smaller than the remainder):

$$\begin{aligned}\frac{1}{3} &= \frac{1}{2^2} + \frac{1}{12} \\ &= \frac{1}{2^2} + \frac{1}{3} \cdot \frac{1}{4}.\end{aligned}$$

This means that we will have the same procedure with the same number but every digit will be shifted by 2 to the right. So we will have

$$\frac{1}{3} = (0.\overline{01})_2.$$

(2018, Semester 2) Q1 iii)

Write 3/5 in base 2.

Repeat the same idea as before: we find the highest power of 2 smaller than 3/5; we get

$$\begin{aligned}\frac{3}{5} &= 1 \times \frac{1}{2} + \frac{1}{10};\\ \frac{1}{10} &= 1 \times \frac{1}{2^4} + \frac{3}{80}\\ &= 1 \times \frac{1}{2^4} + \frac{3}{5} \cdot \frac{1}{2^4}.\end{aligned}$$

This means that we will have a period of 4 starting from the 4th power of the expansion. So we have

$$\frac{3}{5} = (0.\overline{1001})_2.$$

(2021, Term 2 – Test 1) Q2

Write $7\frac{2}{3}$ in base 4.

Split the number into its integer and fractional parts. For the integer part, we can write $7 = 1 \times 4 + 3 \times 4^0$ so $7 = (13)_4$.

For the fractional part, find the biggest power of 4 smaller than $\frac{2}{3}$.

$$\begin{aligned}\frac{2}{3} &= 2 \times \frac{1}{4} + \frac{1}{6} \\ &= 2 \times \frac{1}{4} + \frac{1}{4} \times \frac{2}{3}.\end{aligned}$$

This means that we will have a period of 1 starting from the 1st power of the expansion. So we will have

$$\frac{2}{3} = (0.\overline{2})_4$$

(2021, Term 2 – Test 1) Q2

Write $7\frac{2}{3}$ in base 4.

So we have

$$7\frac{2}{3} = (13)_4 + (0.\overline{2})_4 = (13.\overline{2})_4.$$

(2021, Term 2 – Test 1) Q2 ii)

Write $(12.0\overline{21})_7$ as a rational fraction a/b in base 10.

Split the number up into its integer and fractional parts.

$$(12.0\overline{21})_7 = (12)_7 + (0.0\overline{21})_7.$$

For the integer part, we can write the expression as

$$1 \times 7^1 + 2 \times 7^0 = 9.$$

For the fractional part, expand the periodic part into a geometric series:

$$(0.0\overline{21})_7 = 0 \times \frac{1}{7} + \left(2 \times \frac{1}{7^2} + 2 \times \frac{1}{7^4} + \dots\right) + \left(1 \times \frac{1}{7^3} + 1 \times \frac{1}{7^5} + \dots\right).$$

(2021, Term 2 – Test 1) Q2 ii)

Write $(12.0\overline{21})_7$ as a rational fraction a/b in base 10.

So we have

$$\begin{aligned}
(0.0\overline{21})_7 &= 0 \times \frac{1}{7} + \left(2 \times \frac{1}{7^2} + 2 \times \frac{1}{7^4} + \dots\right) + \left(1 \times \frac{1}{7^3} + 1 \times \frac{1}{7^5} + \dots\right) \\
&= \frac{2}{7^2}\left(1 + \frac{1}{7^2} + \frac{1}{7^4} + \dots\right) + \frac{1}{7^3}\left(1 + \frac{1}{7^2} + \frac{1}{7^4} + \dots\right) \\
&= \frac{2}{7^2}\left(\frac{1}{1 - \frac{1}{7^2}}\right) + \frac{1}{7^3}\left(\frac{1}{1 - \frac{1}{7^2}}\right) \\
&= \frac{2}{7^2}\left(\frac{7^2}{48}\right) + \frac{1}{7^3}\left(\frac{7^2}{48}\right) = \frac{2}{48} + \frac{1}{7 \times 48} \\
&= \frac{15}{336} \\
&= \frac{5}{112}.
\end{aligned}$$

(2021, Term 2 – Test 1) Q2 ii)

Write $(12.0\overline{21})_7$ as a rational fraction a/b in base 10.

To recap:

(I) We split $(12.0\overline{21})_7$ into $(12)_7 + (0.0\overline{21})_7$.

(II) We found:

$$(12)_7 = 9, \quad (0.0\overline{21})_7 = \frac{5}{112}.$$

(III) So we have

$$(12.0\overline{21})_7 = 9 + \frac{5}{112} = \frac{1013}{112}.$$

Converting to and from base m^2

If we know the expansion of a number in base m, then we can easily find the expansion in base m^2.

General strategy

Group the digits in blocks of 2's from right to left and convert the blocks of 2 digits into the respective digit in base m^2.

If we know the expansion of a number in base m^2, then we can also convert it to a number in base m.

General strategy

Take each digit in base m^2 and rewrite it in base m in blocks of 2's. Then concatenate all of them in the same order.

(2019, Term 2) Q1 ii)

(a) Write 153 in base 3.

(b) Using your calculations for part (a), write the above number in base 9.

(a) By the Euclidean algorithm,

$$\begin{aligned} 153 &= 1 \cdot 3^4 + 72, \\ 72 &= 2 \cdot 3^3 + 18, \\ 18 &= 2 \cdot 3^2 + 0. \end{aligned}$$

So

$$153 = 3^4 + 2 \cdot 3^3 + 2 \cdot 3^2 = (12200)_3.$$

(2019, Term 2) Q1 ii)

(a) Write 153 in base 3.

(b) Using your calculations for part (a), write the above number in base 9.

(b) Let's remind ourselves that

$$153 = (12200)_3.$$

To convert from base 3 to base 9, we group two digits at a time from right to left:

$$\underbrace{01}\,\underbrace{22}\,\underbrace{00}.$$

We add an additional 0 to group up all of the digits into groups of two.
We see that

$$(01)_3 = (1)_9, \quad (22)_3 = (8)_9, \quad (00)_3 = (0)_9.$$

In other words,

$$153 = (12200)_3 = (180)_9.$$

(2018, Semester 2) Q1 ii)

(a) Write 327 in base 9.

(b) Using your calculations for part (a), write the above number in base 3.

(a) Similar to the previous part, by the Euclidean algorithm,

$$327 = 4 \cdot 9^2 + 3,$$
$$3 = 3 \cdot 9^0 + 0.$$

So

$$327 = (403)_9.$$

(2018, Semester 2) Q1 ii)

(a) Write 327 in base 9.

(b) Using your calculations for part (a), write the above number in base 3.

(b) From the computation from part (a), split each digit and convert them into two digits in base 3. For example, 4 is 11 in base 3. So we have

$$(4)_9 = (11)_3, \quad (0)_9 = (00)_3, \quad (3)_9 = (10)_3.$$

So we have

$$327 = (403)_9 = (110010)_3.$$

(2017, Semester 2) Q1 iv)

(a) Write 375 in base 2.

(b) Using your calculations for part (a), write the above number in base 4.

(a) **Answer**: $375 = (101110111)_2$.

(b) From the right to the left, group each digit in pairs to get

$$\underbrace{01}\,\underbrace{01}\,\underbrace{11}\,\underbrace{01}\,\underbrace{11}.$$

Then write each pair of digits in base 4. We get

$$(01)_2 = 1, \quad (11)_2 = 3.$$

Then concatenate each of them in the same order:

$$375 = (101110111)_2 = (11313)_4.$$

Base 2 representation – GCD in Binary

Let m, n be positive integers (in base 2).

(i) if m and n are both even, then $\gcd(m, n) = 2 \cdot \gcd(m/2, n/2)$;

(ii) if m and n are both odd (with $m > n$), then $\gcd(m, n) = \gcd(m - n, n)$;

(iii) if one of m and n is even (assume m is), then $\gcd(m, n) = \gcd(m/2, n)$;

(iv) if $m = n$, then $\gcd(m, n) = m$.

Continued fractions

Another way to represent a number is by its **continued fraction** representation. A continued fraction is of the form

$$N = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}} = [a_1; a_2, a_3, a_4, \dots].$$

Some notes on continued fractions:

- If a continued fraction terminates, then it is rational.
- If a continued fraction is periodic, then it is irrational. We denote the period by a bar at the top: $[a_1; \overline{a_2, a_3}]$ denotes that the continued fraction is periodic by a_2 and a_3.

Finding continued fractions I

Continued fraction → number

If N is in *continued fraction* form, then expand out the continued fraction and solve from bottom up. Combine two fractions together and keep simplifying it until you get to the top.

If N is periodic, start by solving for the periodic part and then re-combine for the final answer.

Finding continued fractions II

Number → continued fraction – Continued fraction algorithm

Input: N, some number.

Algorithm:

(I) Set $a_1 = \lfloor N \rfloor$ and set $r_1 = N - a_1$.

(II) Reciprocate r_1 to get $\dfrac{1}{r_1}$.

(III) If we've already seen $\dfrac{1}{r_1}$, then we have a period and we can terminate the algorithm early; otherwise, set $a_2 = \left\lfloor \dfrac{1}{r_1} \right\rfloor$ and repeat steps (I) and (II) with a_2 and r_1.

(IV) Terminate if the numerator hits 1 and include the denominator as the last digit of the continued fraction representation.

Output: $N = [a_1; a_2, a_3, \ldots, a_n]$.

Continued fractions – Number → CF

(2016, Semester 2) Q1 iv)

Define the Golden Ratio and find its continued fraction expansion.

Let φ be the golden ratio. The value of φ is

$$\varphi = \frac{1+\sqrt{5}}{2}.$$

We begin to find the continued fraction representation.

(I) Let $a_1 = \lfloor \varphi \rfloor = 1$. Then write

$$r_1 = \varphi - a_1 = \frac{1+\sqrt{5}}{2} - 1 = \frac{-1+\sqrt{5}}{2}.$$

(II) Reciprocate r_1 to get

$$\frac{1}{r_1} = \frac{2}{-1+\sqrt{5}} = -\frac{2(-1-\sqrt{5})}{4} = \frac{1+\sqrt{5}}{2}.$$

(III) We've already seen this so our continued fraction terminates with a period of 1. If we don't see something we've already seen before, then we repeat step (I) with $a_2 = \left\lfloor \frac{1}{r_1} \right\rfloor$.

(IV) Output $\varphi = [a_1; \overline{a_1}] = [1; \overline{1}]$.

Continued fractions

(2019, Term 2) Q1 iv)

(a) Expand 147/32 into a continued fraction.

(b) Compute the value of the periodic continued fraction $[0; 2, \overline{2, 1}]$ where $\overline{**}$ means a periodic repetition of $**$.

(2019, Term 2) Q1 iv)

Expand 147/32 into a continued fraction.

(I) Let $a_1 = \lfloor 147/32 \rfloor = 4$. Then write

$$r_1 = 147/32 - a_1 = \frac{147 - 128}{32} = \frac{19}{32}.$$

(II) Reciprocate r_1 to get $\frac{1}{r_1} = \frac{32}{19}$.

(III) Repeat steps (I) and (II) with $a_2 = \lfloor 1/r_1 \rfloor = 1$. Then write

$$r_2 = \frac{1}{r_1} - a_2 = \frac{32 - 19}{19} = \frac{13}{19}.$$

(IV) Reciprocate r_2 to get $\frac{1}{r_2} = \frac{19}{13}$.

(2019, Term 2) Q1 iv)

Expand 147/32 into a continued fraction.

(V) Repeat steps (I) and (II) with $a_3 = \lfloor 1/r_2 \rfloor = 1$. Then write

$$r_3 = \frac{1}{r_2} - a_3 = \frac{19 - 13}{13} = \frac{6}{13}.$$

(VI) Reciprocate r_3 to get $\dfrac{1}{r_3} = \dfrac{13}{6}$.

(VII) Repeat steps (I) and (II) with $a_4 = \lfloor 1/r_3 \rfloor = 2$. Then write

$$r_4 = \frac{1}{r_3} - a_4 = \frac{13 - 12}{6} = \frac{1}{6}.$$

(VIII) Since the numerator is 1, we terminate our algorithm with $a_5 = 6$. Output

$$147/32 = [a_1; a_2, a_3, a_4, a_5] = [4; 1, 1, 2, 6].$$

(2019, Term 2) Q1 iv)

Compute the value of the periodic continued fraction $[0; 2, \overline{2, 1}]$ where $\overline{**}$ means a periodic repetition of $**$.

(I) We can begin by dealing with the periodic part first. Let $x = [0; \overline{2, 1}]$. Then we have

$$x = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \ddots}}}} = \cfrac{1}{2 + \cfrac{1}{1+x}}.$$

We can solve for x:

$$\begin{aligned} x &= \cfrac{1}{2 + \cfrac{1}{1+x}} \\ &= \cfrac{1}{\cfrac{2(1+x)+1}{1+x}} \\ &= \frac{1+x}{3+2x}. \end{aligned}$$

(2019, Term 2) Q1 iv)

Compute the value of the periodic continued fraction $[0; 2, \overline{2, 1}]$ where $\overline{**}$ means a periodic repetition of $**$.

Continuing from the previous slide, we have

$$\begin{aligned} x = \frac{1+x}{3+2x} &\implies x(3+2x) = 1+x, \\ &\implies 2x^2 + 2x - 1 = 0, \\ &\implies x = \frac{-2 \pm \sqrt{12}}{4} = \frac{-1 \pm \sqrt{3}}{2}. \end{aligned}$$

Since $x > 0$, we take $x = \dfrac{-1+\sqrt{3}}{2}$.

(2019, Term 2) Q1 iv)

Compute the value of the periodic continued fraction $[0; 2, \overline{2, 1}]$ where $\overline{**}$ means a periodic repetition of $**$.

(II) Now, we can compute the actual value. Set $L = [0; 2, \overline{2, 1}]$. Then we have

$$L = 0 + \frac{1}{2 + x} = \frac{1}{2 + \frac{-1+\sqrt{3}}{2}} = \frac{2}{3 + \sqrt{3}} = \frac{3 - \sqrt{3}}{3}.$$

So we have

$$[0; 2, \overline{2, 1}] = \frac{3 - \sqrt{3}}{3}.$$

3. Modular arithmetic

The Congruence Relation

For $a, n \in \mathbb{Z}, a \; mod \; n$ is the remainder (in $\mathbb{N}$) obtained when a is divided by n, that is, r, if

$$a = nq + r, \quad \text{where } 0 \leq r < n.$$

We say that integers a and b are *congruent modulo* n (or a is *congruent* to b modulo n), and write $a \equiv b (\text{mod } n)$ iff $n|(a - b)$, iff $\exists k \in \mathbb{Z}$ such that $a = b + kn$.

The Congruence Relation

Suppose $a \equiv b \ (mod\ n)$ and $c \equiv d \ (mod\ n)$. Then

- $(a + c) \equiv (b + d) \ (mod\ n)$
- $ac \equiv bd \ (mod\ n)$
- $a^m \equiv b^m \ (mod\ n)$ for all $m \in \mathbb{N}$.

The Congruence Relation

The congruence relation is an equivalence relation on $\mathbb{Z}$.

1) $a \sim a$
2) $a \sim b \implies b \sim a$
3) $a \sim b$ and $b \sim c \implies a \sim c$

Thus, $\mathbb{Z}$ is partitioned into equivalence classes $\{[a] \mid 0 \leq a < n\}$.

The Congruence Relation

The set of integers modulo n

With the natural definition of addition and multiplication, $\mathbb{Z}_n$ is a commutative ring with identity (1).

1) Closure under addition
2) Associative under addition
3) Commutative under addition
4) Existence of an additive identity (0)
5) Existence of additive inverses
6) Closure under multiplication
7) Associative under multiplication
8) Distributive under multiplication
9) **Commutative under multiplication**
10) **Existence of multiplicative identity (1).**

(2021, Term 2 - Tutorial Chapter 3) Q3 c)

By working modulo 3, show that $2^{2^n} + 5$ is always composite for every positive integer n.

(2021, Term 2 - Tutorial Chapter 3) Q3 c)

By working modulo 3, show that $2^{2^n} + 5$ is always composite for every positive integer n.

Observe that $2 \equiv -1 \pmod 3$. Raising both sides to the power of 2^n, we have

$$2^{2^n} \equiv (-1)^{2^n} \pmod 3.$$

Since 2^n is even, then $(-1)^{2^n} = 1$. In other words, we have

$$2^{2^n} \equiv 1 \pmod 3.$$

Adding 5 to both sides give us

$$2^{2^n} + 5 \equiv 1 \pmod 3 + 5 \equiv 0 \pmod 3.$$

In other words, we have $2^{2^n} + 5 = 3k$ for some integer k. But $2^{2^n} > 0$ which implies that $2^{2^n} + 5 > 3$ and so $k > 1$. This implies that $2^{2^n} + 5$ will always have a factor of 3 which means that it is composite for all n.

Inverses in $\mathbb{Z}_n$

A non-zero a in $\mathbb{Z}_n$ has an inverse iff gcd(a,n)=1.

In general, if $ab = ac \ (mod\ n)$, you cannot in general conclude that $b \equiv c \ (mod\ n)$ even if $a \not\equiv 0 \ (mod\ n)$.

Inverses in $\mathbb{Z}_n$

The commutative ring $\mathbb{Z}_n$ is a field iff n is a prime.

From the previous slide, we can see that is n is a prime, the all the elements of $\mathbb{Z}_n$ have an inverse element. This property in combination with those inherited from $\mathbb{Z}_n$ being a commutative ring with identity implies that the set along with the usual definitions of addition and multiplication is in fact a field.

Groups

Definition of a group

Let G be a non-empty set whose elements satisfy the following five rules:

1) Closure under the group operation
2) Associative under the group operation
3) **Commutative under the group operation (Abelian)**
4) Existence of an identity element
5) Existence of element inverses

The set $\mathbb{Z}_n$ forms a commutative group under the operation of addition (identity is 0) but not under multiplication.

Common tests for divisibility

- A number is divisible by 2 iff its last digit is divisible by 2.
- A number is divisible by 4 iff the last two digits form a number which is divisible by 4.
- A number is divisible by 5^a iff its last a digits are divisible by 5^a.
- A number is divisible by 9 or 3 iff the sum of its digits is divisible by 9 or 3 respectively.
- Double the last digit and subtract it from the remaining truncated number. If the result is divisible but 7, then so was the original number.

Divisibility Tests

(2021, Term 2 - Tutorial Chapter 3) Q16

Test the number 7689627 for divisibility by 9, 11, 13 and 17.

Divisibility Tests

(2021, Term 2 - Tutorial Chapter 3) Q16

Test the number 7689627 for divisibility by 9, 11, 13 and 17.

First we will test divisibility by 9 (mostly because it's easiest).

$$7 + 6 + 8 + 9 + 6 + 2 + 7 = 45$$

Since $9 \mid 45$, then $9 \mid 7689627$.
Now we will test divisibility by 11 using the alternate sum test.

$$7 - 6 + 8 - 9 + 6 - 2 + 7 = 11$$

Since $11 \mid 11$, then $11 \mid 7689627$.
Testing divisibility by 13 and 17 will require some deeper thinking.

Divisibility Tests

(2021, Term 2 - Tutorial Chapter 3) Q16

Test the number 7689627 for divisibility by 9, 11, 13 and 17.

Note that $1000 \equiv -1 \ (mod\ n)$. So, we can apply a similar alternating sum test to 11 except we now need to group 3 digits at a time starting from the right.

$$7 - 689 + 627 = -55 \equiv 10 \ (mod\ n)$$

Since $13 \nmid 45$, then $13 \nmid 7689627$.

For 17, we need to pull a few more tricks out of the bag.

Divisibility Tests

(2021, Term 2 - Tutorial Chapter 3) Q16

Test the number 7689627 for divisibility by 9, 11, 13 and 17.

Let's begin by trying to develop a method similar to the test for divisibility by 7. Subtract a multiple y of the number's last digit b from the remaining number $\frac{n-b}{10}$ and assume we're successful in obtaining a multiple of 17 $(17x)$ where $x, y, b, n \in \mathbb{Z}^+$.

$$\begin{aligned} 17x &= \frac{n-b}{10} - yb \\ 170x &= n - b - 10yb \\ n &= 170x + (10y+1)b \\ n &= 17\left(10x + \left(\frac{10y+1}{17}\right)b\right) \end{aligned}$$

(2021, Term 2 - Tutorial Chapter 3) Q16

Test the number 7689627 for divisibility by 9, 11, 13 and 17.

$$n = 17\left(10x + \left(\frac{10y+1}{17}\right)b\right)$$

So, we can see that if we make the right choice of y and the new number is divisible by 17, so is the original. Since n is an integer, we need to choose y such that this remains true in our expression.

$$y = 1: \quad \frac{10y+1}{17} = \frac{11}{17} \notin \mathbb{Z}^+$$
$$y = 2: \quad \frac{10y+1}{17} = \frac{21}{17} \notin \mathbb{Z}^+$$

Divisibility Tests

(2021, Term 2 - Tutorial Chapter 3) Q16

Test the number 7689627 for divisibility by 9, 11, 13 and 17.

$$n = 17\left(10x + \left(\frac{10y+1}{17}\right)b\right)$$

$$\begin{aligned} y = 1: &\quad \frac{10y+1}{17} = \frac{11}{17} \notin \mathbb{Z}^+ \\ y = 2: &\quad \frac{10y+1}{17} = \frac{21}{17} \notin \mathbb{Z}^+ \\ &\quad \vdots \\ y = 5: &\quad \frac{10y+1}{17} = \frac{51}{17} = 3 \in \mathbb{Z}^+ \end{aligned}$$

(2021, Term 2 - Tutorial Chapter 3) Q16

Test the number 7689627 for divisibility by 9, 11, 13 and 17.

So using $y = 5$:

$$\begin{aligned} 768962 - 5(7) &= 768927 \\ 76892 - 5(7) &= 76857 \\ 7685 - 5(7) &= 7650 \\ 765 - 5(0) &= 765 \\ 76 - 5(5) &= 51 = 3(17) \end{aligned}$$

Hence, by working backwards through the sequence, $17 \mid 7689627$.

Linear Congruence Equations

The simplest congruence problems are *linear congruences.*

$$ax \equiv b \ (mod \ n)$$

These are easy to solve over $\mathbb{Q}$ but much more interesting to solve them over $\mathbb{Z}_n$.

Linear Congruence Equations

Suppose n is a positive integer and $d = gcd(a, n)$.

(i) Then the equation $ax \equiv b \ (mod\ n)$ has a solution iff $d \mid b$.

(ii) Moreover, if $d \mid b$ and $a = da', n = dn', b = db'$, then it has d solutions which are all residues $(mod\ n)$ congruent to the unique solution to $a'x \equiv b' \ (mod\ n')$

This theorem is really important to remember as you'd hate to waste time in an exam trying to solve a linear congruence only to get to the end and realise it doesn't have a solution.

Linear Diophantine Equations

What is a Diophantine equation?

A Diophantine equation is an equation where we seek only **integer** solutions. Assuming $a, b, b \in \mathbb{Z}$, if there is one unknown ($ax = b$) then an integer solution exists iff $a \mid b$/ Suppose then that there are two unknowns, thus we seek to solve $ax + by = c$.

Important to note that the equation $ax + by = c$, where $a, b, c \in \mathbb{Z}$ has a solution in $\mathbb{Z}$ iff $d \mid c$, where $d = gcd(a, b)$. **Why do we know this to be true?**

Linear Diophantine Equations

(2016, Semester 2) Q1 iii)

Find all integers x and y with

$$4x + 5y = 18.$$

How many of the solutions lie in the positive quadrant?

Linear Diophantine Equations

(2016, Semester 2) Q1 iii)

Find all integers x and y with

$$4x + 5y = 18.$$

How many of the solutions lie in the positive quadrant?

We need to consider a modulus that is going to isolate one of the variables and I like to look at the one with the smallest coefficient first.

$$\begin{aligned} 4x + 5y &\equiv 18 \ (mod\ 5) \\ 4x &\equiv 3 \ (mod\ 5) \\ 16x &\equiv 12 \ (mod\ 5) \\ \therefore x &\equiv 2 \ (mod\ 5) \end{aligned}$$

Linear Diophantine Equations

(2016, Semester 2) Q1 iii)

Find all integers x and y with

$$4x + 5y = 18.$$

How many of the solutions lie in the positive quadrant?

Now that we know $x = 2 + 5t$ for some $t \in \mathbb{Z}$, let's substitute this back into the original equation.

$$\begin{aligned} 4(2 + 5t) + 5y &= 18 \\ 8 + 20t + 5y &= 18 \\ 5y &= 10 - 20t \\ y &= 2 - 4t \end{aligned}$$

(2016, Semester 2) Q1 iii)

Find all integers x and y with

$$4x + 5y = 18.$$

How many of the solutions lie in the positive quadrant?

To figure out how many solutions lie in the positive quadrant, we will restrict our expressions for x and y to be strictly positive and find the corresponding values for t.

$$\begin{aligned} 2 + 5t &> 0 \\ t &> \frac{-2}{5} \geq 0 \end{aligned}$$

Linear Diophantine Equations

(2016, Semester 2) Q1 iii)

Find all integers x and y with

$$4x + 5y = 18.$$

How many of the solutions lie in the positive quadrant?

$$\begin{aligned} 2 - 4t &> 0 \\ t &< \frac{1}{2} \leq 0 \end{aligned}$$

Thus, there is only one solution in the positive quadrant at $t = 0$ which is $(x, y) = (2, 2)$. (This can also be seen intuitively by looking at the previous result)

The Chinese Remainder Theorem

CRT Definition

Suppose $n_1, n_2, ..., n_k \in \mathbb{N}$ with $gcd(n_i, n_j) = 1$ for each $i.j$ with $1 \leq i < j \leq k$. Then there is a **unique solution** modulo $n = n_1 n_2 ... n_k$ to the simultaneous equations

$$x \equiv a_1 \ (mod \ n_1)$$
$$x \equiv a_2 \ (mod \ n_2)$$
$$...$$
$$x \equiv a_k \ (mod \ n_k)$$

The Chinese Remainder Theorem

CRT Algorithm

Assume $gcd(n_i, n_j) - 1,\ 1 \leq i < j \leq k$.

i Let $n = n_1 n_2 ... n_k$.

ii For each i define $m_i = n/n_i$ and the defined y_i solving the congurence $m_i y_i \equiv 1\ (mod\ n_i)$.

iii Compute and output $x \equiv a_1 m_1 y_1 + ... + a_k m_k y_k\ (mod\ n)$.

4. Powers and roots

Fermat's Little Theorem

Suppose that p is prime. Then *any* integer a satisfies the property:

$$a^p \equiv a \pmod{p}.$$

Additionally, if a is not divisible by p, then a satisfies the property:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Euler's φ function

Define $\varphi(n)$ to count the number of **relatively prime** integers smaller than n.

(Some properties of φ)

- If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.
- Let $p_1, p_2, \ldots, p_k$ be the **unique** prime factors of n. Then

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

- If n is prime, then $\varphi(n) = n - 1$.

(2021, Term 2 – Sample Test 2C) Q2 iii)

Let p be an odd prime. Find another integer n such that $\varphi(n) = \varphi(p)$.

Since p is an **odd** prime, then every integer smaller than p is relatively prime to p. In other words, $\gcd(m, p) = 1$ for every $1 \leq m < p$. So if $m < p$, then we have that

$$\varphi(m \cdot p) = \varphi(m)\varphi(p).$$

We now use the fact that 2 is prime. But since 2 is prime, then $\varphi(2) = 2 - 1 = 1$. In other words, we have

$$\varphi(2p) = \varphi(2)\varphi(p) = \varphi(p).$$

It suffices to choose $n = 2p$.

(2021, Term 2 – Test 2) Q2 iii)

Show that there are infinitely many positive integers n such that $10 \mid \varphi(n)$.

Method 1: We claim that $n = 5^\alpha \cdot 2^\beta$ for $\alpha, \beta \geq 2$ satisfy the condition. By its alternative definition, we have that

$$\begin{aligned}\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right) &= 5^\alpha \cdot 2^\beta \left(1-\frac{1}{5}\right)\left(1-\frac{1}{2}\right) \\ &= 5^\alpha \cdot 2^\beta \left(\frac{4}{5}\right)\left(\frac{1}{2}\right) \\ &= 5^{\alpha-1} \cdot 2^{\beta-1} \cdot 4 = 10\left(5^{\alpha-2} \cdot 2^{\beta-2} \cdot 4\right).\end{aligned}$$

As long as $\alpha, \beta \geq 2$, then $5^{\alpha-2} \cdot 2^{\beta-2} \cdot 4$ is an integer which implies that 10 divides $\varphi(n)$. Since α and β can be made arbitrarily, there are infinitely many n's to choose.

(2021, Term 2 – Test 2) Q2 iii)

Show that there are infinitely many positive integers n such that $10 \mid \varphi(n)$.

Method 2: Since $\varphi(11) = 11 - 1 = 10$, then pick $n = 11p$ where p is a prime and $p \neq 11$ since

$$\varphi(11p) = \varphi(11)\varphi(p) = 10(p-1).$$

Since there are infinitely many primes, then there are infinitely many positive choices for n such that $10 \mid \varphi(n)$.

Euler's theorem

We begin to generalise Fermat's Little Theorem.

Euler's theorem

Let a, n be integers such that $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Fermat's Little Theorem is realised when $n = p$ is prime since we have

$$a^{\varphi(p)} \equiv 1 \pmod{p} \iff a^{p-1} \equiv 1 \pmod{p}.$$

We can use this to greatly reduce the number of computations to find powers.

(2021, Term 2 – Test 2) Q2 i)

Use Euler's theorem to show that $37^{23} \equiv 37^{-1} \pmod{52}$.

Since $\gcd(37, 52) = 1$, by Euler's theorem, $37^{\varphi(52)} \equiv 1 \pmod{52}$. Since $52 = 2 \times 3 \times 13$, then we have

$$\varphi(52) = \varphi(6 \cdot 13) = \varphi(6)\varphi(13) = \varphi(2)\varphi(3)\varphi(13) = 24.$$

Thus,

$$37^{24} \equiv 1 \pmod{52}.$$

So we have

$$37^{23} = 37^{24-1} = 37^{24} \cdot 37^{-1} \equiv 1 \cdot 37^{-1} \pmod{52} \equiv 37^{-1} \pmod{52}.$$

Primitive roots

Order of an element

The **order** an element a (in $\mathbb{Z}_n$) is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Units of $\mathbb{Z}_n$

The units of a ring $\mathbb{Z}_n$ are the elements that have a multiplicative inverse – these are elements with the property $\gcd(a, n) = 1$.
The set of units $\mathbb{Z}_n^*$ form a group under multiplication and $|\mathbb{Z}_n^*| = \varphi(n)$.

A **primitive element** of $\mathbb{Z}_n$ is an element whose order is $\varphi(n)$.

Testing for primitiveness

To check whether a number a is primitive in $\mathbb{Z}_n$, compute the algorithm:

(I) Factor out $n-1$ into a product of primes.

(II) For each *unique prime* q_i in the factorisation of $n-1$, check that $a^{(n-1)/q_i} \not\equiv 1 \pmod{n}$.

(III) If this is true, then a is a primitive root/element in $\mathbb{Z}_n$.

(2017, Semester 2) Q2 ii)

Let $N = 1237$. You are given that $N - 1 = 2^2 \cdot 3 \cdot 103$ and the following table of values:

q	2	5	103
$2^{\frac{N-1}{q}} \mod N$	1236	300	385
$3^{\frac{N-1}{q}} \mod N$	1	300	768
$7^{\frac{N-1}{q}} \mod N$	1236	300	635

Which of the numbers 2, 3 and 7 are primitive elements in $\mathbb{Z}_{1237}^*$? Give brief reasons.

(I) Factor $N - 1$. They have given us the factorised form: $N - 1 = 2^2 \cdot 3 \cdot 103$.

(II) For each *distinct prime* q_i, check that $a^{\frac{N-1}{q_i}} \not\equiv 1 \mod N$. We see that 3 cannot be a primitive element since $3^{\frac{N-1}{2}} \equiv 1 \pmod N$.

(2017, Semester 2) Q2 ii)

Let $N = 1237$. You are given that $N - 1 = 2^2 \cdot 3 \cdot 103$ and the following table of values:

q	2	5	103
$2^{\frac{N-1}{q}} \mod N$	1236	300	385
$3^{\frac{N-1}{q}} \mod N$	1	300	768
$7^{\frac{N-1}{q}} \mod N$	1236	300	635

Which of the numbers 2, 3 and 7 are primitive elements in $\mathbb{Z}_{1237}^*$? Give brief reasons.

(III) Output: 2 and 7 are primitive elements.

Classification of primitive roots

We begin to classify the existence of primitive roots in an arbitrary modulo n ring.

Primitive roots $\mod n$ exist if and only if n is in one of the following forms:

(I) $n = 1, 2$, or 4;

(II) $n = p^k$ for an odd prime p and nonnegative integer k;

(III) $n = 2p^k$ for an odd prime p and nonnegative integer k.

Classification of primitive roots

(2021, Term 2 – Sample Test 2B) Q2 iii)

What is the largest integer $n \leq 57$ such that $\mathbb{Z}_n^*$ has a primitive root?

We look at the possible values of n in one of the forms:

- $n = 1, 2, 4$;
- $n = p^k$ for odd primes p;
- $n = 2p^k$ for odd primes p.

The biggest prime smaller than 57 is $n = 53$. It remains to check values $n = 54, 55, 56, 57$. For $n = 54$, we see that $n = 2 \times 27 = 2 \cdot 3^3$. So $n = 54$ also has a primitive root. We see that $n = 55 = 5 \times 11$ so $\mathbb{Z}_{55}^*$ will have no primitive roots. For $n = 56 = 2 \times 28$, 28 is not a power of an odd prime so $\mathbb{Z}_{56}^*$ does not have a primitive root. Similarly, $n = 57 = 3 \times 19$ won't have a primitive root either. So $n = 54$ is the largest possible integer.

Optional harder questions

(2018, Semester 2) Q2 iv)

Find all integers $n \geq 1$ for which the Euler function $\varphi(n)$ is odd. You must prove your answer.

Recall that

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

So any even number bigger than 2 will force $\varphi(n)$ to be even. Also, since any prime $p > 2$ is odd, then $\varphi(p) = p - 1$, they will also be even. We now look to composite odd integers. Since they are composite, then they can be written as a product of odd primes (by the Fundamental Theorem of Arithmetic).

Write $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, where p_i is an odd prime in the factorisation. Then we have that

$$\begin{aligned}\varphi(n) &= n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{m} \left(\frac{p_i - 1}{p_i}\right) \\ &= p_1^{k_1 - 1} p_2^{k_2 - 1} \dots p_m^{k_m - 1} (p_1 - 1)(p_2 - 1) \dots (p_m - 1).\end{aligned}$$

Since p_i is an odd prime, then $p_i - 1$ must be even. So any odd integer $n > 3$ will produce an even $\varphi(n)$. The only integers n such that $\varphi(n)$ is odd is $n = 1$ (if we define $\varphi(1) = 1$) and $n = 2$ since $\varphi(2) = 2 - 1 = 1$.

(2017, Semester 2) Q2 iii)

Let r be the smallest positive quadratic non-residue modulo $p \geq 3$ that is, the smallest positive integer r for which the congruence $x^2 \equiv r \pmod{p}$ has **no** solution. Prove that r is a prime number.

5. Cryptography and Coding Theory

Cryptography

- Encode messages;
- Decode messages;
- Correct encoded messages.

Encoding and decoding messages

Idea: Find an encoding and decoding system. If we encode a message and decode the encoded message, we should receive the same message.

$$E : x \mapsto x^7 \pmod{26} \implies D : x \mapsto x^7 \pmod{26}.$$

We look at two particular cryptographic systems:

- Error-correcting codes,
- RSA.

Error-correcting codes

Codes that can correct (and detect) errors.

Hamming $(7, 4)$ code

The standard Hamming $(7, 4)$ code uses the following matrix:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Start with the original message (a, b, c, d) and encode as (x, y, a, z, b, c, d).

Information rate: $\dfrac{\#\text{ bits in original message}}{\#\text{ bits in encoded message}} = \dfrac{4}{7}$.

Hamming $(7, 4)$ code

When do we have an error?

$\mathbf{c}$ is a codeword of $H\mathbf{c}$ if

$$H\mathbf{c} = \mathbf{0}.$$

An error occurs if $H\mathbf{c} \neq \mathbf{0}$.

The result tells us what column the error occurs.

(2016, Semester 2) Q2 iii)

The standard $(7, 4)$ Hamming code uses the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A message (a, b, c, d) is encoded as (x, y, a, z, b, c, d).

(a) What is the information rate of this code?

(b) Using the scheme above, encode $(0, 0, 1, 1)$.

(c) Correct any error and decode $(0, 1, 0, 0, 1, 1, 1)$, assuming at most once error.

(2016, Semester 2) Q2 iii)

The standard $(7, 4)$ Hamming code uses the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A message (a, b, c, d) is encoded as (x, y, a, z, b, c, d).

(a) What is the information rate of this code?

(b) Using the scheme above, encode $(0, 0, 1, 1)$.

(a) The information rate is $\dfrac{\#\text{ bits in the original message}}{\#\text{ bits in the encoded message}} = \dfrac{4}{7}$.

(b) The encoded message would look like $(x, y, 0, z, 0, 1, 1)$. We just need to find x, y, z.

If $\mathbf{c}$ is a codeword, then we require that $H\mathbf{c} = \mathbf{0}$. This gives us

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 0 \\ z \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} z \\ y \\ x+1 \end{pmatrix}.$$

For this to be a codeword, we require that $z = 0$, $y = 0$, $x + 1 = 0$. This gives us: $z = y = 0$ and $x = 1$ (since we're working in modulo 2). Encode it as

$$\mathbf{c} = (1, 0, 0, 0, 0, 1, 1).$$

(2016, Semester 2) Q2 iii)

The standard $(7, 4)$ Hamming code uses the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A message (a, b, c, d) is encoded as (x, y, a, z, b, c, d).

(c) Correct any error and decode $(0, 1, 0, 0, 1, 1, 1)$, assuming at most once error.

To decode it, check to see if $H\mathbf{c} = \mathbf{0}$.

We get

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0+0+0+0+1+1+1 \\ 0+1+0+0+0+1+1 \\ 0+0+0+0+0+1+0+1 \end{pmatrix}.$$

Simplifying the expression in modulo 2, we get $H\mathbf{c} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$. So there *is* an error and the error is in the 6th column. We decode as $(a, b, c, d) = (0, 1, 0, 1)$.

(2017, Semester 2) Q2 iv)

The standard $(7, 4)$ Hamming code uses the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A message (a, b, c, d) is encoded by $\mathbf{c} = (x, y, a, z, b, c, d)$.

(a) Explain how the ith column of H is constructed.

(b) What is the information rate of this code?

(c) Using the scheme above, encode $(1, 0, 1, 1)$.

(d) Some binary message, (a, b, c, d), encoded as in above, is received as $(0, 1, 0, 0, 1, 1, 0)$. Do you think an error has occurred during the transmissions? Explain your reasons.

(2017, Semester 2) Q2 iv)

The standard $(7, 4)$ Hamming code uses the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A message (a, b, c, d) is encoded by $\mathbf{c} = (x, y, a, z, b, c, d)$.

(a) Explain how the ith column of H is constructed.

(b) What is the information rate of this code?

(a) The ith column of H is simply the binary representation of i with the third row representing the coefficient of 2^0, second row representing the coefficient of 2^1 and the first row representing the coefficient of 2^2.

(b) Original message has length 4 and the encoded message has length 7, so the information rate

$$I = \frac{4}{7}.$$

(2017, Semester 2) Q2 iv)

The standard $(7, 4)$ Hamming code uses the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A message (a, b, c, d) is encoded by $\mathbf{c} = (x, y, a, z, b, c, d)$.

(c) Using the scheme above, encode $(1, 0, 1, 1)$.

(d) Some binary message, (a, b, c, d), encoded as in above, is received as $(0, 1, 0, 0, 1, 1, 0)$. Do you think an error has occurred during the transmissions? Explain your reasons.

(c) The encoded word is (x, y, a, z, b, c, d) where $(a, b, c, d) = (1, 0, 1, 1)$. So we have $\mathbf{c} = (x, y, 1, z, 0, 1, 1)$. We solve $H\mathbf{c} = \mathbf{0}$.

We have

$$H\mathbf{c} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \\ z \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} z+1+1 \\ y+1+1+1 \\ x+1+1 \end{pmatrix}.$$

Remember that we're working in $\mathbb{Z}_2$ and we want $H\mathbf{c} = \mathbf{0}$. Hence,

$$\begin{pmatrix} z+2 \\ y+3 \\ x+2 \end{pmatrix} = \begin{pmatrix} z \\ y+1 \\ x \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

and so $z = 0, y = 1, x = 0$ and the encoded message is $\mathbf{c} = (0, 1, 1, 0, 0, 1, 1)$.

(d) We need to check to see whether $(0,1,0,0,1,1,0)$ has an error. To do this, we check that

$$H\mathbf{c} = \mathbf{0}.$$

Directly computing, we see that

$$H\mathbf{c} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+1 \\ 1+1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Hence, we see that $H\mathbf{c} \neq \mathbf{0}$. This tells us that there is an error. In particular, there is an error in the first value.

RSA code

RSA Code

Input: A message of length m which has no more than n digits.
Algorithm:

(I) Choose primes p, q large enough such that $N = pq > 10^n$.

(II) (**Encoding**) Compute $\varphi(N)$ and choose a power s such that $\gcd(s, \varphi(N)) = 1$.

(III) (**Decoding**) Find t such that

$$st \equiv 1 \pmod{\varphi(N)}.$$

$$E : m \mapsto m^s \pmod{N},$$
$$D : m \mapsto m^t \pmod{N}.$$

(2017, Semester 2) Q2 i)

(a) Compute $\varphi(323)$ (note that $323 = 17 \cdot 19$).

(b) Does the function $m \to m^{10} \mod 323$, sending a message m to the residue $m^{10} \pmod{323}$ give a valid RSA encryption?

(a) Since $323 = 17 \cdot 19$, then $\varphi(323) = \varphi(17 \cdot 19) = 16 \cdot 18 = 288$.

(b) Suitable encoding powers s are chosen such that $\gcd(s, \varphi(N)) = 1$ where $N = 323$ in this case. So we are trying to see whether $\gcd(10, 288) = 1$. But since they are both even, they both have a 2 in common, so we have $\gcd(10, 288) > 1$ and thus, 10 is not a suitable power.

(2016, Semester 2) Q2 i)

(a) Define Euler's phi function and find $\varphi(143)$.

(b) If an RSA code encodes messages with $m \mapsto m^7 \mod 143$, what is the decoding function?

(a) $\varphi(n)$ counts the number of integers smaller than n that are relatively prime to n. Since $143 = 11 \times 13$, then we have

$$\varphi(143) = \varphi(11 \cdot 13) = \varphi(11)\varphi(13) = 120.$$

(b) To decode, we find x such that $7x \equiv 1 \pmod{\varphi(143)} \equiv 1 \pmod{120}$. To find x, we find the inverse of 7 in modulo 120. The inverse of 7 is $x = 103$. So an appropriate decoding function is

$$D : m \mapsto m^{103} \pmod{143}.$$

(2019, Term 2) Q2 iii)

(i) Compute the Euler function $\varphi(323)$ (note that $323 = 17 \cdot 19$).

(ii) Find the smallest possible RSA exponent e so that encoding messages with $m \to m^e \mod 323$ gives a valid RSA encryption. What is the decoding function?

(iii) For the above choice of encoding, what is the decoding function which recovers the original message?

(i) Since $323 = 17 \cdot 19$, then $\varphi(323) = \varphi(17 \cdot 19) = 16 \cdot 18 = 288$.

(ii) Suitable values for the exponent are values e such that $\gcd(e, \varphi(323)) = 1$. To this end, we consider the prime factorisation of 288 which is $288 = 2^5 \cdot 3^2$

(2019, Term 2) Q2 iv)

An RSA code has been constructed using the modulus $M = pq$ which is a product of two primes p and q of the form $p = 2^k + 3$ and $q = 2^n + 1$ with positive integers k and n. Design a strategy to use this information to break this scheme. Explain it on the example $M = 33667$.

Key idea: We need to find a way to be able to find p and q using only the information that the public would know – the value of M. Since we know that $p = 2^k + 3$ and $q = 2^n + 1$, then

$$M = (2^k+3)(2^n+1) = 2^{k+n} + 2^k + 3 \cdot 2^n + 3 = 2^{k+n} + 2^k + 2^{n+1} + 2^n + 3,$$

in binary form. So if we know the binary expansion of M, then we can find the values of k and n for which we can find p and q and subsequently, crack the code.

We shall use $M = 33667$ as an example. Since we know that $M = pq$, then we know that $M = 33667 = 2^{15} + 2^9 + 2^8 + 2^7 + 3$. This means that

$$2^{k+n} + 2^k + 2^{n+1} + 2^n = 2^{15} + 2^9 + 2^8 + 2^7.$$

This tells us that $k + n = 15$. We can deduce that either $n = 8$ or $n = 7$. If $n = 7$, then $n + 1 = 8$ and $k = 9$. But then $k + n \neq 15$. If $n = 8$, then $n + 1 = 9$ and $k = 7$. And indeed, we have that $k + n = 7 + 8 = 15$. Hence, we have that $p = 2^k + 3 = 2^7 + 3$ and $q = 2^n + 1 = 2^8 + 1$ and that cracks the code since we now know the value of p and q.

6. Polynomials

Polynomial rings

We shall make some analogies.

	$\mathbb{Z}_n$	$R[x]$
Elements	$x \mod n$	Polynomials with coefficients in R
Identity	$x = 0$ (additive)	$p(x) = 0$ (additive)
	$x = 1$ (multiplicative)	$p(x) = 1$ (multiplicative)

Polynomial rings work in almost the same fashion as integer rings from Chapter 1!

Greatest common divisor

The **greatest common divisor** between two polynomials (say $f(x)$ and $g(x)$) is a polynomial that factors into both parts (common divisor) and any other factor polynomial $q(x)$ is a factor of the gcd. In other words,

Let $f(x), g(x) \in R[x]$ (not zero). The polynomial $d(x)$ is called the *greatest common divisor* if:

- $d(x) \mid f(x)$ and $d(x) \mid g(x)$ (**common divisor**),
- If $q(x) \mid f(x)$ and $q(x) \mid g(x)$, then $q(x) \mid d(x)$ (**greatest**).

If $d(x)$ is the greatest common divisor, then so is $\lambda \cdot d(x)$. This means that the greatest common divisor of polynomials is **not** unique (unlike the case of integers)!

(2016, Semester 2) Q2 iv)

Find a quadratic polynomial and a cubic polynomial in $\mathbb{Z}[x]$ whose greatest common divisor is x (and explain why the gcd is x).

We will construct these two polynomials. Let $f(x)$ be the quadratic polynomial and $g(x)$ be the cubic polynomial. Since the greatest common divisor is x, then clearly $x \mid f(x)$ and $x \mid g(x)$. So we can write $f(x) = x(ax + b)$ and $g(x) = x(cx^2 + dx + e)$. For there to be no more common factors, $ax + b \nmid cx^2 + dx + e$. There are infinitely many choices we can pick but the easiest choice is $a = 1$, $b = 1$, $c = 1$, $d = 1$, $e = 1$. Thus, we obtain the polynomials

$$f(x) = x^2 + x, \quad g(x) = x^3 + x^2 + x,$$

and this construction guarantees that $\gcd(f(x), g(x)) = x$. These polynomials are also in $\mathbb{Z}[x]$ since the coefficients are integers.

(2017, Semester 2) Q2 v)

Find a polynomial of degree 4 in $\mathbb{Z}[x]$ whose greatest common divisor with the polynomial $x^2(x+1)$ is $x(x+1)$ and prove your answer.

We will tackle this similar to how we tackled the previous question! We shall construct the polynomial. Let $f(x)$ be the degree 4 polynomial in $\mathbb{Z}[x]$. Since $x(x+1)$ is the greatest common divisor, then clearly $x(x+1) \mid f(x)$. So we can write $f(x) = x(x+1)(ax^2+bx+c)$. Since $x(x+1)$ is the *greatest common factor*, then we require that $x \nmid ax^2+bx+c$. Let $a=1$, $b=0$, $c=1$. Then we have

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

Irreducibility

Irreducibility in $F[x]$

A polynomial $p(x)$ in $F[x]$ is said to be *irreducible* if we cannot factor $p(x)$ into a product of polynomials of smaller degrees in $F[x]$.

A way to check whether a polynomial is irreducible in $F[x]$ is to use *Eisenstein's criterion.*

Eisenstein's criterion

Consider some polynomial

$$p(x) = \sum_{i=0}^{n} a_i x^i.$$

Suppose there is a prime number p which divides a_i for $i \neq n$ and p^2 does not divide a_0. If there is, then $p(x)$ is said to be *irreducible.*

Determining whether a polynomial is irreducible

Primitivity of polynomials

A polynomial is said to be *primitive* if the greatest common divisor of the coefficients is 1.

(**Technique 1**) If $p(x)$ is primitive of degree n and it is reducible, then it has a factor of degree $n/2$ or less.

(**Technique 2**) If $p \in \mathbb{Z}[x]$ and $p(r/s) = 0$ for integers r, s with $\gcd(r, s) = 1$, then $s \mid a_n$ and $r \mid a_0$.

(**Technique 3**) If $p(x)$ is irreducible, then so is $q(x) = p(x + a)$ (and vice versa).

Polynomial *fields*

Much like integers, we can define the notion of a polynomial *field*. In the integers case, $\mathbb{Z}_p$ is a field if and only if p is prime – but a prime number is just a number that is *irreducible* since it cannot be written as a product of two integers smaller than p. This works in the same vein with polynomials.

Polynomial field

We say that $F[x]/\langle f(x)\rangle$ is a polynomial *field* if and only if $f(x)$ is irreducible in $F[x]$.

Here, we say $F[x]/\langle f(x)\rangle$ to refer to the polynomial ring modulo $f(x)$.

Field of a elements

If $\mathbb{F} = \mathbb{Z}_n[x]/f(x)$ is a field (i.e. $f(x)$ is irreducible in $F[x]$), then it has $a = n^{\deg(f(x))}$ elements.

(2019, Term 2) Q3 iii)

Show that $f(x) = x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$ and explain why $\mathbb{F} = \mathbb{Z}_2[x]/f(x)$ is a field of 8 elements.

We show that $f(x)$ is irreducible in $\mathbb{Z}_2[x]$. Assume that $f(x)$ is reducible. Since $f(x)$ is primitive, then we can directly apply technique 1. This means that there is a linear factor of $f(x)$. The only possible linear factors in $\mathbb{Z}_2[x]$ are $\{x, x+1\}$. But we see that $f(0) = 1 \neq 0$ and $f(-1) = (-1)^3(-1) + 1 = -1 \neq 0$. Thus, $f(x)$ has no linear factors which means it has no factors. In other words, $f(x)$ is irreducible (think about why this implies it has no quadratic factors either). Since $f(x)$ is irreducible in $\mathbb{Z}_2[x]$, then $\mathbb{F} = \mathbb{Z}_2[x]/f(x)$ is a field. The elements in $\mathbb{F}$ are polynomials of degree 2 or less with coefficients in $\mathbb{Z}_2$. So the elements in $\mathbb{F}$ are

$$\mathbb{F} = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

(2018, Semester 2) Q3 ii)

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.
Prove that $\mathbb{F} = \mathbb{Z}_2[x]/f(x)$ is a field and find the number of elements in $\mathbb{F}$.

To prove that $\mathbb{F}$ is a field, we show that $f(x)$ is irreducible in $\mathbb{Z}_2[x]$. Suppose that $f(x)$ was reducible. Since $f(x)$ is primitive, we can apply technique 1. This means that $f(x)$ has linear factors. The only possible linear factors are $\{x, x+1\}$ and it's easy to check that none of them factor into $f(x)$. This implies that $f(x)$ has no linear factors which imply that $f(x)$ also has no quadratic factors. Thus, $f(x)$ is irreducible. This implies that $\mathbb{F} = \mathbb{Z}_2[x]/f(x)$ is a field with $2^{\deg(f(x))} = 2^3 = 8$ elements.

(2016, Semester 2) Q3 i) and ii)

Let $m_1(x) = x^4 + x + 1$ in $\mathbb{Z}_2[x]$, $F = \mathbb{Z}_2[x]/\langle m_1(x)\rangle$. Also let $m_3(x) = x^4 + x^3 + x^2 + x + 1$.

(i) Are $m_1(x)$ and $m_3(x)$ irreducible? Prove your answer.

(ii) State the number of elements in F.

Suppose that $m_1(x)$ is reducible. Since $m_1(x)$ is primitive, then apply technique 1. This tells us that $m_1(x)$ has a factor of degree 1 or 2. The possible linear factors are $\{x, x+1\}$. We can see that $m_1(x) = x(x^3+1)+1$ and $m_1(x) = x(x+1)(x^2+x+1)+1$. So none of the linear terms are factors. So there must be quadratic factors. The possible quadratic factors are $\{x^2, x^2+1, x^2+x, x^2+x+1\}$. From the previous working, we can see that x^2+x+1 cannot be a factor nor can x^2+x. So the possible factors must be either x^2 or x^2+1 (or both).

We have a few options.

x^2 is the **only** factor. Then we have that

$$m_1(x) = (x^2)^2 = x^4 \neq x^4 + x + 1.$$

So x^2 cannot be the **only** factor.

$x^2 + 1$ is the **only** factor. Then we have that

$$m_1(x) = (x^2 + 1)^2 = x^4 + 2x^2 + 1 = x^4 + 1 \neq x^4 + x + 1.$$

So $x^2 + 1$ cannot be the **only** factor.

x^2 and $x^2 + 1$ are the factors of $m_1(x)$. Then we have that

$$m_1(x) = x^2(x^2 + 1) = x^4 + x^2 \neq x^4 + x + 1.$$

So neither of these cases work which implies that there are no quadratic factors. But that contradicts the fact that $m_1(x)$ is reducible and primitive. Thus, $m_1(x)$ must be irreducible!

We now determine whether $m_3(x)$ is irreducible. Recall that

$$m_3(x) = x^4 + x^3 + x^2 + x + 1.$$

Now, since $m_3(x)$ is a geometric series, then we can write the expression as

$$m_3(x) = \frac{x^5 - 1}{x - 1}.$$

Set $g(x) = m_3(x + 1)$. Then

$$\begin{aligned} g(x) &= \frac{(x+1)^5 - 1}{(x+1) - 1} = \frac{\left(1 + \binom{5}{1}x + \binom{5}{2}x^2 + \binom{5}{3}x^3 + \binom{5}{4}x^4 + \binom{5}{5}x^5\right) - 1}{x} \\ &= \binom{5}{1} + \binom{5}{2}x + \binom{5}{3}x^2 + \binom{5}{4}x^3 + \binom{5}{5}x^4 \\ &= 5 + 10x + 10x^2 + 5x^3 + x^4. \end{aligned}$$

Apply **Eisenstein's criterion** with $p = 5$. We can see that p divides every coefficient except for the leading coefficient and p^2 does not divide the constant. Hence, by Eisenstein's criterion, $m_3(x)$ is irreducible.

(2016, Semester 2) Q3 ii)

(ii) Let $m_1(x) = x^4 + x + 1$ in $\mathbb{Z}_2[x]$, $F = \mathbb{Z}_2[x]/\langle m_1(x) \rangle$.
State the number of elements in F.

Since F is a field, then there are $2^4 = 16$ elements in F.

(MATH3711 – 2021, Term 1) Q2 ii)

Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x]/(x^3 + cx^2 + 1)$ is a field.

Remember that $\mathbb{Z}_n[x]/f(x)$ is a field if and only if $f(x)$ is irreducible in $\mathbb{Z}_n[x]$. Thus, we aim to find all possible $c \in \mathbb{Z}_3$ such that $x^3 + cx^2 + 1$ is irreducible in $\mathbb{Z}_3$. Since $\mathbb{Z}_3$ is relatively small, we just need to check whether which value of c makes $x^3 + cx^2 + 1$ irreducible. Obviously, we can write $x^3 + 1 = (x + 1)(x^2 - x + 1)$ and so $c = 0$ does not make $x^3 + cx^2 + 1$ irreducible. For $c = 1$, we have $f(x) = x^3 + x^2 + 1$. If $x = 1$, then we have that $f(1) = 1 + 1 + 1 = 0$ in $\mathbb{Z}_3$. Hence $x + 2$ is a factor and $f(x) = (x + 2)(x^2 + 2x + 2)$. For $c = 2$, we get that $f(x) = x^3 + 2x^2 + 1$. If $f(x)$ is reducible, then it has linear factors. However, checking $f(0)$, $f(1)$ and $f(2)$ verifies that there are no linear factors. This implies that $f(x)$ is irreducible. Hence, the only possible value of c that makes $\mathbb{Z}_3[x]/(x^3 + cx^2 + 1)$ a field is $c = 2$.

7. Finite fields and BCH codes

Finite fields

We saw an important result in the previous chapter:

$$m(x) \in F[x] \text{ is irreducible } \iff F[x]/\langle m(x)\rangle \text{ is a field.}$$

We use this idea to construct *finite fields*.

(Moore's theorem) Construction of finite fields

Every **finite field** is *isomorphic* to $\mathbb{Z}_p[x]/\langle m(x)\rangle$.

Finite fields can also interchangably be referred to as *Galois fields*, denoted by $\mathrm{GF}(q)$ or $\mathbb{F}_q$.

q denotes the number of elements in the finite field: $q = p^{\deg(m(x))}$.

$$\mathbb{F}_q \cong \mathbb{Z}_p[x]/\langle m(x)\rangle.$$

(Theorem) Order of *Finite fields*

Suppose that F is a finite field. Then $|F| = q = p^k$ for some prime p. The prime p is called the ***characteristic*** of F.

$\mathbb{Z}_2$ is a finite field of characteristic 2;

$\mathbb{Z}_4$ is **not** a finite field; however, a finite field of 4 elements exist with characteristic 2.

$\mathbb{Z}_{13}$ is a finite field of characteristic 13.

(Theorem) Order of elements in *finite fields*

If $\mathbb{F}_q$ is a field of q elements, then $\mathbb{F}_q^*$ has $q-1$ elements (we disregard the 0 element). Then the order of an element in $\mathbb{F}_q^*$ divides $q-1$.

(2020, Term 2) Q2 iv)

Which numbers in the following sequence $2, 7, 9, 12, 16, 19$ can be cardinalities of finite fields? Give reasons.

Every finite field is isomorphic to $\mathbb{Z}_p[x]/\langle f(x)\rangle$ where $f(x)$ is an irreducible polynomial in $\mathbb{Z}_p$. Thus, the only possible cardinalities of finite fields are powers of primes. So the possible cardinalities are

$$2 = 2^1,$$
$$7 = 7^1,$$
$$9 = 3^2,$$
$$16 = 4^2 = 2^4,$$
$$19 = 19^1.$$

(2018, Semester 2) Q3 iii)

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.

(i) Prove that $\mathbb{F} = \mathbb{Z}_2[x]/f(x)$ is a field and find the number of elements in $\mathbb{F}$.

(ii) What are the possible orders of elements in $\mathbb{F}^*$?

(i) Skipped. We covered this earlier.

(ii) Since $\mathbb{F}$ is a field of $2^3 = 8$ elements, then $\mathbb{F}^*$ has $8 - 1 = 7$ elements. The order of the elements must divide 7. So the possible orders are either 1 or 7.

We look at elements with order 7 (more specifically, order $q - 1$) more closely.

Primitive element and *minimal polynomials*

Primitive element

An element $\alpha \in \mathbb{F}_q$ is a ***primitive element*** of $\mathbb{F}_q$ if the order of α is $q-1$.

Minimal polynomial

Let $\alpha \in \mathbb{F}_q$. The ***minimal polynomial*** $m(x)$ of α is the monic polynomial of smallest degree such that $m(\alpha) = 0$.

If $m(x)$ is irreducible and $m(\alpha) = 0$, then $m(x)$ is the minimal polynomial of α.

(2021, Term 2) Tutorial Problem 8, Q6

Let α be a root of $x^3 + 2x + 1$ and $\mathbb{Z}_3(\alpha) = \mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle$.
Is α a primitive element of $\mathbb{Z}_3(\alpha)$? What are the possibilities for the orders of the elements of $\mathbb{Z}_3(\alpha)$?

Since α is a root of $x^3 + 2x + 1$, this means that $\alpha^3 + 2\alpha + 1 = 0$. Equivalently, this implies that

$$\alpha^3 = -2\alpha - 1 \iff \alpha^3 = \alpha + 2.$$

We can now begin to find powers of α. Since the orders of elements in $\mathbb{Z}_3(\alpha)$ must divide the order of $\mathbb{Z}_3(\alpha)$, we need to find the order of $\mathbb{Z}_3(\alpha)$ first. But this is a finite field of order $3^3 = 27$. Hence, orders of elements in $\mathbb{Z}_3(\alpha)$ must divide $q = 27 - 1 = 26$. We just need check α^2 and α^{13}. Clearly α^2 is just α^2.

We see that

$$\begin{aligned}
\alpha^{13} &= \left(\alpha^3\right)^4 \cdot \alpha = (\alpha+2)^4 \cdot \alpha \\
&= \left(\alpha^4 + 8\alpha^3 + 24\alpha^2 + 32\alpha + 16\right) \cdot \alpha \\
&= ((\alpha+2)\cdot\alpha + 2(\alpha+2) + 2\alpha + 1) \cdot \alpha \\
&= \left(\alpha^2 + 2\alpha + 2\alpha + 4 + 2\alpha + 1\right) \cdot \alpha \\
&= \left(\alpha^2 + 6\alpha + 5\right) \cdot \alpha \\
&= \left(\alpha^2 + 2\right) \cdot \alpha \\
&= \alpha^3 + 2\alpha = (\alpha+2) + 2\alpha = 2.
\end{aligned}$$

Since $\alpha^{13} \neq 1$, then 13 is not the order of α. This leaves the only power 26. We can check that it is indeed 1 by noticing that

$$\alpha^{26} = \left(\alpha^{13}\right)^2 = 2^2 = 4 = 1.$$

Thus, α is a primitive root. The possible orders are: $2, 13, 26$.

(2021, Term 2) Tutorial Problem 8, Q13

Suppose α is a root of $x^3 + x + 1$. Find the minimal polynomial in $\mathbb{Z}_2[x]$ of $\alpha^2 + \alpha$ and $\alpha^2 + \alpha + 1$.

Recall that the minimal polynomial is a **monic** polynomial of smallest degree for which β is a root. Since α is a root of $f(x) = x^3 + x + 1$, then we have that

$$f(\alpha) = 0 \iff \alpha^3 + \alpha + 1 = 0 \iff \alpha^3 = \alpha + 1.$$

We see that $\alpha^4 = \alpha^2 + \alpha$ and $\alpha^5 = \alpha^2 + \alpha + 1$ Let $\beta = \alpha^4$ and $\gamma = \alpha^5$. We now find powers of β and γ for which $g(\beta) = 0$ and $h(\gamma)$. We shall start with β. To do this, we construct a table of powers for α.

$$\begin{array}{l|l|l|l} \alpha^0 & 1 & \alpha^4 & \alpha^2+\alpha \\ \alpha^1 & \alpha & \alpha^5 & \alpha^2+\alpha+1 \\ \alpha^2 & \alpha^2 & \alpha^6 & \alpha^2+1 \\ \alpha^3 & \alpha+1 & \alpha^7 & 1 \end{array}$$

We now find powers of α^4 for which $g(\alpha^4) = 0$. This gives us the table of powers for β as

$$\begin{array}{l|l} \beta^0 & 1 \\ \beta^1 = \alpha^4 & \alpha^2+\alpha \\ \beta^2 = \alpha^8 & \alpha \\ \beta^3 = \alpha^{12} & \alpha^2+\alpha+1 \end{array}$$

We see that $\beta^3 + \beta + \beta^0 = (\alpha^2+\alpha+1) + (\alpha^2+\alpha) + 1 = 0$. So the minimal polynomial for $\beta = \alpha^2 + \alpha$ is the polynomial

$$g(x) = x^3 + x + 1.$$

Similarly, we construct the table of powers for $\gamma = \alpha^5$ to get

$$\begin{array}{l|l} \gamma^0 & 1 \\ \gamma^1 = \alpha^5 & \alpha^2 + \alpha + 1 \\ \gamma^2 = \alpha^{10} & \alpha + 1 \\ \gamma^3 = \alpha^{15} & \alpha \end{array}$$

We see that $\gamma^3 + \gamma^2 + 1 = \alpha + (\alpha + 1) + 1 = 0$. So the minimal polynomial for $\gamma = \alpha^2 + \alpha + 1$ is the polynomial

$$h(x) = x^3 + x^2 + 1.$$

(2017, Semester 2) Q3

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.

(i) Show that $f(x)$ is irreducible and explain why $\mathbb{F} = \mathbb{Z}_2[x]/\langle f(x) \rangle$ is a field.

(ii) Find the number of elements in $\mathbb{F}$.

(iii) Let $\alpha = x \pmod{f(x)}$ be the image of x in $\mathbb{F}$. Evaluate

- (a) $(1+\alpha)^{-1}$;
- (b) all powers α^m with $3 \leq m \leq 7$;
- (c) $(1+\alpha+\alpha^2)/(1+\alpha)$.

(iv)
- (a) Use the table computed in Question 3 iii b) to decide whether $\alpha^2 + 1$ is a primitive element of $\mathbb{F}$.
- (b) Use the table to compute $f(\alpha^3)$.
- (c) What is the value of $f(\alpha^2)$?

(2017, Semester 2) Q3 i)

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.
Show that $f(x)$ is irreducible and explain why $\mathbb{F} = \mathbb{Z}_2[x]/\langle f(x) \rangle$ is a field.

If $f(x)$ was reducible, then it would have a linear factor. However, we see that $f(0) = f(1) = 1$. So there are no linear factors which imply there are no quadratic factors either. Hence, $f(x)$ is irreducible in $\mathbb{Z}_2[x]$.

(2017, Semester 2) Q3 ii)

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.
Find the number of elements in $\mathbb{F} = \mathbb{Z}_2[x]/\langle f(x) \rangle$.

There are $2^3 = 8$ elements in $\mathbb{F}$.

(2017, Semester 2) Q3 iii)

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.
Let $\alpha = x \pmod{f(x)}$ be the image of x in $\mathbb{F}$. Evaluate

(a) $(1+\alpha)^{-1}$;

(b) all powers α^m with $3 \leq m \leq 7$;

(c) $(1+\alpha+\alpha^2)/(1+\alpha)$.

(a) We want to find the expression in which $a(1+\alpha) = 1$ in $\mathbb{Z}_2$.
To do this, we use the fact that $f(x) = x^2(x+1)+1$. Since $\alpha = x \pmod{f(x)}$, then $f(\alpha) = 0$. In other words, we have

$$f(\alpha) = \alpha^2(\alpha+1)+1 = 0 \iff \alpha^2(\alpha+1) = 1.$$

This means that the inverse of $\alpha+1$ is α^2.

(b) We shall set up the table of powers.

Since $\alpha^3 + \alpha^2 + 1 = 0$, we also have $\alpha^3 = \alpha^2 + 1$ in $\mathbb{Z}_2$. This creates the table.

α^3	$\alpha^2 + 1$
α^4	$\alpha^2 + \alpha + 1$
α^5	$\alpha + 1$
α^6	$\alpha^2 + \alpha$
α^7	1

(c) By the previous table, we have

$$\frac{1 + \alpha + \alpha^2}{1 + \alpha} = \frac{\alpha^4}{\alpha^5} = \alpha^{-1} = \alpha^6.$$

(2017, Semester 2) Q3 iv)

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.

(a) Use the table to decide whether $\alpha^2 + 1$ is a primitive element of $\mathbb{F} = \mathbb{Z}_2[x]/\langle f(x) \rangle$.

(b) Use the table to compute $f(\alpha^3)$.

(c) What is the value of $f(\alpha^2)$?

(a) Let $\beta = \alpha^3$. We need to see whether β has order 7. We can either do this manually by checking $\beta^k = \alpha^{3k}$ for $k = 1, 2, \ldots, 7$ or noticing that the order of β must divide 7. So it suffices to check $k = 1$. Since $\beta^1 = \alpha^3 \neq 1$, then we can immediately deduce that $\alpha^3 = \alpha^2 + 1$ is a primitive element.

(b)

$$f(\alpha^3) = \left(\alpha^3\right)^3 + \left(\alpha^3\right)^2 + 1 = \alpha^9 + \alpha^6 + 1 = \alpha^2 + (\alpha^2 + \alpha) + 1 = \alpha^5.$$

(c)

$$\begin{aligned} f(\alpha^2) &= \left(\alpha^2\right)^3 + \left(\alpha^2\right)^2 + 1 \\ &= \alpha^6 + \alpha^4 + 1 \\ &= (\alpha^2 + \alpha) + (\alpha^2 + \alpha + 1) + 1 \\ &= 0. \end{aligned}$$

This tells us that the minimal polynomial of α^2 is the same as the minimal polynomial of α!

BCH Codes

We now move on to the last topic of the course (and the very reason why we studied finite fields in the first place!) – BCH codes!

Bose-Chaudhuri-Hocquenghem (BCH) codes

These are more general codes that uses polynomials for encoding and decoding instead of matrices! They can be used to correct multiple errors – though, we only solve up to 2 corrections!

Encoding *BCH codes*

Given a field $\mathbb{Z}_p[x]/m(x)$, we want to encode a message.

(General strategy)

- Construct $C_I(x)$ by taking the values in the message as coefficients of the polynomial.
- Construct $C(x) = C_I(x) + D(x)$ where $D(x)$ is the polynomial found such that $m(x) \mid C(x)$.
- Encode using the coefficients of $C_I(x)$ and $D(x)$.

(2017, Semester) Q3 v)

Let $f(x) = x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$.
A BCH code is obtained from $\mathbb{F} = \mathbb{Z}_2[x]/\langle f(x) \rangle$ by replacing a quadruple (a_6, a_5, a_4, a_3) of elements of $\mathbb{Z}_2$ by $(a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ so that the polynomial

$$a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

is divisible by $f(x)$.
Encode (1101).

Construct $C_I(x) = x^6 + x^5 + x^3$. Construct $C(x) = C_I(x) + D(x) = x^6 + x^5 + x^3 + a_2x^2 + a_1x + a_0$ such that $f(x) \mid C(x)$.

This means that $C(x) = f(x)q(x)$ where $q(x)$ is some degree three polynomial. Observe that $C_I(x) = C(x) + a_2x^2 + a_1x + a_0$. So we can retrieve the unknown coefficients on long division of $C_I(x)$ by $f(x)$. We see that

$$C_I(x) = x^6 + x^5 + x^3 = x^3(x^3 + x^2 + 1).$$

Therefore, $D(x) = a_2x^2 + a_1x + a_0$ is the remainder on division. We force $a_2 = a_1 = a_0 = 0$. So we encode the message as

$$(1, 1, 0, 1) \mapsto (1, 1, 0, 1, 0, 0, 0)$$

Decoding *BCH codes* – single error

Given a field $\mathbb{Z}_p[x]/m(x)$, we want to decode a message.

(General strategy)

(I) Construct $R(x)$ by taking the message values as coefficients of the polynomial.

(II) Compute $R(\alpha)$ where α is the primitive root of $m(x)$.

(III) If $R(\alpha) = 0$, then no error has occurred. Otherwise, there is an error at *exactly* the α^i (i-th) position.

(2021, Term 2) Tutorial Problem 9, Q1

Set $m(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. A single error correcting BCH code is constructed over $GF(8)$ with primitive element α.
Find the error and decode $[1, 1, 0, 1, 1, 0, 1]$.

Begin by constructing the polynomial representation of the message

$$R(x) = x^6 + x^5 + x^3 + x^2 + 1.$$

Then, for the primitive root α, we compute $R(\alpha)$. This gives us

$$R(\alpha) = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1.$$

Since α is the root of $m(x)$, then we need to construct the table of powers.

Since $m(\alpha) = 0$, we have

$$\alpha^3 + \alpha^2 + 1 = 0 \iff \alpha^3 = \alpha^2 + 1.$$

α^0	1
α^1	α
α^2	α^2
α^3	$\alpha^2 + 1$
α^4	$\alpha^2 + \alpha + 1$
α^5	$\alpha + 1$
α^6	$\alpha^2 + \alpha$
α^7	1

Then:

$$\begin{aligned} R(\alpha) &= \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + 1 \\ &= \alpha^2 + \alpha + \alpha + 1 + \alpha^2 + 1 + \alpha^2 + 1 \\ &= \alpha^2 + 1 = \alpha^3. \end{aligned}$$

This means there's an error in the third coefficient. So the correct message should be $[1, 1, 0, 0, 1, 0, 1]$ which decodes by taking the first four digits: $[1, 1, 0, 0]$.

BCH Codes – correct two errors

We need to extend the code to be able to correct at most two errors.

Correcting two errors

To correct two errors, we need to construct a polynomial that contains two primitive roots: α and α^j for some power j.
To find the polynomial, start with a polynomial $m_1(x)$ of which we know that α is a primitive root of (this is usually given to us). Then find another minimal polynomial $m_2(x)$ with primitive root α^j for some power j.
The resulting polynomial is $m(x) = m_1(x) \cdot m_2(x)$.

Encoding BCH codes – two errors

(General strategy)

Exactly the same as the one error case; construct $C_I(x)$ and $C(x) = C_I(x) + D(x)$ such that $m(x) \mid C(x)$.

Decoding BCH codes – two errors

(General strategy)

Construct $R(x)$ and find $R(\alpha)$. If $R(\alpha) = 0$, then there is no error. Otherwise, we have *at least* one error. Compute $R(\alpha^3)$. If $R(\alpha) = \alpha^i$ and $R(\alpha^3) = \alpha^{3i} = R(\alpha)^3$, then there is one error exactly at the i-th location. Otherwise, if $R(\alpha) = \alpha^i$ and $R(\alpha^3) \neq R(\alpha)^3$, then there are two errors.

Let $m_1(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ and let $m_3(x) = x^4 + x^3 + x^2 + x + 1$. An error correcting BCH code is obtained from $F = \mathbb{Z}_2[x]/\langle m_1(x)\rangle$ by replacing a message $(a_{14}, a_{13}, \ldots, a_8)$ by the coefficients of a polynomial $C(x) \in \mathbb{Z}_2[x]$ where

$$\begin{aligned} C(x) &= C_I(x) + r(x) \\ \text{with } C_I(x) &= a_{14}x^{14} + a_{13}x^{13} + \cdots + a_8x^8 \\ \text{and } r(x) &= C_I(x) \pmod{m(x)}, \\ \text{where } m(x) &= m_1(x)m_3(x) = x^8 + x^7 + x^6 + x^4 + 1. \end{aligned}$$

(a) Encode the message $(1, 1, 0, 0, 0, 1, 0)$ using the BCH code above.

(b) For each of the following received messages, find out how many errors it contains (assuming at most 2 errors). If there is one error, then locate and correct the error and decode the message. If there are two errors, do NOT try to locate or correct them.

(A) $(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$

(B) $(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$.

(a) Encode $(1,1,0,0,0,1,0)$. Construct $C_I(x) = x^{14} + x^{13} + x^9$. To find $r(x)$, we need to find $C_I(x) \pmod{m(x)}$. We can do this using long division to get

$$C_I(x) = (x^6+x^4+x^3+x^2+x+1)m(x)+(x^7+x^6+x^5+x^3+x^2+x+1).$$

So we encode it as

$$(1,1,0,0,0,1,0) \mapsto (1,1,0,0,0,1,0,1,1,1,0,1,1,1,1).$$

(b) To decode, we find $R(x)$, find $R(\alpha)$ and compute $R(\alpha^3)$.

(A) Decode $(0,0,0,1,1,1,0,0,1,0,1,1,0,0,1)$. Construct

$$R(x) = x^{11} + x^{10} + x^9 + x^6 + x^4 + x^3 + 1.$$

Find $R(\alpha)$ where α is the primitive root of $m_1(x)$. Since $m_1(x) = x^4 + x + 1$, then we have $\alpha^4 = \alpha + 1$.

We have the table of powers:

α^0	1	α^5	$\alpha^2+\alpha$	α^{10}	$\alpha^2+\alpha+1$
α^1	α	α^6	$\alpha^3+\alpha^2$	α^{11}	$\alpha^3+\alpha^2+\alpha$
α^2	α^2	α^7	$\alpha^3+\alpha+1$	α^{12}	$\alpha^3+\alpha^2+\alpha+1$
α^3	α^3	α^8	α^2+1	α^{13}	$\alpha^3+\alpha^2+1$
α^4	$\alpha+1$	α^9	$\alpha^3+\alpha$	α^{14}	α^3+1

Thus, we have

$$\begin{aligned} R(\alpha) &= \alpha^{11}+\alpha^{10}+\alpha^9+\alpha^6+\alpha^4+\alpha^3+1 \\ &= (\alpha^3+\alpha^2+\alpha)+(\alpha^2+\alpha+1)+(\alpha^3+\alpha)+(\alpha^3+\alpha^2) \\ &\quad +(\alpha+1)+\alpha^3+1 \\ &= \alpha^2+1=\alpha^8. \end{aligned}$$

Compute $R(\alpha^3)$. We have

$$\begin{aligned} R(\alpha^3) &= (\alpha^3)^{11} + (\alpha^3)^{10} + (\alpha^3)^9 + (\alpha^3)^6 + (\alpha^3)^4 + (\alpha^3)^3 + 1 \\ &= \alpha^3 + \alpha^0 + \alpha^{12} + \alpha^3 + \alpha^{12} + \alpha^9 + 1 \\ &= \alpha^9. \end{aligned}$$

Since $R(\alpha)^3 \neq R(\alpha^3)$, we have two errors.

(B) Repeat the same steps as described above.