Topics in Discrete Mathematics

by

Marina Godinho

Lectures notes written for
Mathematics 2T: Topics in Discrete Mathematics course
Based on a set of notes written by
Dr. Richard Steiner and Dr. Spiros Adams-Florou.

School of Mathematics & Statistics
College of Science & Engineering
University of Glasgow
2026

Topics in Discrete Maths 2025–26

COURSE

This is a course on **discrete mathematics**, meaning we are interested in studying **discrete objects**– to us this will mean **finite objects** e.g. finite sets. More generally, discrete mathematics studies **countable objects** e.g. the integers $\mathbb{Z}$.

This course is structured into two chapters:

1) **Enumeration Theory** and
2) **Number Theory and Cryptography**.

These notes might contain typos– so do let me know if you find any.

Table of Contents

Chapter 1 Enumeration Theory

1.1 Basic Counting Principles

The goal of Enumeration Theory is to work out the numbers of elements in finite sets. So, in this chapter we introduce some basic principles which will help us count elements of finite sets.

For example, at the end of this section, we would like to answer the question:

Q1 How many 3-digit numbers are there such that all digits are odd? **A:** 125.

Definition 1.1. The number of elements in a finite set A is denoted $|A|$ [1], one says that $|A|$ is the **cardinality of A**.

1. N.B. $|A|$ is always a non-negative integer

1.1.1 Addition Principle

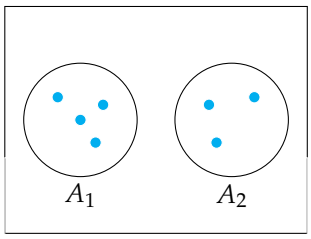
The Addition Principle.

If $A_1, A_2, \ldots, A_n$ are disjoint finite sets, then

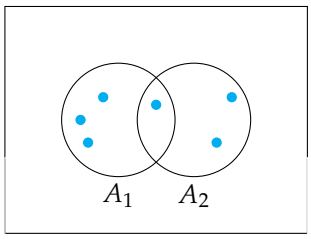
$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|$$

Q2 *What happens if the sets are not disjoint? Can you provide an example supporting your answer?*

We can visualise the addition rule (and its failure when sets are not disjoint) via the following diagrams



$A_1 \cup A_2$



$A_1 \cup A_2$

1.1.2 Multiplication Principle

Definition 1.2. For finite sets $A_1, A_2, \ldots, A_n$ recall that the **cartesian product** of the sets $A_1, A_2, \ldots, A_n$ is

$$A_1 \times A_2 \times \cdots A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$$

the set of ordered n-tuples with first component in A_1, second component in A_2 and so on.

Reality Check 1 Let $A_1 = \{1,2\}$, $A_2 = \{3,4\}$, then

$$A_1 \times A_2 = \{(1,3),(1,4),(2,3),(2,4)\}$$

which can be visualised as the 2×2-grid

	3	4
1	(1,3)	(1,4)
2	(2,3)	(2,4)

The Multiplication Principle.
Let $A_1, A_2, \ldots, A_n$ be finite sets. Then,

$$|A_1 \times A_2 \times \cdots A_n| = |A_1| \times |A_2| \times \cdots |A_n|.$$

Note: This rule can be visualised in the grid in Reality Check 1.

1.1.3 Subtraction Principle

Definition 1.3. If A is a finite set and $B \subset A$, then we can define the set [2]

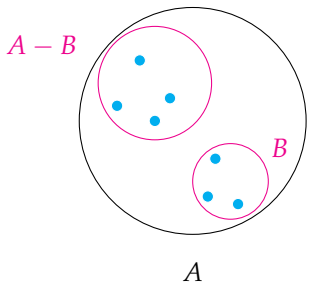
$$A \setminus B = \{a \in A \mid a \notin B\}.$$

2. We will sometimes denote $A \setminus B$ as $A - B$

The Subtraction Principle.
If A is a finite set and $B \subset A$, then

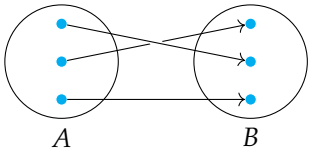
$$|A \setminus B| = |A| - |B|$$

This principle can be visualised in a diagram



1.1.4 Bijection Principle

Let A and B be finite sets. Recall that a function $f\colon A \to B$ is a **bijection** if it is one-to-one (injective) and onto (surjective). That is, a bijection establishes a one-to-one correspondence between all elements of A and all elements of B.



The Bijection Principle.
If there is a bijection $f\colon A \to B$ between finite sets, then $|A| = |B|$.

1.1.5 Examples

Example 1.4. A restaurant serves 3 types of starter, 6 main courses and 5 desserts.

a) How many three-course meals are there?

b) How many two-course meals including a main course?

Solution.

a) Let S, M, D be the sets of starters, main courses and desserts. Then, a three course mean is a triple

$$(\text{choice of start, choice of main, choice of dessert})$$

and so a three course meal is an element of the set $S \times M \times D$. Therefore, the number of three-course meals is

$$|S \times M \times D| = |S| \times |M| \times |D| = 3 \times 6 \times 5 = 90.$$

In other words: We are making three independent choices; for the first one there are 3 options, for the second there are 6 and for the third there are 5.

b) A two course meal including a main is either a couple

$$(\text{choice of starter, choice of main})$$

or

$$(\text{choice of main, choice of dessert}).$$

So, a two course meal including a main is an element of the set

$$(S \times M) \cup (M \times D).$$

Hence the number of two-course meals is

$$|(S \times M) \cup (M \times D)| = |S \times M| + |M \times D| = 3 \times 6 + 6 \times 5 = 48$$

since $S \times M$ and $M \times D$ are disjoint.

Example 1.5. A password on a computer system is a string of 6 characters. Each character is a lower case letter or a digit, and the password must contain at least one digit. How many possible passwords are there?

Solution. Let A be the set of 6-character strings with lower case letters and digits. Let B be the set of 6-character strings which do not contain a digit. Then, the set of passwords which contain at least one digit is $A \setminus B$.

By the subtraction principle, the number of such passwords is

$$|A \setminus B| = |A| - |B|$$

To solve the question, we need to find $|A|$ and $|B|$.

a) Finding $|B|$.

Let L be the set of lower case letters, then $|L| = 26$.

A 6-character string of lower case letters looks like $s_1 s_2 \dots s_6$, where each $s_i \in L$ (for example, *aabbcc*). These strings are the same as a tuple $(s_1, s_2, \dots, s_6)$

Hence, we may view B as the 6-fold cartesian product

$$B = L \times L \times \dots \times L$$

By the product rule,

$$|B| = |L|^6 = 26^6$$

b) Finding $|A|$. Let D be the set of digits.

A 6-character string of lower case letters and digits looks like $s_1 \dots s_6$ (for example, *aa*00*bb*).These strings are a tuple $(s_1, s_2, \dots, s_6)$ where each s_i is either in L or D. That is, $s_i \in L \cup D$. Hence A, the set of all these strings, is the same as the sixfold cartesian product

$$(L \cup D) \times (L \cup D) \dots (L \cup D) = A$$

Observe that since L and D are disjoint,

$$|L \cup D| = |L| + |D| = 26 + 10 = 36$$

by the addition principle. Thus, $|A| = 36^6$ by the multiplication principle.

Therefore, the set of 6-character strings which contain at least one digit is

$$|A| - |B| = 36^6 - 26^6$$

Example 1.6. Let A and B be finite sets. How many functions are there from A to B?

Solution. Suppose A has r elements, then $|A| = r$ and we can write

$$A = \{a_1, a_2, \ldots, a_r\}.$$

To define a function from $f\colon A \to B$, for each member of A one has to choose a member of B to be its image. So, a function is the same as the data

$$\begin{aligned} a_1 &\mapsto b_1 \in B \\ a_2 &\mapsto b_2 \in B \\ &\vdots \\ a_r &\mapsto b_r \in B \end{aligned}$$

Intuitively, one is making r independent choices, and one has $|B|$ possibilities at each stage. So, we should expect the total number of functions to be

$$|B| \times \ldots \times |B| = |B|^r$$

Formally, data defining the function $f\colon A \to B$ is the same as a tuple $(b_1, b_2, \cdots, b_r) \in B \times B \times \ldots \times B$. Hence, the number of functions $A \to B$ is

$$|B \times \ldots \times B| = |B|^r = |B|^{|A|}.$$

1.2 Permutations and Combinations

In this section, we will learn to count how many ways there are to choose k (ordered and unordered) *distinct* elements from a set of n elements.

An example of a question we will learn how to answer is:

Q3 A fair six-sided die is rolled three times. What is the probability that exactly two 6's are rolled? **A:** $\frac{5}{72} \sim 0.097$

Definition 1.7. Suppose that n is a positive integer. Then, recall that

$$n! := n \times n - 1 \times \ldots \times 2 \times 1$$

and we establish by convention that $0! = 1$.

1.2.1 Permutations

Q4 Let S be a set of n elements. Let $r \leq n$. How many ways are there to choose r *ordered* distinct elements from the set S?

Definition 1.8. Let r, n be a pair of integers with $0 < r \leq n$. An **r-permutation** of S is a sequence $s_1 s_2 \ldots s_r$ obtained by ordering r distinct elements of S.

The set of all r-permutations of S will be denoted as $P(S, r)$.

Q5 Let $S = \{a, b, c\}$. What is an example of 2-permutation of S?

Example 1.9. Let $S = \{a, b, c\}$. Then,

$$P(S, 2) = \{ab, ac, ba, bc, ca, cb\}$$

Theorem 1.10. *The number of r-permutations of S is*

$$|P(S, r)| = \frac{n!}{(n-r)!}$$

Proof. [3] To construct a permutation $s_1 \dots s_r$, we have to make the choices:

$$\begin{aligned} &s_1 \in S \\ &s_2 \in S - \{s_1\} \\ &\quad \vdots \\ &s_r \in S - \{s_1, s_2, \dots, s_{r-1}\} \end{aligned}$$

Intuitively, we are making r choices. The first choice has n options. The second choice has $n-1$ options and so on. So we should expect the number of sequences $s_1 \dots s_r$ to be

$$n \times n - 1 \times \dots \times 2 \times 1$$

Formally, a sequence $s_1 \dots s_r$ is the same as a tuple $(s_1, s_2, \dots s_r)$ where $s_1 \in S$, $s_2 \in S - \{s_1\}$, $s_3 \in S - \{s_1, s_2\}$ and so on. Hence, the set of all r-permutations $P(S, r)$ is equal to the set

$$S \times (S - \{s_1\}) \times (S - \{s_1 - s_2\}) \times \dots \times (S - \{s_1, s_2, \dots, s_r\})$$

In other words,

$$|P(S, r)| = |S \times (S - \{s_1\}) \times (S - \{s_1 - s_2\}) \times \dots \times (S - \{s_1, s_2, \dots, s_r\})|$$

So by the multiplication rule, the number of r-permutations is

$$|S| \times |S - \{s_1\}| \times |S - \{s_1 - s_2\}| \times \dots \times |S - \{s_1, s_2, \dots, s_r\}|$$

which is precisely

$$n \times (n-1) \times (n-2) \times \dots \times (n-r) = \frac{n!}{(n-r)!}$$

□

[3] The proof of this theorem at this level of generality is not examinable, but understanding this proof will really help you with some of the more complicated exercises!

1.2.2 Combinations

Q6 Let S be a set of n elements. Let $r \leq n$. How many ways are there to choose r *unordered* distinct elements from the set S?

Choosing r *unordered* distinct elements from the set S is the same as to choosing a subset of S with r elements. So Q4 can be rephrased as: How many subsets of S with r elements are there?

Example 1.11. Consider $S = \{a, b, c\}$. How many 2-element subsets are there?

Because S is small, we can answer this question by the brute force method of listing all of the possibilities

$$\{a, b\}, \{a, c\}, \{b, c\}$$

But this is not such an efficient algorithm for finding this number. Let's consider another approach, which is based on two observations.

1) We can get each 2-permutation of S exactly once by running through all of the 2-element subsets of S and ordering the elements in all possible ways:

2-elements subset		Possible ordering 1	Possible ordering 2
$\{a, b\}$	$\rightsquigarrow$	ab	ba
$\{a, c\}$	$\rightsquigarrow$	ac	ca
$\{b, c\}$	$\rightsquigarrow$	bc	cb

2) For each of these subsets, there are $2! = 2$ ways to list their elements.

Combining 1) and 2),

$$\#\text{2-permutations of } S = \#\text{2-element subsets of } S \times 2!$$

We know from the Permutations section that #of 2-permutations of $S = \frac{3!}{1!}$

So,

$$\#\text{2-element subsets of } S = \frac{3!}{2!} = 3$$

This strategy is how we will answer Q4 generally.

Theorem 1.12. *The number of r-elements subsets (which is the same as the number of ways to choose r unordered distinct elements from S) is*

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

Proof. [4] As in Example 1.11, this can be deduced from two observations.

1) We can get each r-permutation of S exactly once by running through all r-element subsets $\{a_1, a_2, \ldots, a_r\} \subset S$ and ordering the elements of B in all possible ways.

2)We know from Theorem 1.10 that there are $r!$ ways to order the elements of B.

Hence,

$$\#(r\text{-permutations of } S) = \#(r\text{-element subsets of } S) \times r!$$

From Theorem 1.10, we know that there are $\frac{n!}{(n-r)!}$ permutations of S. So,

$$\frac{n!}{(n-r)!} = \#(r\text{-element subsets of } B) \times r!$$

Dividing both sides by $r!$,

$$\#(r\text{-element subsets of } B) = \frac{n!}{(n-r)! \times r!} = \binom{n}{r}$$

□

4. The proof of this theorem at this level of generality is also not examinable, but understanding this proof will really help you with some of the more complicated exercises!

1.2.3 Summary

Say we have a set S with n elements. Let $r \leq n$. Then,

a) The number of ways to choose an *ordered list* of r elements from S:

$$\frac{n!}{(n-r)!} \rightsquigarrow \text{Also counts number of } r\text{-permutations of } S$$

b) The number of ways to choose an *unordered set* of r elements from S is:

$$\binom{n}{r} = \frac{n!}{(n-r)!}\frac{1}{r!} \rightsquigarrow \text{Also counts } r\text{-element subsets of } S$$

1.2.4 Examples

Example 1.13. a) How many ways are there to order the 26 letters of the alphabet?

b) How many of these ways have the 5 vowels in a consecutive block?

Solution.

a) Let $S_1 = \{a, b, \ldots, z\}$ be the set of letters in the alphabet (so $|S| = 26$). We are looking for permutations of S_1 of length 26. So, from Theorem 1.10,

$$|P(S_1, 26)| = 26!$$

b) We first ask the question: For each block of vowels, how many ways are there to order the block and the 21 consonants. Let B be a block of vowels (e.g. B is the block "AIOUE"). Then, we want to order all of the elements in the set

$$S_2 = \{21 \text{ consonants}, B\}$$

The number of possible orderings is $|P(S_2, 22)| = 22!$.

We next ask: How many blocks of vowels are there? This is the same as asking how many 5-permutations are there of the set

$$V = \{A, I, E, O, U\}.$$

Theorem 1.10 tells us $|P(V, 5)| = 5!$.

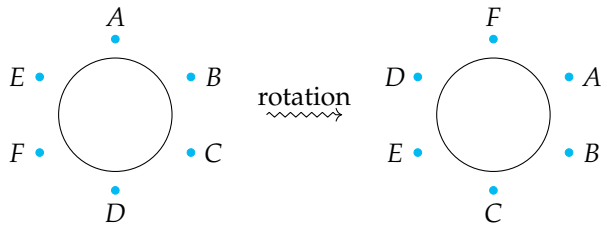
Thus, there are 5! blocks and for each block there are 22! factorial ways to order the block with the consonants, and so there are $5! \times 22!$ possible ordering of the alphabet where the vowels are in a consecutive block.

Example 1.14. How many ways are there to seat 6 people round a circular table, if seating arrangements are considered to be the same when one is a rotation of the other?

Solution. Asking how many ways are there to order 6 people around the table is the same as asking how many 6-permutations are there of the set

$$S = \{6 \text{ people}\}.$$

By Theorem 1.10, there are 6! ways to assign 6 people to the 6 seats. However, for any given ordering, there are five other orderings which are its rotations e.g.



Thus, for each seating arrangement, there are 6 orderings which are considered the same seating arrangement. So, the required answer is

$$\#\begin{pmatrix}\text{seating ar-}\\ \text{rangements}\end{pmatrix} = \frac{\#(\quad \text{orderings} \quad)}{6} = 6!/6 = 5!$$

Example 1.15. A coin is tossed 10 times. How many of the 2^{10} possible outcomes contain (a) exactly 2 heads, (b) at least three tails.

Solution. (a) Let $S = \{\text{toss}_1, \text{toss}_2, \ldots, \text{toss}_{10}\}$.

Answering (a) amounts to choosing 2 tosses from S and declaring them to be heads, and then declaring all other tosses to be tails. That is, we are choosing a 2-element subset of S. By Theorem 1.12, there are

$$\binom{10}{2}$$

2-element subsets.

(b) The set of all possible outcomes has cardinality 2^{10}. We exclude the outcomes with 0, 1 or 2 members, giving an answer of

$$2^{10} - \binom{10}{0} - \binom{10}{1} - \binom{10}{2}.$$

Example 1.16 (Pascal's identity)**.** Prove that for integers $0 < r < n$ then

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

Solution. This is our first example of a *counting argument* or a *combinatorial proof*. We show LHS = RHS by showing that the LHS and RHS are both ways to count the same objects, and so they have to be equal.

Let S be a set with n elements. We know that $\binom{n}{r}$ counts the number of r-element subsets of S. We will show that the RHS also corresponds to the number of r-elements subsets of S.

Let's choose any element $s_0 \in S$, and let B be any r-element subset of S. Then, we have two cases to consider: B either contains s_0 or doesn't.

(1) If B does not contain s_0, then B is a subset of $S - \{s_0\}$.

(2) On the other hand, if B contains s_0, then we may write

$$B = \{s_0, b_2, \ldots, b_r\} = \{s_0\} \cup \{b_2, \ldots, b_r\}$$

Notice that the set $\{b_2, \ldots, b_r\}$ does not contain s_0 and so it is a subset of $S - \{s_0\}$.

In other words, an r-element subset of S is either (1) an r-element subset of $S - \{s_0\}$ [Case (1)] or (2) B is the union of $\{s_0\}$ with an $(r-1)$-element subset of $S - \{s_0\}$ [Case 2].

This observation means that

$$\#\underbrace{\begin{pmatrix} r\text{-element} \\ \text{subsets of } S \end{pmatrix}}_{\text{From subsection 1.2.2 this is } \binom{n}{r}} = \#\underbrace{\begin{pmatrix} r\text{-element subsets} \\ \text{of } S - \{s_0\} \end{pmatrix}}_{\text{From subsection 1.2.2, this is } \binom{n-1}{r}} + \#\underbrace{\begin{pmatrix} (r-1)\text{-element} \\ \text{subsets of } S - \{s_0\} \end{pmatrix}}_{\text{From subsection 1.2.2, this is } \binom{n-1}{r-1}}.$$

Thus:

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$$

as required.

1.3 Multinomial Coefficients

In general the question we want to answer in this section is:

Q7 If you have n elements which you wish to divide into r distinct piles of sizes n_1, n_2, …, n_r, then how many ways are there to do that?

We will use *Multinomial Coefficients* for this.

1.3.1 Definition of Multinomial Coefficient

Definition 1.17. Let n be an integer, and let $n_1, n_2 \ldots, n_r$ be integers such that $n_1 + n_2 + \ldots + n_r = n$. The *multinomial coefficient* is given by

$$\binom{n}{n_1, n_2, \ldots, n_r} := \frac{n!}{n_1! n_2! \ldots n_r!}$$

Example 1.18. What is $\binom{6}{1,2,3}$?

Solution.

$$\binom{6}{1,2,3} = \frac{6!}{1! \times 2! \times 3!} = 60$$

1.3.2 Using Multinomial Coefficients in Enumeration Theory

By the end of this section, our goal is to answer questions such as:

Q8 How many strings can be made by using the letters of the word "COFFEE"? **A:** $\frac{6!}{2!\times 2!} = 180$.

Example 1.19. How many strings can be made by using the letters of the word "MISSISSIPPI"?

Solution.

This question can be rephrased as:

How many 11-letter strings can be made, using

a) 1 letter "M",

b) 4 letters "I",

c) 4 letters "S",

d) 2 letters "P"?

We can think of this question in the following way: Imagine that there are 11 "slots" for the letters; then we want to know how many ways are there to choose

a) 1 slot to be an "M",

b) 4 slots to be an "I",

c) 4 slots to be an "S"

d) 2 slots to be a "P".

So, we have a set of 11 slots

$$S = \{-_1, -_2, \ldots, -_{11}\}$$

and we want to count the number of ordered choices of 11 elements where we declare (1) the first chosen slot to be an M. (2) the second, third, fourth and fifth slots to be I's and so on.

For example, the sequence

$$\underbrace{-_1}_{M} \quad \underbrace{-_4\,-_6\,-_7\,-_8}_{I} \quad \underbrace{-_2\,-_3\,-_5\,-_9}_{S} \quad \underbrace{-_{10}\,-_{11}}_{P}$$

corresponds to choosing the string "MSSISIIISPP"

and the sequence

$$\underbrace{-_1}_{M} \quad \underbrace{-_8\,-_7\,-_6\,-_4}_{I} \quad \underbrace{-_2\,-_3\,-_5\,-_9}_{S} \quad \underbrace{-_{10}\,-_{11}}_{P}$$

corresponds to choosing the string "MSSISIIISPP"

There are 11! ways to make sequences with 11 elements from the set of slots S [Why?]. However, notice e.g. that the two sequences above correspond to the same string. So we are double counting!

It turns out [Why?] that for each string, there are 4!4!2! sequences which produce the same string. Hence, the total number of strings is

$$\frac{11!}{4! \times 4! \times 2! \times 1!} = \binom{11}{1,4,4,2}$$

The question of Example 1.19 is a particular case of the more general question Q7. To answer this question, we introduce the definition.

Definition 1.20. Let S be a set with n elements. A *partition* of S is a list of subsets $S_1, S_2, \ldots, S_r \subset S$ which are

a) nonempty,

b) disjoint

c) such that $S_1 \cup S_2 \cup \ldots \cup S_r = S$.

Example 1.21. A partition of $S = \{a, b, c\}$ is, for example, $S_1 = \{a\}$ and $S_2 = \{b, c\}$.

The answer to Q7 is given by the following theorem.

Theorem 1.22. *Let S be a set with n elements. Let n_1, n_2, …, n_r be integers such that $n_1 + n_2 + \ldots + n_r = n$. Then, the number of ways of partitioning S into subsets S_1, S_2, …, S_r such that S_i has n_i elements is the multinomial coefficient*

$$\binom{n}{n_1, n_2, \ldots, n_r}$$

In less abstract terms, this theorem is saying that if you have n elements which you wish to divide into r distinct piles of sizes n_1, n_2, …, n_r, then there are

$$\binom{n}{n_1, n_2, \ldots, n_r}$$

ways to do that.

The proof of this theorem follows along the lines of the solution to Example 1.19.

Example 1.23. How many ways are there to paint 12 distinguishable rooms so that 3 of them are pink, 2 are green, 2 are yellow and the rest are white?

Solution. We would like to partition the

$$S = \{\text{room}_1, \text{room}_2, \ldots, \text{room}_{12}\}$$

into four sets

a) $S_1 = \{\text{pink rooms}\}$, $|S_1| = 3$.

b) $S_2 = \{\text{green rooms}\}$, $|S_2| = 2$.

c) $S_3 = \{\text{yellow rooms}\}$, $|S_3| = 2$.

d) $S_4 = \{\text{white rooms}\}$, $|S_4| = 11 - 3 - 2 - 2 = 5$.

Thus, the number of partitions of S satisfying this is:

$$\binom{12}{3,2,2,5} = \frac{12!}{3! \times 2! \times 2! \times 5!}$$

1.3.3 Multinomial Theorem

Binomial coefficients $\binom{n}{r} = \frac{n!}{(n-r)!}$ are so called because they appear in the expansion of powers of two-term expressions. More precisely, the *binomial theorem* states that

$$\begin{aligned}(x+y)^n &= \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r \\ &= \underbrace{\binom{n}{0} x^n}_{r=0} + \underbrace{\binom{n}{1} x^{n-1} y}_{r=1} + \ldots + \underbrace{\binom{n}{n-1} x y^{n-1}}_{r=n-1} + \underbrace{\binom{n}{n} y^n}_{r=n}\end{aligned}$$

We will prove a more general theorem: The multinomial theorem.

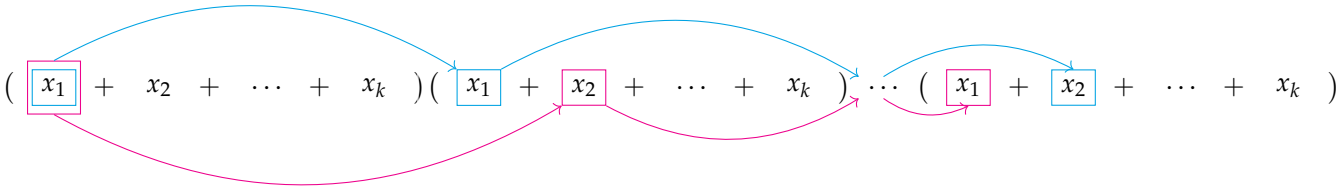
Theorem 1.24. *There is an identity*

$$(x_1 + x_2 + \ldots + x_k)^n = \sum_{r_1 + r_2 + \ldots + r_k = n} \binom{n}{r_1, r_2, \ldots, r_k} x_1^{r_1} x_2^{r_2} \ldots x_k^{r_k}$$

Proof. To compute $(x_1 + x_2 + \ldots + x_k)^n$ directly, we would write

$$(x_1 + x_2 + \ldots + x_k)^n = \underbrace{(x_1 + x_2 + \ldots + x_k) \times \ldots \times (x_1 + x_2 + \ldots + x_k)}_{n \text{ times}}$$

Computing this product means summing over all possible products



so we would get something such as

$$x_1^n + x_1 x_2 x_1^{n-2} + \ldots$$

or more precisely, the sum expansion of $(x_1 + x_2 + \ldots + x_k)^n$ is the sum of all possible sequences

$$x_{i_1} \times x_{i_2} \times \ldots \times x_{i_k}$$

of length n, where each x_{i_1}, $x_{i_2}, \ldots, x_{i_k}$ is chosen from the set of $\{x_1, x_2, \ldots, x_k\}$.

We want to know how many combinations contain

- The term "x_1" exactly r_1 times
- The term "x_2" exactly r_2 times
- $\vdots$
- The term "x_k" exactly r_k times.

[This should remind you of the Example 1.19, where we asked how many 11-letter strings can be formed with 1 M, 4 I's, 4 S's and 2 P's... we can think of a term

$$x_{i_1} \times x_{i_2} \times \ldots \times x_{i_k}$$

as a "string" with k "letters", where each "letter" is an element of the set $\{x_1, \ldots, x_k\}$. We want to know how many strings we can make with a precise amount of x_1's, x_2's and so on.]

So, similarly to the example 3.6, we can consider a set of n slots

$$S = \{-_1, -_2, \ldots, -_n\}$$

and we want to count how many ways there are to partition it into k subsets:

$$\begin{aligned} S_1 &= \{\text{Slots which we will declare to be } x_1\}, |S_1| = r_1, \\ S_2 &= \{\text{Slots which we will declare to be } x_2\}, |S_2| = r_2, \\ &\vdots \\ S_k &= \{\text{Slots which we will declare to be } x_k\}, |S_k| = r_k \end{aligned}$$

From Theorem 1.22, this is $\binom{n}{r_1,\ldots,r_k}$.

Hence, if we run through all possible sequences of length n

$$x_{i_1} \times x_{i_2} \times \ldots \times x_{i_k}$$

where each x_{i_1}, $x_{i_2}, \ldots, x_{i_k}$ is chosen from the set of $\{x_1, x_2, \ldots, x_k\}$, then we will get the term

$$x_1^{r_1} x_2^{r_2} \ldots x_k^{r_k}$$

$\binom{n}{r_1,\ldots,r_k}$ times. □

Example 1.25. What is the coefficient of the term $x^2y^3z^2$ in the sum expansion of $(x+y+z)^7$?

Solution. The coefficient is:

$$\binom{7}{2,3,2} = \frac{7!}{2! \times 3! \times 2!} = 7 \times 6 \times 5 = 210$$

.

1.3.4 Multinomial Theorem (Addendum)

In this quick subsection, we will go through the proof of the multinomial theorem for a concrete case, this will hopefully make the general proof clearer.

Example 1.26 (of the Multinomial theorem proof)**.** There is an identity

$$(x+y+z)^3 = \sum_{r_1+r_2+r_3=3} \binom{3}{r_1, r_2, r_3} x^{r_1} y^{r_2} z^{r_k}$$

Proof. To compute $(x+y+z)^3$ directly, we would write

$$\begin{aligned}(x+y+z)^3 &= (x+y+z)\times(x+y+z)\times(x+y+z)\\ &= xxx+xxy+xxz+xyx+xyy+xyz+xzx+xzy+xzz\\ &\quad +yxx+yxy+yxz+yyx+yyy+yyz+yzx+yzy+yzz\\ &\quad +zxx+zxy+zxz+zyx+zyy+zyz+zzx+zzy+zzz\end{aligned}$$

So notice that the sum expansion of $(x+y+z)^3$ is the sum of all possible sequences of length 3 which we can form with the variables x, y, z.

Next, notice that $xxy = xyx = yxx = x^2y$. In other words, all of the sequences which have two x's and one y are the same, and we can simplify the expression above by collecting all of the terms that have exactly two x's and one y

$$\begin{aligned}(x+y+z)^3 &= xxx+xxy+xxz+xyx+xyy+xyz+xzx+xzy+xzz\\ &\quad +yxx+yxy+yxz+yyx+yyy+yyz+yzx+yzy+yzz\\ &\quad +zxx+zxy+zxz+zyx+zyy+zyz+zzx+zzy+zzz\\ &= 3x^2y+xxx+xxz+xyy+xyz+xzx+xzy+xzz\\ &\quad +yxy+yxz+yyx+yyy+yyz+yzx+yzy+yzz\\ &\quad +zxx+zxy+zxz+zyx+zyy+zyz+zzx+zzy+zzz\end{aligned}$$

We knew there were three terms with two x's and one y by directly counting. Instead of directly counting, we could try to think about it combinatorially. We could ask: How many possible sequences of length 3 formed with the variables x, y, z can we make which have exactly two x's and one y.

Now, this is similar to the problem in Example 1.19. We can think of a sequence of length 3 as a string with 3 letters, and we are asking the question: How many 3 letter strings can we make with exactly two x's and one y?

So, as in Example 1.19, we consider the set of empty slots

$$S = \{-_1, -_2, -_3\}$$

and we want to count how many ways there are to partition it into subsets:

$$\begin{aligned}S_1 &= \{\text{Slots which will be declared to be } x\}, |S_1| = 2,\\ S_2 &= \{\text{Slots which will be declared to be } y\}, |S_2| = 1,\\ S_3 &= \{\text{Slots which will be declared to be } y\}, |S_3| = 0.\end{aligned}$$

From Theorem 1.22, this is $\binom{3}{2,1,0} = 3$.

More generally, given any r_1, r_2, r_3 such that $r_1 + r_2 + r_3 = 3$, then the number of times $x^{r_1}y^{r_2}z^{r_3}$ appears in the sum expansion is the same as the number of 3 letter strings which we can make from the letters x, y, z and which contain the term

a) x exactly r_1 times,

b) y exactly r_2 times,

c) z exactly r_3 times.

and we know that this is the same as paritioning the set S of slots into

$$S_1 = \{\text{Slots which will be declared to be } x\}, |S_1| = r_1,$$
$$S_2 = \{\text{Slots which will be declared to be } y\}, |S_2| = r_2$$
$$S_3 = \{\text{Slots which will be declared to be } z\}, |S_3| = r_3.$$

From Theorem 1.22, this is $\binom{3}{r_1,r_2,r_3} = 3$. □

1.4 Ordered partitions with possibly empty parts

In general, we want to answer the question:

Q9 If you have n indistinguishable elements, which you wish to divide into r distinct piles, how many ways are there to do that?

For instance, by the end of this section, we should be able to answer the following question.

Q10 There are 12 indistinguishable rooms to be painted pink, green, yellow and white. Assuming you have enough paint of each colour to paint any number of rooms, how many ways are there to paint the 12 rooms? **A:** 455

Example 1.27. There are 12 indistinguishable glasses to be filled with red wine, white wine or orange juice. In how many ways can this be done?

Solution. Since the glasses are indistinguishable, we only care about the number of glasses filled with each kind of drink. Let

$$x = \#(\text{red wine glasses})$$
$$y = \#(\text{white wine glasses})$$
$$z = \#(\text{orange juice glasses}).$$

Since there are 12 glasses in total, these numbers must satisfy

$$x + y + z = 12$$

In other words, the number of ways of filling the glasses is the same as the number of triples (x, y, z) of integers satisfying $x + y + z = 12$. Hence, we are interested in counting these triples.

We can do this by forming a string with 14 characters, 12 of which are "G" and two of which are empty spaces e.g.

$$\underbrace{GGG}_{x=3} \quad \underbrace{GGGGG}_{y=5} \quad \underbrace{GGGG}_{z=4}$$

There are three blocks of Gs whose lengths give the integers (x, y, z); in the example above, the string corresponds to the triple $(3, 5, 4)$.

Thus, the number of of triples (x, y, z) of integers satisfying the equation $x + y + z = 12$ is the same as the number of such strings.

The number of such strings is the number of ways of choosing 12 positions out of 14 positions and declaring them to be Gs. By 1.12, this is $\binom{14}{12} = 91$.

This example is a particular case of the general question Q9. This general question is answered by the following theorem

Theorem 1.28. *The number of ways to partition a set of n indistinguishable elements into r disjoint possibly empty subsets is*

$$\binom{n+r-1}{n}$$

Proof. Let

$$S = \{a_1, \ldots, a_n\}$$

be a set of n indistinguishable elements.

We would like to partition S into subsets $S_1, \ldots S_r$, where S_i are disjoint and $S_1 \cup \ldots \cup S_r = S$.

Since the elements $a_1, \ldots, a_n$ are indistinguishable, all we care about is the number of elements in each subset $S_1, \ldots S_n$. Let

$$n_i = |S_i|.$$

Then, in other words, the number of ways to partition S into r disjoint possibly empty subsets is the same as the number of tuples of nonnegative integers $(n_1, \ldots n_r)$ satisfying

$$n_1 + \ldots + n_r = n.$$

Hence, we are interested in counting these tuples.

We can do this by forming a string of length $n + r - 1$, where n characters are Ys and $r - 1$ characters are empty spaces. For example,

$$\underbrace{YYY}_{\#Ys \text{ represents } n_1} \overbrace{\quad}^{\text{space \#1}} \underbrace{YYYYY}_{\#Ys \text{ represents } n_2} \overbrace{\quad}^{\text{space \#2}} \ldots \overbrace{\quad}^{\text{space \#}(r-1)} \underbrace{YYYY}_{\#Ys \text{ represents } n_r}$$

which would represent a tuple $(3, 5, \ldots, 4)$. Hence, the number of tuples we are interested in is the same as the number of such strings.

The number of such strings is the same as the number of possible ways to choose n positions out of a set of $n + r - 1$ positions. By 1.12 this is is:

$$\binom{n+r-1}{n}.$$

□

Notice that an alternate way to state this theorem is:

Theorem 1.29. *The number of solutions of the equation*

$$n_1 + n_2 + \ldots + n_r = n$$

such that $n_1, n_2, \ldots, n_r$ are nonnegative integers is

$$\binom{n+r-1}{n}.$$

1.4.1 Examples

Example 1.30. What is the number of solutions in nonnegative integers of the equation

$$x_1 + x_2 + \ldots + x_{10} = 21$$

Solution. We can use Theorem 1.29 with $n = 21$ and $r = 10$. Hence, the number of solutions is

$$\binom{n+r-1}{n} = \binom{21+10-1}{21} = \binom{30}{21} = \frac{30!}{21! \times 9!}$$

Example 1.31. What is the number of ways of choosing 10 marbles from a pile of blue, red, and yellow marbles with at least 10 marbles of each colour and with marbles of the same colour being indistinguishable?

Proof. Since the marbles of each colour are indistinguishable, we only care about the number of each colour we choose. Let

$$\begin{aligned} x_r &= \#(\text{red marbles}) \\ x_b &= \#(\text{blue marbles}) \\ x_y &= \#(\text{yellow marbles}). \end{aligned}$$

Hence, we want to know how many triples (x_r, x_b, x_y) of nonnegative integers satisfying

$$x_r + x_b + x_y = 10$$

exist. By Theorem 1.29, there are

$$\binom{10+3-1}{10} = \binom{12}{10} = 66$$

ways of choosing marbles. □

Example 1.32. a) What is the number of ways of dividing 10 indistinguishable marbles into 3 cans?

b) What is the number of ways of dividing 10 indistinguishable marbles into 3 cans such that no can is empty?

Solution.

a) We apply Theorem 1.28with $n = 10$ and $r = 3$. So, there are

$$\binom{10+3-1}{10} = \binom{12}{10} = 66$$

ways.

b) Since every can has at least one marble, we first put one marble in each can. We are left with $10 - 3 = 7$ marbles to divide between the three cans. By Theorem 1.28, there are

$$\binom{7+3-1}{7} = 36$$

ways of dividing the marbles.

Example 1.33. a) What is the number of solutions in nonnegative integers of the equation

$$x_1 + x_2 + x_3 = 10$$

b) What is the number of solutions in *positive* integers of the equation

$$x_1 + x_2 + x_3 = 10$$

Solution.

a) By Theorem 1.29, this is

$$\binom{10+3-1}{10} = \binom{12}{10} = 66$$

b) We want to count all nonnegative solutions to the equation

$$x_1 + x_2 + x_3 = 10$$

such that $x_1, x_2, x_3 \geq 1$.

Let us define variables y_1, y_2, y_3 such that

$$\begin{aligned} y_1 &= x_1 - 1 \\ y_2 &= x_2 - 1 \\ y_3 &= x_3 - 1. \end{aligned}$$

Notice that $y_1, y_2, y_3 \geq 0$.

Moreover, the triple of **positive integers** (x_1, x_2, x_3) satisfies the equation

$$x_1 + x_2 + x_3 = 10 \tag{1}$$

if and only if the triple of **nonnegative integers** (y_1, y_2, y_3) satisfies the equation

$$y_1 + y_2 + y_3 = 7 \tag{2}$$

Hence, the number of positive solutions to Equation (1) the same as the number nonnegative solutions to (2).

We know from Theorem 1.29 that there are

$$\binom{7+3-1}{7} = 36$$

solutions to Equation (2).

Example 1.34. How many solutions in nonnegative integers are there to the inequality

$$x_1 + x_2 + x_3 \leq 22$$

Solution. let $y = 22 - x_1 - x_2 - x_3$. Notice that a triple of nonnegative integers (x_1, x_2, x_3) satisfies

$$x_1 + x_2 + x_3 \leq 22 \tag{3}$$

if and only if h $y \geq 0$ and the tuple (x_1, x_2, x_3, y) satisfies

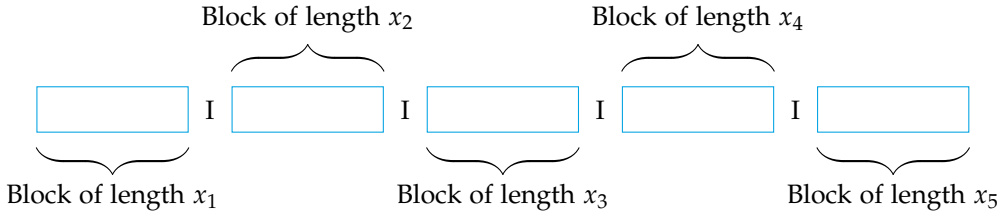
$$x_1 + x_2 + x_3 + y = 22 \tag{4}$$

Thus, the number of nonnegative solutions to Equation (3) is the same as the number of nonnegative solutions to Equation (4). By Theorem 1.29 this is

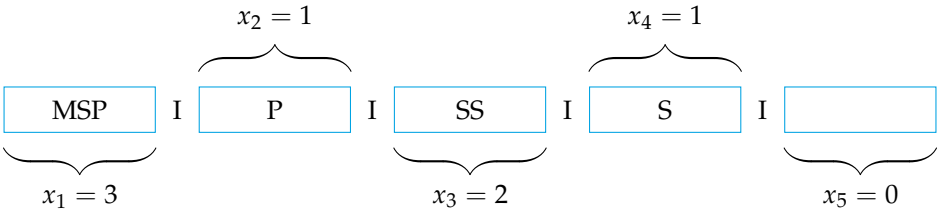
$$\binom{22+4-1}{22} = \binom{25}{22} = 2300.$$

Example 1.35. How many eleven-letter codewords can be formed by arranging the letters of the word MISSISSIPPI such that no two of the Is are adjacent?

Solution. We can imagine that the four I's are fixed, and that the other 7 letters must form five blocks of lengths x_1, x_2, x_3, x_4 and x_5.



For example we can have a string:



Notice that $x_1, x_5 \geq 0$, but x_2, x_3 and x_4 must be at least one since, otherwise, we would have consecutive Is.

We want to answer the questions:

a) How many possible ways are there to distribute the lengths of the blocks?

b) For each configuration of the blocks, how many ways are there to distribute the letters?

To answer (a), note that the number of possibilities for the length of the blocks is the number of solutions to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 7 \tag{5}$$

with $x_1, x_5 \geq 0$ and and $x_2, x_3, x_4 \geq 1$. Let

$$\begin{aligned} y_2 &= x_2 - 1 \\ y_3 &= x_3 - 1 \\ y_4 &= x_4 - 1. \end{aligned}$$

Then, the number of solutions to the Equation (5) is the same as the number of solutions to the equation

$$x_1 + y_2 + y_3 + y_4 + x_5 = 4 \tag{6}$$

which, by Theorem 1.29, is

$$\binom{4+5-1}{4} = \binom{8}{4} = 70.$$

Hence, there are 70 possible configuration of blocks around the Is.

Let us next consider question (b). For each configuration of the block, we have to distribute the 7 remaining letters: 1 M, 4 Ss, 2 Ps. To do this, we have a set of slots

$$S = \{-_1, \ldots, -_7\}$$

and we have to partition it into the sets

$$\begin{aligned} S_1 &= \{\text{Slots declared to be M}\}, \quad |S_1| = 1 \\ S_2 &= \{\text{Slots declared to be S}\}, \quad |S_2| = 4 \\ S_3 &= \{\text{Slots declared to be P}\}, \quad |S_3| = 2 \end{aligned}$$

Using Theorem 1.22, there are

$$\binom{7}{1,4,2} = \frac{7!}{4! \times 2!} = 105$$

ways of doing this.

Thus, the total number of codewords is $70 \times 105 = 7350$.

1.5 Inclusion-Exclusion Principle

By the end of this section, we should be able to answer the following question.

Q11 Find the number of positive integers less than or equal to 200 which are divisible by 3, 5, or 7. **A:** 108

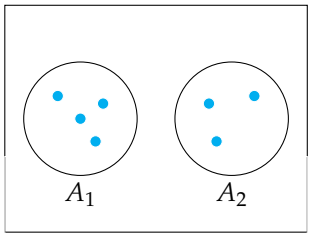
Let A and B be finite sets. Recall the **Addition Principle**: If A and B are disjoint, then

$$|A \cup B| = |A| + |B|.$$

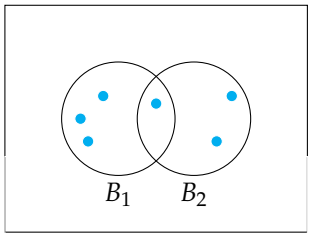
In general, however,

$$|A \cup B| \leq |A| + |B|$$

because in $|A| + |B|$, the elements of $A \cap B$ are double counted. Pictorially,



$A_1 \cup A_2$



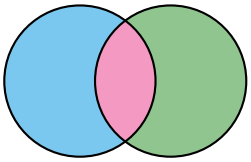
$B_1 \cup B_2$

Lemma 1.36. *Let A and B be finite sets. Then,*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Proof. This essentially follows from three observations. First, notice that $A \cup B$ has three disjoint subsets:

a) $\mathbf{A - (A \cap B)}$
b) $\mathbf{B - (A \cap B)}$
c) $\mathbf{A \cap B}$



Moreover, these three subsets are such that

$$(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B) = A \cup B$$

Finally, since the subsets appearing in the LHS are all disjoint, we can apply the addition principle:

$$\begin{aligned} |A \cup B| &= |A - (A \cap B)| + |B - (A \cap B)| + |A \cap B| \\ &= |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| \\ &\qquad \text{(Subtraction principle)} \\ &= |A| + |B| - |A \cap B| \end{aligned}$$

□

Example 1.37. Suppose now we have finite sets A, B, C. Then, the result of Lemma 1.36 can be iterated in order to compute $|A \cup B \cup C|$.

Let $X = B \cup C$. Then,

$$A \cup B \cup C = A \cup X$$

and so

$$\begin{aligned} |A \cup B \cup C| &= |A \cup X| \\ &= |A| + |X| - |A \cap X| && \text{(By Lemma 1.36)} \\ &= |A| + |B \cup C| - |A \cap X| && \text{(since } X = B \cup C\text{)} \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap X| && \text{(By Lemma 1.36)} \end{aligned}$$

Now,

$$A \cap X = A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

The latter equality can be seen via the diagrams:

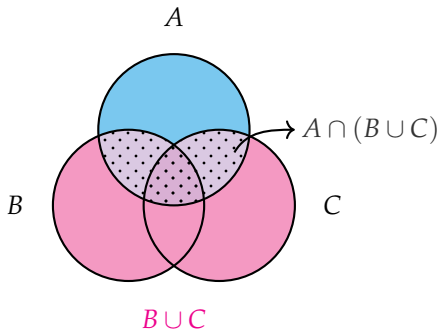


Diagram 1

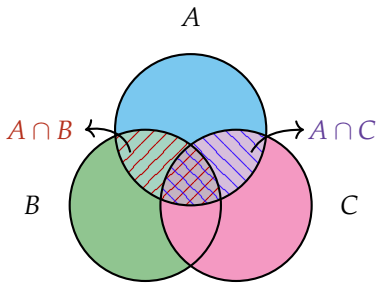


Diagram 2

Thus, by Lemma 1.36,

$$|A \cap X| = |(A \cap B) \cup (A \cap C)| = |A \cap B| + |B \cap C| - |(A \cap B) \cap (B \cap C)|.$$

Finally, notice that

$$(A \cap B) \cap (B \cap C) = A \cap B \cap C.$$

(This can also be seen in Diagram 2 above!)

Hence,

$$|A \cap X| = |A \cap B| + |A \cap C| - |A \cap B \cap C|$$

Putting this all together,

$$|A \cup B \cup C| = |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap C|$$

The general formula for when we have n sets is given by the Inclusion-Exclusion Principle.

Theorem 1.38 (Inclusion-Exclusion Principle). *Let $A_1, \ldots, A_n$ be finite sets. Then,*

$$|A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n|$$

Try to expand this formula out in the case of A_1, A_2, A_3, A_4.

Definition 1.39. Let $x \in \mathbb{R}$. Then the *floor* of x, denoted as $\lfloor x \rfloor$ is the highest integer less than or equal to x. E.g. $\lfloor 43.8 \rfloor = 43$.

Example 1.40. Find the number of positive integers less than or equal to 100 which are divisible by 3 or 7.

Solution. Consider sets

$$A = \{\text{positive integers less than or equal to 100 and divisible by 3}\},$$
$$B = \{\text{positive integers less than or equal to 100 and divisible by 7}\},$$
$$A \cup B = \{\text{positive integers less than or equal to 100 and divisible by 3 or 7}\}$$

We thus want to find $|A \cup B|$. By the Inclusion-Exclusion principle,

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{7}$$

a) Finding $|A|$.

An integer d is divisible by 3 if $d = 3 \times n$ for some integer n. We can therefore list all of the integers smaller than or equal to 100 which are divisible by 3 as:

$$3 \times 1, \quad 3 \times 2 \quad , \quad \ldots \quad , \quad \underbrace{3 \times 33}_{\substack{33 \text{ is the highest} \\ \text{integer } n \text{ such} \\ \text{that } 3 \times n \leq 100}} \quad , \quad \cancel{3 \times 34};$$

Hence,

$$|A| = \begin{pmatrix} \text{highest integer } n \\ \text{such that} \\ 3 \times n \leq 100 \end{pmatrix} = 33$$

where we found that the highest such integer was 33 by trial and error. More easily,

$$\begin{pmatrix} \text{highest integer } n \\ \text{such that} \\ 3 \times n \leq 100 \end{pmatrix} = \lfloor \frac{100}{3} \rfloor = 33$$

b) Finding $|B|$

Similarly, $|B| = \lfloor \frac{100}{7} \rfloor = 14$.

c) Finding $|A \cap B|$

Observe that

$$\begin{aligned} A \cap B &= \{\text{positive integers less than or equal to 100 and divisible by 3 and 7}\} \\ &= \{\text{positive integers less than or equal to 100 and divisible by } 3 \times 7 = 21\} \end{aligned}$$

Thus,

$$|A \cap B| = \lfloor \frac{100}{21} \rfloor = 4.$$

Subbing all this back into Equation (7),

$$|A \cup B| = 33 + 14 - 4 = 43.$$

Example 1.41. An Enigma machine has 5 rotors. Each day 3 rotors must be chosen in order, subject to the condition that no rotor may be chosen in the same position on two consecutive days. Given yesterday's choice, how many choices are possible today?

Solution. Let

$$S = \{\text{rotor 1}, \text{rotor 2}, \text{rotor 3}, \text{rotor 4}, \text{rotor 5}\}$$

be the set of 5 rotors. A choice of 3 rotors in order corresponds to a 3-permutation of S, and so the set of all possible choices is $P(S, 3)$.

Suppose that the choice of rotors yesterday was:

$$\text{rotor } a, \text{ rotor } b, \text{ rotor } c.$$

Let

$$\begin{aligned} A_1 &= \{\text{3-permutations with the same rotor as yesterday in position 1}\} \\ &= \{\text{rotor } a, \text{ rotor } i, \text{ rotor } j \mid \text{ rotor } i, \text{ rotor } j \in P(S - \{\text{rotor } a\}, 2)\} \end{aligned}$$

Define A_2 and A_3 similarly. Then, the set of possible choices today where at least one rotor is in the same position as it was yesterday is $A_1 \cup A_2 \cup A_3$. Hence, using the Inclusion-Exclusion Principle, the number of desired choices today is

$$\begin{aligned} |P(S,3) - A_1 \cup A_2 \cup A_3| &= |P(S,3)| - |A_1 \cup A_2 \cup A_3| \\ &= \frac{5!}{2!} - |A_1 \cup A_2 \cup A_3| \quad \text{(By Theorem 1.10)} \\ &= 60 - |A_1| - |A_2| - |A_3| \\ &\quad + |A_1 \cap A_2| + |A_2 \cap A_3| + |A_1 \cap A_2| \\ &\quad - |A_1 \cap A_2 \cap A_2| \qquad (8) \end{aligned}$$

Therefore, it suffices to find the cardinalities of the sets in Equation (8).

First, notice that an element of A_1 is a sequence

$$\text{rotor } a, \text{rotor } i, \text{rotor } j$$

where rotor i, rotor j is a 2-permutation of $S - \{\text{rotor } a\}$. So every element of A_1 corresponds to exactly one element of $P(S - \{\text{rotor} a\}, 2)$ and vice-versa. Therefore,

$$|A_1| = |P(S - \{\text{rotor } a\}, 2)| = \frac{4!}{2!} = 12$$

Similarly,

$$|A_2| = |A_3| = \frac{4!}{2!} = 12.$$

Next, consider the set

$$A_1 \cap A_2 = \{\text{rotor } a, \text{ rotor } b, \text{ rotor } j \mid \text{ rotor } j \in S - \{\text{rotor } a, \text{ rotor } b\}\}.$$

Every element of this set corresponds to exactly one element of the set $S - \{\text{rotor } a, \text{rotor } b\}$ and vice-versa. Therefore,

$$|A_1 \cap A_2| = |S - \{\text{rotor } a, \text{rotor } b\})| = 3$$

Similarly,

$$|A_1 \cap A_3| = |A_2 \cap A_3| = 3.$$

Finally, observe that

$$A_1 \cap A_2 \cap A_3 = \{\text{rotor } a, \text{ rotor } b, \text{ rotor } c\}$$

and so it only has one element.

Putting all of this into Equation 2, we get that

$$|A_1 \cup A_2 \cup A_3| = 28$$

and so, subbing this into Equation 1, we get that the number of desired choices today is

$$60 - 28 = 32.$$

1.6 Derangements

Definition 1.42. A derangement of an n-permutation is a new permutation with the same n elements and where no element appears in its original position.

Example 1.43. Let $S = \{1, 2, 3, 4, 5\}$. What are examples of derangement of the permutation: 1234?

Solution. There are 9 of them. Here are a few: $2341, 2413, 2341, \ldots$

Example 1.44. Let $S = \{1, 2, 3\}$ and write d_3 for the number of derangements of the permutation $1, 2, 3$. What is d_3?

Solution. Let

$$\begin{aligned} A_1 &= \{\text{3-permutations of } S \text{ with element 1 in position 1}\} \\ &= \{1, a_2, a_3, \mid a_2, a_3 \in P(S - \{1\}, 2)\}\}. \end{aligned}$$

Define A_2 and A_3 similarly. Then, $A_1 \cup A_2 \cup A_3$ is the set of 3-permutations of S where there is at least one element $i \in S$ which is in position i.

Therefore, the set of derangements of $1, 2, 3$ is

$$P(S, 3) - A_1 \cup A_2 \cup A_3.$$

Hence,

$$d_3 = |P(S,3)| - |A_1 \cup A_2 \cup A_3| = 3! - |A_1 \cup A_2 \cup A_3| \qquad (9)$$

To compute $|A_1 \cup A_2 \cup A_3|$ we will use some facts:

a) $|A_1| = |A_2| = \ldots = |A_n| = (3-1)! = 2! = 2$, [Why?]

b) $|A_1 \cap A_2| = |A_1 \cap A_3| = |A_2 \cap A_3| = (3-2)! = 1! = 1$, [Why?]

c) $|A_1 \cap A_2 \cap A_3| = |(3-3)! = 0! = 1$. [Why?]

By the Inclusion-Exclusion Principle,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = &|A_1| + |A_2| + |A_3| \\ &- |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &+ |A_1 \cap A_2 \cap A_3| \end{aligned}$$

which simplifies to

$$|A_1 \cup A_2 \cup A_3| = 2+2+2-1-1-1+1 = 4.$$

Plugging this back into Equation (9),

$$d_3 = 3! - 4 = 2.$$

In general,

Theorem 1.45. *Let $S = \{a_1, \ldots, a_n\}$ and write d_n for the number of derangements of the permutation $a_1, a_2, \ldots, a_n$. Then,*

$$d_n = n! \times \sum_{i=0}^{n} \frac{(-1)^i}{i!}.$$

Proof. Let

$$A_i = \{n\text{-permutations of } S \text{ with element } a_i \text{ in position } i\}.$$

E.g. A_1 is the set of n-permutations of S which look like

$$a_1, a_{i_2}, \ldots, a_{i_n}$$

Then,

$$A_1 \cup \ldots \cup A_n = \{n\text{-permutations which have } a_i \text{ in position } i \text{ for at least one } i\}$$

I.e. $A_1 \cup \ldots \cup A_n$ is the set of permutations where there is one i such that a_i is in its original position.

Therefore, the set of derangements of $a_1, a_2, \ldots, a_n$ is

$$P(S,n) - A_1 \cup \ldots \cup A_n$$

Hence,

$$d_n = |P(S,n)| - |A_1 \cup \ldots \cup A_n| = n! - |A_1 \cup \ldots \cup A_n| \qquad (10)$$

To compute $|A_1 \cup \ldots \cup A_n|$ we will use some facts:

a) Let r be an integer with $1 \leq r \leq n$. Then,

$$|A_1 \cap \ldots \cap A_r| = (n-r)!.$$

In fact, the intersection of any combination of r subsets

$$A_{i_1} \cap \ldots \cap A_{i_r}$$

chosen from the list $A_1, \ldots, A_n$ has $(n-r)!$ elements. [Why? Hint: The permutations in this intersection are the same thing as permutation of the $n-r$ elements which are not fixed in the intersection]

b) There are $\binom{n}{r}$ combinations of r subsets chosen from the list $A_1, \ldots, A_n$. [Why?]

By the Inclusion-Exclusion Principle,

$$|A_1 \cup \ldots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \ldots + \sum_{i_1<\ldots<i_r} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}| + \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n| \tag{11}$$

From fact (a) with $r = 1$, we know that

$$\begin{aligned} \sum_i |A_i| &= |A_1| + \ldots + |A_n| \\ &= \underbrace{(n-1)! + (n-1)! + \ldots + (n-1)!}_{n \text{ times}} \\ &= n \times (n-1)! \\ &= \frac{n!}{1!}. \end{aligned} \tag{12}$$

Similarly, by fact (a) with $r = 2$,

$$\begin{aligned} \sum_{i<j} |A_i \cap A_j| &= \underbrace{|A_1 \cap A_2| + |A_1 \cap A_3| + \ldots + |A_{n-1} \cap A_n|}_{\substack{\text{Summing over all possible combinations of 2 subsets chosen from the list } A_1, \ldots, A_n. \\ \text{By fact (b), there are } \binom{n}{2} \text{ combinations.}}} \\ &= \underbrace{(n-2)! + \ldots + (n-2)!}_{\binom{n}{2} \text{ times}} \\ &= \binom{n}{2} \times (n-2)! \\ &= \frac{n!}{2!}. \end{aligned} \tag{13}$$

In fact, by fact (a), for each $3 \leq r \leq n$,

$$\sum_{i_1<i_2<\ldots<i_r} |A_{i_1} \cap \ldots \cap A_{i_r}| = \underbrace{|A_1 \cap A_2 \cap \ldots \cap A_r| + |A_2 \cap A_3 \cap \ldots \cap A_r \cap A_{r+1}| + \ldots}$$

Summing over all possible combinations of r subsets chosen from the list $A_1, \ldots, A_n$.
By fact (b), there are $\binom{n}{r}$ combinations.

$$= \underbrace{(n-r)! + \ldots + (n-r)!}_{\binom{n}{r} \text{ times}}$$

$$= \binom{n}{r} \times (n-r)!$$

$$= \frac{n!}{r!}. \tag{14}$$

Substituting Equations (12)-(14) in Equation (11) we get that

$$|A_1 \cup \ldots \cup A_n| = \underbrace{\frac{n!}{1!}}_{\substack{r=1\\ \text{subsets}}} - \underbrace{\frac{n!}{2!}}_{\substack{r=2\\ \text{subsets}}} + \underbrace{\frac{n!}{3!}}_{\substack{r=3\\ \text{subsets}}} - \ldots + (-1)^n \underbrace{\frac{n!}{n!}}_{\substack{r=n\\ \text{subsets}}}$$

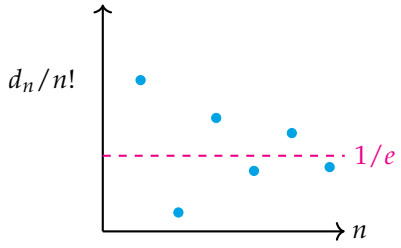
Substituting this expression into Equation (10) gives us

$$\begin{aligned} d_n &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \ldots + (-1)^n \frac{n!}{n!} \\ &= n! \times \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}\right) \\ &= n! \times \sum_{i=0}^{n} \frac{(-1)^i}{i!}. \end{aligned}$$

□

Corollary 1.46. *As $n \to \infty$, then $\frac{d_n}{n!} \to \frac{1}{e}$.*

Proof. From Theorem 1.45, $\frac{d_n}{n!} = \sum_{i=0}^{n} \frac{(-1)^i}{i!} \to \frac{1}{e}$ as $n \to \infty$. The graph would look something like this:



□

Example 1.47. For Secret Santa, n people throw their name into a hat. Each person then takes out a name from the hat at random. In the limit for very large n, what is the probability that no participant gets their own name back?

Solution. Let P be the probability that no participant gets their own name back. Then,

$$P = \frac{\text{\# outcomes where no participant gets their own name}}{\text{\#outcomes}}$$

We can compute P by considering the set of all names,

$$S = \{\text{name } 1, \ldots, \text{name } n\}.$$

An outcome is the same an n-permutation of S. For example, the permutation

$$\text{name } n, \text{name } n-1, \ldots, \text{name } 1$$

represents the outcome where the first participant gets name n, the second gets name $n-1$ and so on.

By Theorem 1.10, there are $n!$ permutations, and so the number of all outcomes is $n!$.

To compute the number of outcomes where no participant gets their own name, consider the permutation of S:

$$\text{name } 1, \text{name } 2, \ldots, \text{name } n.$$

which represents the outcome where *everyone* gets their own name back.

Then, the outcomes where no one gets their own name back are the same as the derangements of this permutation.

Thus, the number of outcomes where no one gets their own name back is d_n

Therefore, $P = \frac{d_n}{n!}$ and so, by Corollary 1.46, as $n \to \infty$, then $\frac{d_n}{n!} \to 1/e$. Hence, in the limit of very large n,

$$P = \frac{1}{e} \sim 0.37$$

1.7 Recurrence Relations

Example 1.48. Suppose that a loan of £100 is repaid by monthly instalments of £5, and that each month interest of 2% is added to the remaining balance. Let the remaining balance at the end of the nth month be a_n pounds. Compute a_n

Solution.

$$\boxed{a_0 = 100} \qquad \text{(starting balance)}$$

$$a_1 = \underbrace{1.02 \times a_0}_{\text{add 2\% interest to the balance at the end of the previous month}} \overbrace{-\ 5}^{\text{pay £5}}$$

$$\vdots$$

$$\boxed{a_n = 1.02 \times a_{n-1} - 5}$$

This allows us to construct a sequence:

$$\begin{aligned} a_0 &= 100 \\ a_1 &= 97 \\ a_2 &= 93.94 \\ a_3 &= 90.82 \\ &\vdots \end{aligned}$$

In the example above we defined a sequence (a_n) by defining the nth term of the sequence as an expression of the previous terms. Such an expression is called a **recurrence relation**.

We used this relation to compute the terms $a_1, a_2, \ldots$ successively starting with the value a_0 which we declared to be 100. The specification $a_0 = 100$ is called the **initial condition**.

In some cases, it is possible to find a formula for a_n in terms of n. This is called solving the recurrence relation with initial conditions .

1.7.1 Iteration

In simple cases, we can sometimes solve the recurrence relation with initial conditions using *iteration*.

Example 1.49. Solve the recurrence relation

$$a_n = 1.02 \times a_{n-1} - 5 \quad (n \geq 1)$$

with $a_0 = 100$.

Solution. Applying the recurrence relation again and again:

$a_1 = 1.02 \times a_0 - 5 - 5$

$a_2 = 1.02 \times a_1 - 5 = 1.02 \times \big(1.02 \times a_0 - 5\big) - 5 = 1.02^2 \times a_0 - (1.02 + 1) \times 5$

$a_3 = 1.02 \times a_2 - 5 = 1.02 \times \big(1.02^2 \times a_0 - (1.02 + 1) \times 5\big) - 5 = 1.02^3 \times a_0 - (1.02^2 + 1.02 + 1) \times 5$

From these first three terms, it is reasonable to guess that a_n must satisfy the formula:

$$a_n = 1.02^n \times a_0 - (1.02^{n-1} + 1.02^{n-2} + \ldots + 1.02 + 1) \times 5. \qquad (15)$$

As you will show in your tutorial sheet, it follows by induction that a_n satisfies Equation (15). We can further simplify this equation by using the geometric series to show that

$$(1.02^{n-1} + 1.02^{n-2} + \ldots + 1.02 + 1) = \frac{1 - 1.02^n}{1 - 1.02} = 50 \times (1.02^n - 1)$$

so that

$$\begin{aligned} a_n &= 1.02^n \times a_0 - 250 \times (1.02^n - 1) \\ &= (a_0 - 250) \times 1.02^n + 250 \end{aligned}$$

Finally, to get a closed formula for a_n only in terms of n, we sub the initial condition $a_0 = 100$ into the Equation above

$$a_n = 250 - 150 \times 1.02^n.$$

1.7.2 First Order Linear Recurrence Relations with Constant Coefficients

A first order linear recurrence relation with constant coefficients is a recurrence relation of the form

$$a_n = Aa_{n-1} + B(n)$$

where A is a nonzero constant and $B(n)$ is an expression in terms of n.

Example 1.50. The recurrence relation

$$a_n = a_{n-1} + 3^{n-1}$$

is a first order linear recurrence relation.

As you will show in your tutorial exercises, if $B(n) = C$ is a constant, we can always use the iteration process in Example 1.49 to solve these recurrence relations. In fact, you will show that a recurrence relation of this form always has the general solution:

$$a_n = K \cdot A^n + \frac{1 - A^n}{1 - A} \times C$$

where K is a constant to be determined by initial conditions.

Example 1.51. If we substitute $A = 1.02$ and $B(n) = -5$ in the equation above, then we recover the solution of Example 1.49.

1.7.3 Second Order Linear Recurrence Relations with Constant Coefficients

It is not always possible to use the iteration method to solve more complicated recurrence relations with initial conditions. For example, it is not generally possible to solve *second order recurrence relations* using iteration.

A second order linear recurrence relation with constant coefficients is a recurrence relation of the form

$$a_n = Aa_{n-1} + Ba_{n-2} + C(n)$$

where A, B are nonzero constants and $C(n)$ is an expression in terms of n.

If $C = 0$, then the recurrence relation is homogeneous.

1.7.4 Solving Homogenous Second Order Recurrence Relations

We will learn how to solve the recurrence relation

$$a_n = Aa_{n-1} + Ba_{n-2} \tag{16}$$

The process of solving homogeneous second order recurrence relations is very similar to the process of solving second order ODEs (which you might have learned in Maths 1 or 2D)!

The main idea is the following: If we can find two linearly independent expressions f_n and g_n in terms of n which both satisfy Equation (16) (I.e. f_n and g_n satisfy the rules

$$f_n = Af_{n-1} + Bf_{n-2}$$
$$g_n = Ag_{n-1} + Bg_{n-2}.$$

as in Equation (16)), then the general solution to Equation (16) will be

$$a_n = K \times f_n + L \times g_n$$

where K and L are constants to be determined by initial conditions.

Example 1.52. Let's consider a recurrence relation

$$a_n = 5a_{n-1} - 6a_{n-2} \tag{17}$$

with initial conditions $a_0 = 0$ and $a_1 = 1$.

We can try to guess two expressions f_n and g_n which satisfy Equation (16).

Let's guess $f_n = 2^n$. Then we can check that it satisfies Equation (16):

$$5f_{n-1} - 6f_{n-2} = 5 \times 2^{n-1} - 6 \times 2^{n-2} = 2^{n-2} \times (5 \times 2 - 6) = 2^{n-2} \times 2^2 = 2^n = f_n$$

Similarly, $g_n = 3^n$ satisfies Equation (16).

Hence, the general solution to Equation (16) is:

$$a_n = K \times 2^n + L \times 3^n,$$

where we can find the constants K and L by subbing in our initial conditions.

Since $a_0 = 0$ and $a_1 = 1$, then

$$\begin{aligned} 0 = a_0 &= K \times 2^0 + L \times 3^0 = K + L \\ 1 = a_1 &= 2K + 3L \end{aligned}$$

Solving the equations for K and L gives $K = -1$ and $L = 1$. That is, the solution is

$$a_n = -2^n + 3^n. \quad \square$$

In the example above, we just guessed the expressions $f_n = 2^n$ and $g_n = 3^n$. However, guessing random functions isn't a very efficient process to solve these equations!

Q12 What is an efficient way to guess expressions f_n and g_n which will satisfy Equation (16)?

A: Let's say we have a recurrence relation as in Equation (16). We can try to guess a function $f_n = t^n$, where t is any nonzero number, and we can "force" f_n to satisfy Equation (16).

The expression $f_n = t^n$ satisfies Equation (16) if and only

$$\begin{aligned} & f_n = Af_{n-1} + fh_{n-2} \\ \iff & t^n = At^{n-1} + Bt^{n-2} \\ \iff & t^n - At^{n-1} - Bt^{n-2} = 0 \\ \iff & t^{n-2} \times (t^2 - At - B) = 0. \end{aligned}$$

Since $t \neq 0$, the equation above is satisfied if and only if

$$t^2 - At - B = 0. \tag{18}$$

Hence, f_n satisfies Equation (16) if and only if t is a root of the Equation (18). Equation (18) is called the auxiliary equation associated to Equation (16).

If the auxiliary equation has two distinct roots α and β, then this means we have found two expressions $f_n = \alpha^n$ and $g_n = \beta^n$ which satisfy the recurrence relation! In other words, we have proved the theorem:

Theorem 1.53. *If the auxiliary equation has two distinct roots α and β, then the general solution of Equation (16) is*

$$a_n = K \times \alpha^n + L \times \beta^n$$

where K and L are constants to be determined by the initial conditions.

Note: This method also works for homogeneous first order recurrence relations. In the first order case, $B = 0$ and so the auxiliary equation is:

$$0 = t^2 - At = t \times (t - A)$$

which has one root $\alpha = A$. When working with first order recurrence relations, we only need to find one linearly independent solution and so the general solution is:

$$a_n = K \cdot A^n$$

where K is a constant to be determined by initial conditions.

Example 1.54. Consider again a recurrence relation in Equation (17)

$$a_n = 5a_{n-1} - 6a_{n-2}$$

with $a_0 = 0$ and $a_1 = 1$. Then, $A = 5$, $B = -6$ and so the auxiliary equation is:

$$0 = t^2 - 5t + 6 = (t-2)(t-3).$$

which has roots $\alpha = 2$ and $\beta = 3$. Hence, the solution to this recurrence relation is

$$a_n = K \times 2^n + L \times 3^n$$

where K and L can be determined by the initial conditions:

$$0 = a_0 = K \times 2^0 + L \times 3^0 = K + L$$
$$1 = a_1 = 2K + 3L$$

Solving the equations for K and L gives $K = -1$ and $L = 1$. That is, the solution is

$$a_n = -2^n + 3^n. \quad \square$$

In examples, we will run into cases where the auxiliary equation only has one (repeated) root. To solve these cases we will need:

Theorem 1.55. *If the auxiliary equation has only one root α, then the general solution of Equation (16) is*

$$a_n = K \times \alpha^n + L \times n \times \alpha^n$$

where K and L are constants to be determined by the initial conditions.

Example 1.56. Solve the recurrence relation

$$a_n = 4a_{n-1} - 4_{n-2}$$

with $a_1 = 1$ and $a_2 = 3$.

Solution. Here, $A = 4$, $B = -4$, and so the auxiliary equation is

$$0 = t^2 - 4t + 4 = (t-2)^2.$$

which has only one root $\alpha = 2$, and so the general solution is:

$$a_n = K \times 2^n + L \times n \times 2^n = 2^n \times (K + L \times n)$$

where K and L are constants to be determined by the initial conditions:

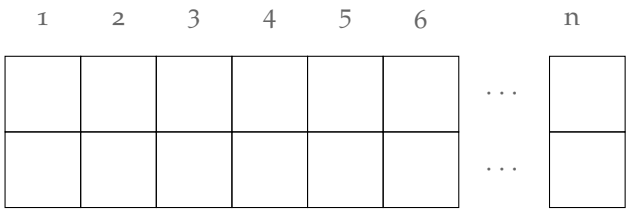
$$1 = a_1 = 2K + 2L$$
$$3 = a_2 = 4K + 8L.$$

These equations imply that $K = L = 1/4$. Thus, the solution is

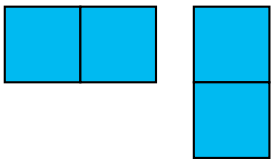
$$a_n = \frac{2^n}{4} \times (1 + n).$$

1.7.5 Combinatorial Example

Imagine you have a $2 \times n$ board:

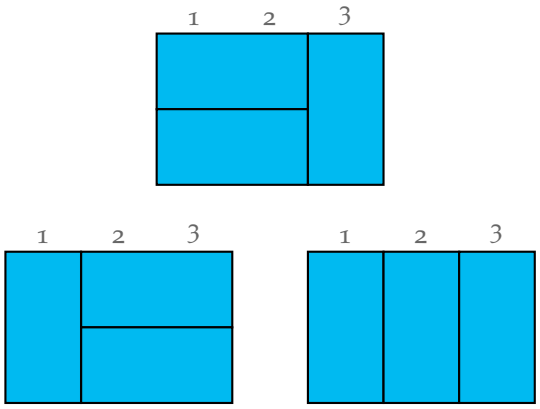


and let's say we have dominos



A **tiling** of a $2 \times n$ board is a a placement of identical domino pieces filling out the board entirely.

For example, there are 3 possible tilings of a 2×3-board is:



The question we will answer is: How many possible tilings are there of a $2 \times n$ board?

Solution. Let b_n denote the number of tilings of a $2 \times n$ board. We will first show that

a) $b_0 = 1$, $b_1 = 1$

b) $b_n = b_{n-1} + b_{n-2}$.

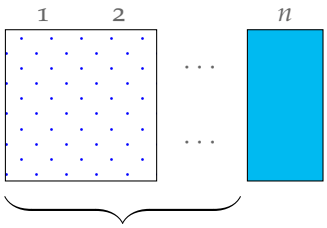
and then we will solve this recurrence relation.

a) We will just establish by convention that there is only one way to tile a 2×0 board: You don't tile it at all! Hence, $b_0 = 1$.

   Moreover, there is only one way to tile a 2×1 board: we place a vertical domino in column 1, hence $b_1 = 1$.

b) To prove (b), let's say we will start tiling the $2 \times n$ board from the right. Notice that we can start tiling in one of two possible ways:

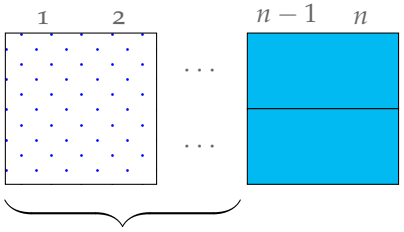
(1) We place a vertical domino in column n. Then, we are left with a $2 \times (n-1)$ board which needs to be tiled. There are b_{n-1} ways to tile this board.



Any tiling of a $2 \times (n-1)$-board

$\implies$ There are b_{n-1} possible tilings if we start this way.

(2) We place two horizontal dominos in columns $n-1$ and n. Then, we are left with a $2 \times (n-2)$ board which needs to be tiled. There are b_{n-2} ways to tile this board.



Any tiling of a $2 \times (n-2)$-board

$\implies$ There are b_{n-2} possible tilings if we start this way.

Thus, the number of total possible ways to tile a $2 \times n$ board is

$$b_n = b_{n-1} + b_{n-2}$$

c) All that's left to do is solve the recurrence relation

$$b_n = b_{n-1} + b_{n-2}$$

with $b_0 = b_1 = 1$.

This is a second order homogenous linear recurrence relation with constant coefficients, hence we start by writing down the auxiliary equation

$$t^2 - 1 - 1 = 0$$

which has roots

$$\alpha = \underbrace{\frac{1+\sqrt{5}}{2}}_{\text{Golden ratio}}$$

$$\beta = \frac{1-\sqrt{5}}{2}.$$

Therefore, the general solution is:

$$b_n = K \times \left(\frac{1+\sqrt{5}}{2}\right)^n + L \times \left(\frac{1-\sqrt{5}}{2}\right)^n$$

where K and L are constants. Plugging in the initial conditions

$$1 = b_0 = K + L$$
$$1 = b_1 = K \times \left(\frac{1+\sqrt{5}}{2}\right) + L \times \left(\frac{1-\sqrt{5}}{2}\right)$$

Solving for K and L gives

$$K = \frac{1}{\sqrt{5}}$$
$$L = -\frac{1}{\sqrt{5}}.$$

Thus,

$$b_n = \frac{1}{\sqrt{5}} \times \left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

The sequence (b_n) is the *Fibonacci Sequence*.

1.7.6 Solving Inhomogenous Recurrence Relations

We will learn how to solve recurrence relations of the form

$$a_n = Aa_{n-1} + Ba_{n-2} + C(n) \tag{19}$$

where A and B are constants (with $A \neq 0$) and $C(n)$ is a nonzero expression in terms of n.

We say that the homogeneous equation associated to Equation (19) is

$$a_n = Aa_{n-1} + Ba_{n-2}. \tag{20}$$

A special solution to Equation (19) is any expression $a_n^{(s)}$ in terms of n which satisfies Equation (19).

Example 1.57. Consider the recurrence relation

$$a_n = a_{n-1} + 3^{n-1}.$$

Then, the expression $a_n^{(s)} = \frac{1}{2} \times 3^n$ is a special solution to this recurrence relation since:

$$a_{n-1}^{(s)} + 3^{n-1} = \frac{1}{2} \times 3^{n-1} + 3^{n-1} = \frac{3}{2} \times 3^{n-1} = \frac{1}{2} \times 3^n = a_n^{(s)}$$

Theorem 1.58. *Suppose we have a recurrence relation as in Equation (19). Let $a_n^{(h)}$ be the general solution to the associated homogeneous recurrence relation. Let $a_n^{(s)}$ be any special solution to Equation (19). Then, the general solution to Equation (19) is:*

$$a_n = a_n^{(h)} + a_n^{(s)}.$$

Example 1.59. Solve the recurrence relation

$$a_n = a_{n-1} + 3^{n-1}$$

with $a_0 = 1$.

Solution.

The recurrence relation has special solution $a_n^{(s)} = \frac{1}{2} \times 3^n$.

The homogeneous recurrence relation associated to it is

$$a_n = a_{n-1}$$

which is a first order recurrence relation with $A = 1$. Hence, it has general solution

$$a_n^{(h)} = 1^n \times a_0^{(h)} = a_0^{(h)}$$

where $a_0^{(h)}$ is a constant to be determined later.

Therefore, the general solution to the recurrence relation is:

$$a_n = a_n^{(s)} + a_n^{(h)} = \frac{1}{2} \times 3^n + a_0^{(h)}.$$

Plugging in the initial condition:

$$1 = a_0 = \frac{1}{2} \times 3^0 + a_0^{(h)}$$

and solving for $a_0^{(h)}$ gives

$$a_0^{(h)} = \frac{1}{2}$$

Therefore,

$$a_n = \frac{1}{2} \times (3^n + 1).$$

Q13 How to determine special solutions $a_n^{(s)}$?

A: We can try to make educated guesses– Special solutions are usually similar to $C(n)$, hence try guessing expressions which are similar to $C(n)$. For example,

$C(n)$	Try for $a_n^{(s)}$
$c \times r^n$ for $c, r \in \mathbb{R}$	$K \times r^n$ for $K \in \mathbb{R}$
$c \times e^{r \times n}$ for $c, r \in \mathbb{R}$	$K \times e^{r \times n}$
$c_1 \cos(r_1 \times n) + c_2 \sin(r_2 \times n)$ for $c_1, c_2, r_1, r_2 \in \mathbb{R}$	$K_1 \cos(r_1 \times n) + K_2 \sin(r_2 \times n)$ for $K_1, K_2 \in \mathbb{R}$
$c_0 + c_1 n + c_2 n^2 + \ldots + c_j n^j$ for $c_0, \ldots, c_j \in \mathbb{R}$ with $c_j \neq 0$	$K_0 + K_1 n + K_2 n^2 + \ldots + K_j n^j$ for $K_0, \ldots, K_j \in \mathbb{R}$ with $K_j \neq 0$.

Note: If $C(n) = c_j n^j$, still need to try $K_0 + K_1 n + K_2 n^2 + \ldots + K_j n^j$ not just $K_j n^j$.

In certain cases, we can we more precise.

Consider a recurrence relation as in Equation (19), and suppose that it is a second order recurrence relation. I.e. suppose that $B \neq 0$.

The homogeneous recurrence relation associated to Eq (19) has the auxiliary equation:

$$0 = t^2 - At - B$$

with roots α and β.

Lemma 1.60. *If $C(n) = c \times r^n$, where c is a constant, then*

a) If $r \neq \alpha$ and $r \neq \beta$, then $a_n^{(s)} = K \times r^n$, where K is a constant.

b) If $r = \alpha \neq \beta$, then $a_n^{(s)} = K \times n \times r^n$, where K is a constant.

c) If $r = \alpha = \beta$, then $a_n^{(s)} = K \times n^2 \times r^n$, where K is a constant.

Note: This also applies to first order recurrence relations. I.e. if $a_n = A \times a_{n-1} + c \times r^n$, and if $A \neq r$, then $a_n^{(s)} = K \times r^n$. If $A = r$, then $a_n^{(s)} = K \times n \times r^n$.

Example 1.61. Solve the recurrence relation

$$a_n = 3a_{n-1} + 10a_{n-2} + 7 \times 5^n \qquad \text{(Equation 3)}$$

with $a_0 = 4$ and $a_1 = 3$.

Solution. (1) First find $a_n^{(h)}$.

The associated homogeneous recurrence relation is

$$a_n = 3a_{n-1} + 10a_{n-2}$$

which has auxiliary equation

$$0 = t^2 - 3t - 10 = (t-5)(t+2)$$

with roots $\alpha = 5$ and $\beta = -2$.

Thus,

$$a_n^{(h)} = K' \times 5^n + L' \times (-2)^n.$$

where K' and L' are constants to be determined later.

(2) Next find $a_n^{(s)}$.

Since $C(n) = 7 \times 5^n$, then $C(n)$ is as in Lemma 1.60 (b). Thus, the special solution is

$$a_n^{(s)} = K \times n \times 5^n$$

for some constant K, which is part of our guess. To find K, we plug $a_n^{(s)}$ into the recurrence relation in Eq (19) and solve for K:

$$K \times n \times 5^n = 3 \times K \times (n-1) \times 5^{n-1} + 10 \times K \times (n-2) \times 5^{n-2} + 7 \times 5^n$$

Solving for K gives $K = 5$. Thus,

$$a_n^{(s)} = n \times 5^{n+1}$$

(3) Solve Equation (19)

The general solution to Eq. (19) is:

$$a_n = a_n^{(h)} + a_n^{(s)} = K' \times 5^n + L' \times (-2)^n + n \times 5^{n+1}$$

Now that we have the full general solution, we can plug in the initial conditions to find K' and L'.

Plugging in initial conditions:

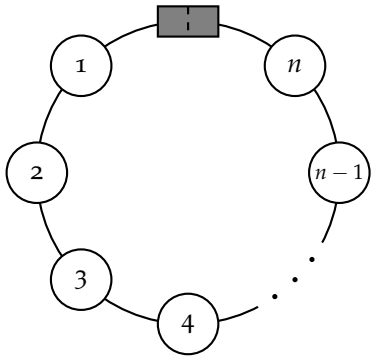
$$4 = a_0 = K' + L'$$
$$3 = a_1 = 5K' - 2L' + 25$$

Solving for K' and L' gives $K' = -2$ and $L' = 6$. Thus, ,

$$a_n = n \times 5^{n+1} - 2 \times 5^n + 6 \times (-2)^n.$$

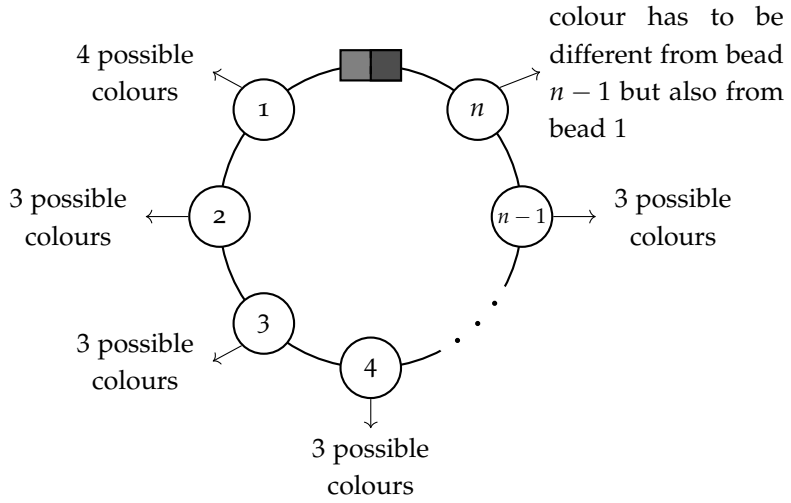
1.7.7 Combinatorial Example 2

Suppose we have a bracelet with n beads:



Let b_n be the number of ways of colouring these beads pink, yellow, green, blue such that adjacent beads have different colours (Note: Bead 1 and bead n are adjacent). What is b_n?

Solution. If we begin by colouring bead 1:



How to count the possibilities of the last bead?

Notice that

$$\underbrace{\#\begin{pmatrix}\text{bracelets with bead}\\ n \text{ painted a different colour than}\\ \text{beads } n-1 \textbf{ and } 1\end{pmatrix}}_{b_n} = \underbrace{\#\begin{pmatrix}\text{bracelets with bead}\\ n \text{ painted a different colour than}\\ \text{bead } n-1\end{pmatrix}}_{M} - \underbrace{\#\begin{pmatrix}\text{bracelets with bead}\\ n \text{ painted a different colour than } n-\\ 1 \text{ but same colour}\\ \text{as } 1\end{pmatrix}}_{N}$$

and so we just need to compute M and N.

Well, we can compute M in the following way: There are 4 possible colours for bead 1, 3 possible colours for beads $2, 4, \dots n$. Therefore,

$$M = 4 \times 3^{n-1}.$$

Next, we compute N. In these cases, the colour of bead n is determined by bead 1. So, to compute N, we need to count how many ways there are to colour beads $1, 2, \dots n-1$ such that

a) Adjacent beads have different colours,

b) Bead $n-1$ has a different colour than bead 1.

Notice that this is just b_{n-1} (i.e. it is the number of ways to colour a bracelet with $n-1$ beads such that adjacent beads have different colours).

Thus, b_n is given by the recurrence relation:

$$b_n = M - N = 4 \times 3^{n-1} - b_{n-1}. \tag{21}$$

The initial condition is $b_1 = 0$, since the first bead is adjacent to itself and so there is no way to colour one bead such that adjacent beads have different colours.

All that's left is to solve this recurrence relation! To do this, we need to find $b_n^{(h)}$ and $b_n^{(s)}$.

The associated homogeneous equation is:

$$b_n^{(h)} = -b_{n-1}^{(h)}$$

which has general solution

$$b_n^{(h)} = (-1)^n \times b_0^{(h)}.$$

For a special solution, since $C(n) = 4 \times 3^{n-1}$ (and $3 \neq -1$) we can try

$$b_n^{(s)} = K \times 3^n.$$

Plugging $b_n^{(s)}$ into Equation (21)

$$K \times 3^n = 4 \times 3^{n-1} - K \times 3^{n-1}$$

and solving for K gives $K = 1$.

Thus, the general solution to Equation (21)is:

$$b_n = b_n^{(h)} + b_n^{(s)} = (-1)^n \times b_0^{(h)} + 3^n.$$

Plugging in initial conditions,

$$0 = b_1 = -b_0^{(h)} + 3$$

Solving for $b_0^{(h)}$ gives $b_0^{(h)} = 3$. Thus,

$$b_n = 3 \times (-1)^n + 3^n.$$

Q14 Bonus: Can you find a formula for b_n if instead of 4 colours we have k colours?

1.7.8 Bonus: Higher Orders

A *j*th order homogeneous linear recurrence relation with constant coefficients is a recurrence relation of the form

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_j a_{n-j} \tag{22}$$

The process of solving these equations is very similar to the process of solving second order relations, except that now we need to find j linearly independent trial functions.

Equation 5 has auxiliary equation :

$$t^j - C_1 t^{j-1} - C_2 t^{j-2} - \ldots - C_{j-1} t - C_j$$

Theorem 1.62. *If the auxiliary equation has j distinct roots $\alpha_1, \ldots, \alpha_j$ then the general solution to Equation (22) is*

$$a_n = K_1 \times \alpha_1^n + K_2 \times \alpha_2^n + \ldots + K_j \times \alpha_j^n$$

where $K_1, \ldots, K_j$ are constants to be determined from the initial conditions.

Theorem 1.63. *If the auxiliary equation has s distinct roots $\alpha_1, \ldots, \alpha_s$ with multiplicities $m_1, \ldots, m_s$, then the general solution to Equation 6 is:*

$$\begin{aligned} a_n = {} & K_{1,0} \times \alpha_1^n + K_{1,1} \times n \times \alpha_1^n + K_{1,2} \times n^2 \times \alpha_1^n + \ldots + K_{1,m_1-1} \times n^{m_1-1} \times \alpha_2^n \\ & + K_{2,0} \times \alpha_2^n + K_{2,1} \times n \times \alpha_2^n + K_{2,2} \times n^2 \times \alpha_2^n + \ldots + K_{2,m_2-1} \times n^{m_2-1} \times \alpha_2^n \\ & \vdots \\ & + K_{s,0} \times \alpha_s^n + K_{s,1} \times n \times \alpha_s^n + K_{s,2} \times n^2 \times \alpha_s^n + \ldots + K_{s,m_s-1} \times n^{m_s-1} \times \alpha_s^n \end{aligned}$$

where $K_{i,\ell}$ are constants to be determined from the initial conditions.

Example 1.64. Solve the recurrence relation

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

with $a_1 = 3$,$a_2 = 6$ and $a_3 = 14$.

Solution. The auxiliary equation is

$$0 = t^3 - 6t^2 + 11t - 6 = (t-1)(t-2)(t-3)$$

which has roots $\alpha_1 = 1$, $\alpha_2 = 2$ and $\alpha_3 = 3$. Thus, the general solution is

$$a_n = K \cdot 1^n + L \cdot 2^n + M \cdot 3^n == K + L \cdot 2^n + M \cdot 3^n.$$

The initial conditions give

$$\begin{aligned} 3 &= a_1 = K + 2L + 3M \\ 6 &= a_2 = K + 4L + 9M \\ 14 &= a_3 = K + 8L + 27M. \end{aligned}$$

Solving for K, L, M gives $K = 1$, $L = \frac{1}{2}$, and $M = \frac{1}{3}$. Hence, the solution is

$$a_n = 1 + 2^{n-1} + 3^{n-1}.$$

Example 1.65. Solve the recurrence relation

$$a_n = 5a_{n-1} - 8a_{n-2} + 4a_{n-3}$$

with $a_0 = 6$,$a_1 = 7$ and $a_2 = 11$.

Solution. The auxiliary equation is

$$0 = t^3 - 5t^2 + 8t - 4 = (t-1)(t-2)^2$$

which has root $\alpha_1 = 1$ and repeated root $\alpha_2 = 2$. Thus, the general solution is:

$$a_n = K \cdot 1^n + L \cdot 2^n + M \cdot n \cdot 2^n = K + L \cdot 2^n + M \cdot n \cdot 2^n$$

The initial conditions give

$$\begin{aligned} 6 &= a_0 = K + L \\ 7 &= a_1 = K + 2L + 2M \\ 11 &= a_2 = K + 4L + 8M. \end{aligned}$$

Solving for K, L, M gives $K = 7$, $L = -1$, and $M = 1$. Hence,t he solution is

$$a_n = 7 - 2^n + n \cdot 2^n.$$

Chapter 2 Number Theory and Cryptography

So far: We have been counting whole numbers of things, and so we have been using the *natural numbers* as tools.

From now on: We will study the natural numbers themselves.

In this second part of the course, we will be tackling the question:

Q1 What problems can we solve with just the properties of the natural numbers themselves?

This is one of the main questions studied by *number theory*.
We will also study the applications of number theory to:

- Cryptography,
- Error detecting/Correcting codes.

2.1 Congruence to a Modulus

The goal of this section is to revise some modular arithmetic.

2.1.1 Divisibility

Definition 2.1. Given integers m and a we say that m *divides* a and write $m \mid a$ if $\frac{a}{m}$ is an integer. If $\frac{a}{m}$ is not an integer, we write $m \nmid n$.

> **Note:** $m \mid a$ if and only if $a = qm$ for some integer q.

Q2 Can we write a in terms of m if $m \nmid a$?

Lemma 2.2 (Division Algorithm). *Let m be a positive integer and let a be an arbitrary integer. Then, there are unique integers q and r with $0 \leq r < m$ such that $a = qm + r$.*

Proof. Left as an exercise. The idea is that we can always take a large enough q so that $r = a - qm$ is as small as possible. □

> **Note:** In the expression $a = qm + r$, the integer q is called the quotient and the integer r is called the remainder when one divides a by m.

2.1.2 Congruence to a modulus

Our goal now is to build up modular arithmetic.

Definition 2.3. Let m be a positive integer and let a and b be any integers. We say that a and b are congruent modulo m and write

$$a \equiv b \mod m$$

if a and b have the same remainder when divided by m.

If a and b are not congruent modulo m we write

$$a \not\equiv b \mod m$$

Note: For an equivalent definition of congruence:

$$\begin{aligned} a \equiv b \mod m &\iff \\ a = q_1 m + r, \\ b = q_2 m + r &\iff \\ a - b = (q_1 - q_1)m &\iff m \mid (a-b) \end{aligned}$$

In practice, this latter condition is sometimes easier to use.

Example 2.4. Some simple examples:

- $17 \equiv -23 \mod 5$

  since $17 - (-23) = 40$ and $5 \mid 40$.

- $10 \not\equiv 3 \mod 4$

  since $10 - 3 = 7$ and $4 \nmid 7$.

We would like to work with integers up to this notion of congruence, and we would like to check that congruence is "compatible" with addition, subtraction and multiplication.

Theorem 2.5. *Let m be a positive integer, and a_1, a_2, b_1, b_2 be integers. If $a_1 \equiv a_2 \mod m$ and $b_1 \equiv b_2 \mod m$ then*

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \mod m \\ a_1 - b_1 &\equiv a_2 - b_2 \mod m \\ a_1 b_1 &\equiv a_1 b_2 \mod m \end{aligned}$$

Proof. Exercise. □

Another interesting object we can define is the *congruence class of an integer modulo m*.

Definition 2.6. Let m be a positive integer and let a be any integer. Write $a = qm + r$. The set

$$\begin{aligned} [a]_m &= \{\text{integers which are congruent to } b \text{ modulo } m\ \} \\ &= \{\text{integers which have remainder } r \text{ when dividing by } m\} \end{aligned}$$

is called the congruence class or residue class of a modulo m.

Note: If a and b are integers with the same remainder when dividing by m then $[a]_m = [b]_m$! We call the elements a and b representatives of the same congruence class.

Note: Let a be any integer. Then, we can use the division algorithm to write $a = qm + r$. Since $r = 0 \times m + r$, then $[a]_m = [r]_m$ by the observation above. Hence, a and its remainder always represent the same congruence class.

E.g. $5 = \underbrace{1}_{q} \times \underbrace{3}_{m} + \underbrace{2}_{r}$, and so $[5]_3 = [2]_3$.

Note: Write $a = qm + r$. Then, we can list all of the elements in $[a]_m$ in the following way:

$$\ldots,\ (q-2)m+r\,,\ (q-1)m+r\,,\ qm+r\,,\ (q+1)m+r\,,\ (q+2)m+r\ldots$$

Example 2.7. The congruence class of 5 modulo 3 is

$$\begin{aligned}
[5]_3 &= \{\ldots,\ -1\times 3+2\ ,\ 0\times 3+2\ ,\ 1\times 3+2\ ,\ 2\times 3+2\ ,\ 3\times 3+2\ ,\ldots\}\\
&= \{\ldots,-1,2,5,8,11,\ldots\}\\
&= [2]_3\\
&= [8]_3\\
&= [-1]_3\\
&\ \ \vdots
\end{aligned}$$

Example 2.8. We can also ask the question: How many congruence classes modulo 3 are there?

Solution. Consider the congruence classes

$$\begin{aligned}
[0]_3 &= \{\ldots,-6,-3,0,3,6,\ldots\} && (r=0)\\
[1]_3 &= \{\ldots,-5,-2,1,4,7,\ldots\} && (r=1)\\
[2]_3 &= \{\ldots,-4,-1,2,5,8,\ldots\} && (r=2)
\end{aligned}$$

We claim that these are all of the congruence classes.

Let a be any integer. Then, by the division algorithm, $a = 3q + r$. The remainder r when dividing by 3 is bounded by $0 \leq r < 3$, so the only possible values for the remainder are: $0, 1, 2$

Since $[a]_3 = [r]_3$, then $[a]_3$ must be equal to one of: $[0]_3, [1]_3, [2]_3$.

More generally, the remainder when dividing by m is bounded by $0 \leq r < m$, and so the only possible values for r are $0, 1, \ldots, m-1$. Hence, there are m congruence classes modulo m:

$$[0]_m, [1]_m, \ldots, [m-1]_m.$$

We can now define the set

$$\mathbb{Z}/m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

of congruence classes modulo m. We can define addition, subtraction and multiplication on this set due to the following result.

Theorem 2.9. *Let m be a positive integer and let $[a]_m$ and $[b]_m$ be congruence classes in $\mathbb{Z}/m$. Define the operations:*

$$[a]_m + [b]_m = [a+b]_m$$
$$[a]_m - [b]_m = [a-b]_m$$
$$[a]_m \times [b]_m = [ab]_m.$$

Then, these operations are well-defined.

Proof. This essentially follows from Theorem 2.5; Try proving this as an exercise! □

Let's break this theorem down. This theorem has two components.

a) The first part of the theorem gave us a recipe to add the congruence classes $[a]_m$ and $[b]_m$:

- Choose representatives a and b from the congruence classes we are adding.
- Compute the sum $a + b$
- Then, take the congruence class $[a+b]_m$.
- Let r be the remainder of $a + b$ when dividing by m. We may want to re-write $[a+b]_m = [r]_m$.

For example, $[1]_3 + [5]_3 = [6]_3 = [0]_3$.

Similarly, the theorem gives us recipes for subtraction and multiplication.

b) The second part of the theorem states that the operations we defined are *well-defined*. What does well-definedness mean?

When we write down the equation

$$[1]_3 + [5]_3 = [1+5]_3$$

we are *making a choice of representatives* of the congruence classes and *using these representatives to compute the sum*. What happens if we chose different representatives?

We know that

$$[1]_3 = [4]_3$$
$$[5]_3 = [8]_3$$

So, for addition to be well-defined, we must have:

$$[1]_3 + [5]_3 = [4]_3 + [8]_3$$

So we need to make sure the recipe gives us the same result for these two sums.

In other words, we need to make sure that we always get the same result regardless of the choice of representatives we use. We need to check that:

If $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$, then $[a_1]_m + [b_1]_m = [a_2]_m + [b_2]_m$.

This statement proves well-definedness for addition.

Try proving this! Hint: It follows from Theorem 2.5.

Bonus note: Theorem 2.9 tells us that $(\mathbb{Z}/m, +)$ forms a group!

Corollary 2.10. *Let m and k be a positive integers and let $a = qm + r$ be any integer. Then,*

$$[a]_m^k = [r]_m^k = [r^k]_m$$

Example 2.11. Compute $([35]_2)^{300!}$.

Solution. $35 = 2 \times 17 + 1$. Hence

$$([35]_2)^{300!} = [1^{300!}]_2 = [1]_2$$

From here on out, if the context is clear, we may drop the $[-]_m$ notation. So instead of writing

$$[1]_3 + [5]_3 = [0]_3$$

we might write

$$1 + 5 = 0 \mod 3.$$

2.2 Greatest Common Divisor

Definition 2.12. Let a and b be two integers not both zero. Their greatest common divisor , denoted $\gcd(a, b)$, is the largest integer d such that d is a factor of both a and b.

Example 2.13. $\gcd(\underbrace{6}_{2,3}, \overbrace{10}^{2,5}) = 2$.

The greatest common divisor of two numbers can usually be calculated quickly, even for large values, by using the Euclidean algorithm.

Example 2.14. Find the $\gcd(25, 89)$.

Solution. The Euclidean algorithm runs as follows:

$$\begin{aligned}
89 &= 3 \times 25 + 14 \\
25 &= 1 \times 14 + 11 \\
14 &= 1 \times 11 + 3 \\
11 &= 3 \times 3 + 2 \\
3 &= 1 \times 2 + \underbrace{1}_{\substack{\text{last} \\ \text{nonzero} \\ \text{remainder}}} \\
2 &= 2 \times 1 + 0
\end{aligned}$$

Hence, $\gcd(25, 89) = 1$.

Another important result is:

Proposition 2.15 (Bézout's identity)**.** *Let a and b be integers not both zero. Then there are integers r and s such that*

$$ra + sb = \gcd(a, b)$$

Proof. ① Choose integers r, s such that $ra + sb$

- is positive,
- and as small as possible.

We will show that $d = \gcd(a, b)$.

② Let us first show that d divides both a and b. Using the division algorithm, we may write

$$a = qd + t$$

with $0 \leq t < d$. Therefore,

$$t = a - q\underbrace{d}_{ra+sb} = a - q(ra + sb) = \underbrace{(1 - qr)}_{r'} a + \underbrace{(-qs)}_{s'} b.$$

Thus,

$$0 \leq t = r'a + s'b < d = ra + sb.$$

However, by our choice of r and s, there cannot exist integers r' and s' such that $r'a + s'b$ is positive and $r'a + s'b < ra + sb$. Therefore, t cannot be positive $\implies t = 0$.

Hence, $a = qd$ and $d \mid a$. Similarly, $d \mid b$.

③ Let us now show that d is the greatest common divisor of a and b. Suppose that $c \mid a$ and $c \mid b$. Then, there are integers q_1, q_2 with $a = q_1 c$ and $b = q_2 c$. Therefore,

$$d = ra + sb = r(q_1 c) + s(q_2 c) = (rq_1 + sq_2)c$$

Thus, $c \mid d$. Since $d \geq 0$, it must be that $c \leq d$. Hence,

$$d \geq (\text{any common divisor of } a \text{ and } b)$$

and so $d = \gcd(a, b)$. □

Bézout's identity gives us the existence of integers r and s, but in order to actually find them we should use *reverse substitution* in the Euclidean algorithm.

Example 2.16. Find integers r and s such that $25r + 89s = \gcd(25, 89)$.

Solution. Given the Eucliden algorithm in Example 2.14, reverse substitution runs as:

$$
\begin{aligned}
14 &= 1 \times 89 - 3 \times 25 \\
11 &= 1 \times 25 - 14 = 1 \times 25 - (1 \times 89 - 3 \times 25) = -1 \times 89 + 4 \times 25 \\
3 &= 14 - 11 = (1 \times 89 - 3 \times 25) - (-1 \times 89 + 4 \times 25) = 2 \times 89 - 7 \times 25 \\
2 &= 11 - 3 \times 3 = (-1 \times 89 + 4 \times 25) - 3 \times (2 \times 89 - 7 \times 25) = -7 \times 89 + 25 \times 25 \\
1 &= 3 - 2 = (2 \times 89 - 7 \times 25) - (-7 \times 89 + 25 \times 25) = 9 \times 89 - 32 \times 25
\end{aligned}
$$

Thus, we may take $r = -32$ and $s = 9$.

Definition 2.17. Two integers a and b are coprime if $\gcd(a, b) = 1$.

We can use what we have learned so far to solve new problems in modular arithmetic.

Proposition 2.18. *Let m be a positive integer and let a be any integer. Then there is an integer r such that $ra \equiv 1 \mod m$ if and only if a and m are coprime.*

Proof. We're proving an "if and only if" so we need to prove two directions:

a) $ra \equiv 1 \mod m \implies \gcd(a, m) = 1$ (a is coprime to m),

b) $\gcd(a, m) = 1 \implies ra \equiv 1 \mod m$.

(b) Suppose that $\gcd(a, m) = 1$. Then, we can use Bézout's identity to find integers r and s such that

$$
\begin{aligned}
ra + sm = \gcd(a, m) = 1 \implies \\
ra = 1 - sm = (-s)m + 1
\end{aligned}
$$

Thus, the remainder when dividing ra by m is 1 and we conclude that $ra \equiv 1 \mod m$.

(a) Suppose there is an integer r such that $ra \equiv 1 \mod m$. Then, we can use the division algorithm to write:

$$
\begin{aligned}
ra = qm + 1 \implies \\
1 = ra - qm
\end{aligned}
$$

Let d by any common divisor of a and m. Then, we can write $a = c_1 d$ and $m = c_2 d$. Subbing this back into the equation above,

$$1 = r(c_1 d) = q(c_2 d) = (rc_1 + qc_2)d$$

which tells us that $d \mid 1$. But the only number that divides 1 is 1. Hence, $d = 1$.

In other words, we have shown that the only possible common divisor of a and m is 1. So,

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

□

Example 2.19. From example 2.14, we know that 25 and 89 are coprime. So, the theorem above tells us that there is an integer r such that $25r \equiv 1 \mod 89$.

Find a positive integer r such that

$$25r \equiv 1 \mod 89.$$

Solution. From example 2.16, we know that

$$1 = 9 \times 89 - 32 \times 25$$

Hence,

$$25 \times (-32) \equiv 1 \mod 89.$$

Let r be a positive integer with $r \equiv (-32) \mod 89$. Since multiplication is compatible with congruence,

$$25 \times r \equiv 25 \times (-32) \equiv 1 \mod 89.$$

Hence, we need to find positive r with $r \equiv (-32) \mod 89$. This means that we are looking for positive r which can be written as

$$r = 89k + (-32)$$

for any integer k.

Thus, we can just take $k = 1$ to get

$$r = 89 - 32 = 57.$$

Example 2.20. Consider

$$\mathbb{Z}/12 = \{0, 1, \ldots, 11\}.$$

The integers in $\mathbb{Z}/12$ which are coprime to 12 are:

$$x_1 = 1, x_2 = 5, x_3 = 7, x_4 = 11.$$

We can write down a *multiplication table* for the set of integers $\{1, 5, 7, 11\}$ in the following way:

$\overbrace{\times}^{\text{mod } 12}$	1	5	7	11
1	$1 \times 1 \mod 12 = 1$	5	7	11
5	$5 \times 1 \mod 12 = 5$	1	11	7
7	$7 \times 1 \mod 12 = 7$	11	1	5
11	$11 \times 1 \mod 12 = 11$	7	5	1

- $1, 5, 7$ and 11 all appear exactly once in each row and each column.
- Each column is a reordering of the list $1, 5, 7, 11$.
- What this means is if $a \in \{1, 5, 7, 11\}$, then

$$1a \mod 12, 5a \mod 12, 7a \mod 12, 11a \mod 12$$

is reordering of the list: $1, 5, 7, 11$.

For example, if we multiply $1, 5, 7, 11$ by $x_2 = 5$ we get

$$5, 1, 11, 7 \mod 12.$$

Notice that this is the second row of the multiplication table.

Bonus note: This means that the set $\{1, 5, 7, 11\}$ of integers coprime to 12 together with multiplication mod 12 forms a group.

The phenomenon we see in Example 2.20 is true in general.

Theorem 2.21. *Let m be a positive integer and consider*

$$\mathbb{Z}/m = \{0, 1, \ldots, m-1\}.$$

Let

$$x_1, x_2, \ldots, x_k$$

be the integers in $\mathbb{Z}/m$ which are coprime to m.

Then, for $x_i \in \{x_1, \ldots, x_k\}$, the list

$$x_i x_1 \mod m\ ,\ x_i x_2 \mod m \ldots,\ x_i x_k \mod m$$

is just a reordering of $x_1, x_2, \ldots, x_k$.

Note: In example 2.20, we have $m = 12$ and

$$x_1 = 1, x_2 = 5, x_3 = 7, x_4 = 11.$$

If we choose $i = 2$, then we can compute

$$x_2 x_1,\ x_2 x_2,\ x_2 x_3,\ x_2 x_4 \mod 12 = 5, 1, 11, 7$$

Notice that this is just the second row in the multiplication table in Example 2.20 (it's also the second column in the multiplication table).

In fact for every i.

$$x_i x_1,\ x_i x_2, \ldots,\ x_i x_k \mod m$$

is the ith row in the multiplication table.

Proof of Theorem 2.21. Let $x_i \in \{x_1, \ldots, x_k\}$. We just need to show that each integer in the list

$$x_i x_1,\ x_i x_2, \ldots,\ x_i x_k \mod m$$

appears exactly once in the list $x_1, x_2, \ldots, x_k$. This can be proved by showing:

1) Each integer

$$x_i x_1 \ , \ x_i x_2 \ \ldots, \ x_i x_k \mod m$$

appears in the list $x_1, x_2, \ldots, x_n$. I.e. each integer

$$x_i x_1 \ , \ x_i x_2 \ \ldots, \ x_i x_k \mod m$$

is coprime to m.

2) Each integer in the list

$$x_i x_1 \ , \ x_i x_2 \ \ldots, \ x_i x_k \mod m$$

appears only once in the list $x_1, x_2, \ldots, x_n$. I.e. the integers

$$x_i x_1 \ , \ x_i x_2 \ \ldots, \ x_i x_k \mod m$$

are distinct.

1) We first show that $x_i x_1 \mod m$ is coprime to m.

Since x_i and x_1 are coprime to m, Proposition 2.18 tells us that there is are integers r, s such that

$$\begin{aligned} sx_i &= 1 \mod m, \\ rx_1 &= 1 \mod m. \end{aligned} \tag{23}$$

Multiplying the equations above together gives

$$(rx_i) \cdot (sx_1) = 1 \mod m.$$

Hence,

$$\underbrace{(rs)}_{r'} \cdot (x_i x_1) = 1 \mod m.$$

Thus we have found an iteger r' such that

$$r'(x_i x_1) = 1 \mod m.$$

Proposition 2.18 tells us that $x_i x_1$ is coprime to m.

Since $x_1, x_2, \ldots, x_k$ are all of the integers coprime to m, then $x_i x_1$ is in the the list $x_1, x_2, \ldots, x_k$.

For the same reasons, each integer $x_i x_2 \ , \ x_i x_3 \ , \ \ldots \ , \ x_i x_k$ is in the list $x_1, x_2, \ldots, x_k$.

2) We now just need to show now that $x_i x_1 \ , \ \ldots \ x_i x_k$ are distinct integers. We will use the fact that in Equation (23) we found an integer s such that $sx_i = 1 \mod m$.

Let j, n be integers with $1 \leq j, n \leq k$ and suppose that

$$x_i x_j = x_i x_n \mod m.$$

Then, we can multiply both sides of this equation by s to get

$$\begin{aligned} &\underbrace{(sx_i)}_{1} x_j = \underbrace{(sx_i)}_{1} x_n \mod m \implies \\ &x_j = x_k \qquad\qquad\qquad \implies \\ &j = k. \end{aligned}$$

□

2.3 Binary Notation

Our goal is to introduce binary notation and use this to prove results in arithmetic modulo m.

Q3 Compute

$$a = 4 \times 25 \times 9 \times 13 \mod 89,$$
$$b = 13^{43} \mod 89.$$

Solution. We can use a calculator to compute $4 \times 25 \times 9 \times 13 = 11700$ and then find the remainder when dividing 11700 by 89 by taking

$$r = 11700 - \lfloor \frac{11700}{89} \rfloor \times 89 = 41$$

Hence, $a = 41 \mod 89$.

We can similarly, compute b by computing on the calculator

$$r = 13^{43} - \lfloor \frac{13^{43}}{89} \rfloor \times 89$$

This, however, is not very efficient because 13^{43} is a very large number. Is there a more efficient way? Yes – using the *binary expansion* of a number.

Let n be a positive integer. Usually, we write n in decimal notation: we represent n as a string of digits

$$a_m a_{m-1} \dots a_0$$

with $a_i \in \{0, 1, ..., 9\}$. For example,

$$\underbrace{5}_{b_3}\ \underbrace{0}_{b_2}\ \underbrace{7}_{b_1}\ \underbrace{3}_{b_0}.$$

The decimal notation for n means that

$$n = 10^m a_m + 10^{m-1} a_{m-1} + \ldots + 10^1 a_1 + 10^0 a_0.$$

For example,

$$5073 = (10^3 \times 5) + (10^2 \times 0) + (10^1 \times 7) + (10^0 \times 3)$$

Instead of using base 10, we can use base 2. This is binary notation.

In binary notation, we represent an integer n as a string $b_m b_{m-1} \dots b_0$ with $b_i \in \{0, 1\}$. This means that

$$n = 2^{m-1} b_{m-1} + 2^{m-2} b_{m-2} + \ldots + 2^1 b_1 + 2^0 b_0.$$

Now, since the only possible values for b_i are 0 and 1, we can rewrite n as

$$n = 2^{j_1} + 2^{j_2} + \ldots + 2^{j_k}$$

with $j_1, \dots, j_k$ distinct integers.

Example 2.22. What decimal number does the binary number 1001 0110 represent?

Solution. Notice that we begin reading from the right so $b_0 = 0$, $b_1 = 1$ and so on. Hence,

$$n = \underbrace{1}_{b_7}\ \underbrace{0}_{b_6}\ \underbrace{0}_{b_5}\ \underbrace{1}_{b_4}\ \underbrace{0}_{b_3}\ \underbrace{1}_{b_2}\ \underbrace{1}_{b_1}\ \underbrace{0}_{b_0}.$$

In decimal notation we have:

$$\begin{aligned} n &= 2^7 \cdot 1 + 2^6 \cdot 0 + 2^5 \cdot 0 + 2^4 \cdot 1 + 2^3 \cdot 0 + 2^2 \cdot 1 + 2^1 \cdot 1 + 2^0 \cdot 0 \\ &= 2^7 + 2^4 + 2^2 + 2^1 \\ &= 150. \end{aligned}$$

Example 2.23. Write 43 in binary notation.

Solution. We first need to find the binary expansion of 43, i.e. write 43 as a sum of powers of two. There are two methods to do this.

Method 1

- The largest power of 2 less than or equal to 43 is $2^5 = 32$. So we can write $43 = 2^5 + 11$.
- The largest power of 2 less than or equal to 11 is $2^3 = 8$ so we can write $43 = 2^5 + 2^3 + 3$.
- The largest power of 2 less than or equal to 3 is 2^1, so $43 = 2^5 + 2^3 + 2^1 + 2^0$.

Converting to binary notation means that we have (remember that we start from the right)

$$\begin{aligned} b_0 &= 1 \\ b_1 &= 1 \\ b_2 &= 0 \qquad \text{(since } 2^2 \text{ does not appear in the binary expansion)} \\ b_3 &= 1 \\ b_4 &= 0 \qquad \text{(since } 2^4 \text{ does not appear in the binary expansion)} \\ b_0 &= 1. \end{aligned}$$

Thus 43 in binary notation is

$$101011$$

Method 2
We can use the formula

$$2^r b_r = n - \sum_{i=0}^{r-1} 2^i b_i \mod 2^{r+1}$$

to find the binary expansion of 43 in the following way:

$$
\begin{aligned}
2^0 b_0 &= 43 \mod 2 = 1 \mod 2 \implies b_0 = 1 \\
2^1 b_1 &= \underbrace{42}_{(43-1)} \mod 4 = 2 \mod 4 \implies b_1 = 1 \\
2^2 b_2 &= \underbrace{40}_{(42-2)} \mod 8 = 0 \mod 8 \implies b_2 = 0 \\
2^3 b_3 &= \underbrace{40}_{(40-0)} \mod 16 = 8 \mod 16 \implies b_3 = 1 \\
2^4 b_4 &= \underbrace{32}_{(40-8)} \mod 32 = 0 \mod 32 \implies b_4 = 0 \\
2^5 b_5 &= \underbrace{32}_{(32-0)} \mod 64 = 32 \mod 64 \implies b_5 = 1 \\
2^6 b_6 &= \underbrace{0}_{32-32} \mod 128.
\end{aligned}
$$

The process concludes since we hit zero; i.e.

$$43 = 2^0 + 2 + 2^3 + 2^5.$$

Why does the second process work?

A positive integer n has binary expansion

$$n = 2^0 b_0 + \underbrace{2^1 b_1 + 2^2 b_2 + 2^3 b_2 + 2^4 b_4 + \ldots}_{\text{all of these terms are multiples of 2}}$$

Finding b_0:
Notice that

$$2^1 b_1 + 2^2 b_2 + 2^3 b_2 + 2^4 b_4 + \ldots = 0 \mod 2$$

since all of the terms are multiples of 2.

Thus,

$$n = 2^0 b_0 \mod 2.$$

Finding b_1:
In the binary expansion of n,

$$n = 2^0 b_0 + 2^1 b_1 + \underbrace{2^2 b_2 + 2^3 b_2 + 2^4 b_4 + \ldots}_{\text{all of these terms are multiples of 4}}$$

Hence

$$2^2 b_2 + 2^3 b_2 + 2^4 b_4 + \ldots = 0 \mod 4.$$

Thus,

$$\begin{aligned} n &= 2^0 b_0 + 2^1 b_1 \mod 4 \implies \\ 2^1 b_1 &= n - 2^0 b_0 \mod 4. \end{aligned}$$

Finding b_2:
In the binary expansion of n,

$$n = 2^0 b_0 + 2^1 b_1 + 2^2 b_2 + \underbrace{2^3 b_2 + 2^4 b_4 + \ldots}_{\text{all of these terms are multiples of 8}}$$

Hence

$$2^3 b_2 + 2^4 b_4 + \ldots = 0 \mod 8.$$

Thus,

$$\begin{aligned} n &= 2^0 b_0 + 2^1 b_1 + 2^2 b_2 \mod 8 \implies \\ 2^2 b_2 &= n - 2^0 b_0 - 2^1 b_1 \mod 8 \end{aligned}$$

We can keep on going to find $b_3, \ldots$ until we find a k where

$$\begin{aligned} n - 2^0 b_0 - 2^1 b_1 - \ldots - 2^k b_k = 0 &\implies \\ n = 2^0 b_0 + 2^1 b_1 + \ldots + 2^k b_k. & \end{aligned}$$

More formally (Non-examinable):
We can write the binary expansion of n as:

$$n = \sum_{i=0}^{k} 2^i b_i = \sum_{i=0}^{r-1} 2^i b_i + 2^r b_r + \underbrace{\sum_{i=r+1}^{k} 2^i b_i}_{\text{All terms are multiples of } 2^{r+1} \implies = 0 \mod 2^{r+1}}$$

Hence,

$$2^r b_r = n - \sum_{i=0}^{r-1} 2^i b_i \mod 2^{r+1}.$$

We are now ready to learn how to compute $b^k \mod m$; we will use the method of *repeated squaring*.

Example 2.24. Compute $13^{43} \mod 89$; that is, find the remainder when 13^{43} is divided by 89.

Solution.

Step 1 Write 43 as a sum of powers of 2. From Example 12.2, we know that

$$43 = 2^5 + 2^3 + 2^1 + 1$$

Thus,

$$\begin{aligned} 13^{43} &= (13^{2^5}) \times (13^{2^3}) \times (13^2) \times (13^1) \\ &= (13^{32}) \times (13^8) \times (13^2) \times (13^1) \qquad \text{(Equation 2)} \end{aligned}$$

Step 2 Compute successive powers of 13 modulo 89:

$$\begin{aligned} 13^1 &= 13 \mod 89 \\ 13^2 &= 169 \mod 89 = -9 \mod 89 \\ 13^4 &= (13^2)^2 = (-9)^2 \mod 89 = 81 \mod 89 = -8 \mod 89 \\ 13^8 &= (13^4)^2 = (-8)^2 \mod 89 = 64 \mod 89 = -25 \mod 89 \\ 13^{16} &= (13^8)^2 = (-25)^2 \mod 89 = 625 \mod 89 = 2 \mod 89 \\ 13^{32} &= (13^{16})^2 = 2^2 \mod 89 = 4 \mod 89 \end{aligned}$$

Step 3 Substitute these values back into Equation 2.

$$13^{43} = (4) \times (-25) \times (-9) \times (13) = 11700 = 41 \mod 89.$$

2.4 Prime Numbers

Yhe goal of this section is to use prime numbers to prove some especially nice properties of congruence modulo m.

Definition 2.25. A prime number is an integer $p > 1$ with no positive factors other than 1 and p.

Prime numbers can be thought of as the building blocks of the integers. This intuition is formalised by the *prime factorisation theorem*.

Theorem 2.26 (Prime Factorisation)**.** *Let $n > 1$ be an integer. Then, there are prime numbers $p_1 < p_2 < \ldots < p_k$ and positive integers $a_1, a_2, \ldots a_k$ such that*

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

Example 2.27.

$$180 = 2^2 \cdot 3^2 \cdot 5$$

Arithmetic modulo p has an especially nice property.

Proposition 2.28. *Let p be prime number and let a be an integer not divisible by p. Then, there is an integer r such that $ra \equiv 1 \mod p$.*

Proof. By Proposition 2.18, if a and p are coprime, then there is an r such that $ra \equiv 1 \mod p$. Hence, it is enough to show that a and p are coprime, i.e. $\gcd(a, p) = 1$.

Since p is prime, its only divisors are 1 and p. Since by assumption a is not divisible by p, the only common divisor between a and p is 1. Thus, $\gcd(a, p) = 1$. □

Finally, we will use prime factorisation to get a result which will be a useful tool to us.

Theorem 2.29. *Let $m > 1$ be an integer with prime factorisation*

$$m = p_1^{a_1} \times \ldots \times p_k^{a_k}.$$

Let a, b be any integers. Then,

$$a \equiv b \mod m$$

if and only if

$$a \equiv b \mod p_i$$

for all $p_1, \ldots, p_k$.

Proof. ($\Longrightarrow$) Suppose that $a \equiv b \mod m$. Recall that this is equivalent to: $m \mid (a-b)$.

Since $m = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, this means that $p_i^{a_i} \mid (a-b)$ for all $p_1, \ldots, p_k$. Thus,

$$a \equiv b \mod p_i^{a_i}.$$

($\Longleftarrow$) Suppose that

$$a \equiv b \mod p_i^{a_i}$$

for all $p_1, \ldots, p_k$. Then, $p_i^{a_i} \mid (a-b)$. Hence, there are integers q_i with

$$\begin{aligned} a - b &= q_1 p_1^{a_1} \\ a - b &= q_2 p_2^{a_2} \\ &\vdots \\ a - b &= q_k p_k^{a_k}. \end{aligned}$$

① We first claim that $(a-b) = q_2' \cdot p_2^{a_2} \cdot p_1^{a_1}$. We will prove this by showing that $p_2^{a_2} \mid q_1$.

Since

$$q_1 \cdot p_1^{a_1} = a - b = q_2 \cdot p_2^{a_2},$$

then $p_2^{a_2} \mid q_1 \cdot p_1^{a_1}$. But p_1 and p_2 are distinct primes, so

$$\begin{aligned} p_2 \nmid p_1 &\implies \\ p_2^{a_2} \nmid p_1^{a_1} &\implies \\ p_2^{a_2} \mid q_1. & \end{aligned}$$

Therefore, there is an integer q_2' such that

$$\begin{aligned} q_1 = q_2' \cdot p_2^{a_2} &\implies \\ a - b = q_1 \cdot p_1^{a_1} = q_2' \cdot p_2^{a_2} \cdot p_1^{a_1} & \end{aligned}$$

② We repeat this process for p_3.

Since

$$q_2' \cdot p_2^{a_2} \cdot p_1^{a_1} = a - b = q_3 \cdot p_3^{a_3}$$

it similarly follows that $p_3^{a_3} \mid q_2'$. Therefore, there is an integer q_3' with

$$\begin{aligned} &q_2' = q_3' \cdot p_3^{a_3} \implies \\ &a - b = q_2' \cdot p_2^{a_2} \cdot p_1^{a_1} = q_3' \cdot p_3^{a_3} \cdot p_2^{a_2} \cdot p_1^{a_1} \end{aligned}$$

③ Repeating the process for $p_4, \ldots, p_k$ we get that

$$\begin{aligned} a - b &= q_k' \cdot \underbrace{p_k^{a_k} \cdot \ldots \cdot p_2^{a_2} \cdot p_1^{a_1}}_{m} \\ &= q_k' \cdot m, \end{aligned}$$

and so $m \mid (a - b)$. This is equivalent to $a \equiv b \mod m$. □

Example 2.30. Show that $900 \equiv 0 \mod 36$.

Solution. The prime factorisation of 36 is $36 = 2^2 \cdot 3^2$.

By Theorem 13.1, $900 \equiv 0 \mod 36$ if and only if

$$\begin{cases} 900 \equiv 0 \mod 2^2 & (\text{Equation 1}) \\ 900 \equiv 0 \mod 3^2 & (\text{Equation 2}) \end{cases}$$

Notice that 900 is divisible by 4 so Equation 1 holds. Moreover, 900 is divisible by 9, so Equation 2 also holds. Hence, $900 \equiv 0 \mod 36$.

Definition 2.31. An integer $n > 1$ which is not prime is called composite .

[I.e. $n > 1$ is composite if and only if there is an integer d such that $d \mid n$ and $1 < d < n$.]

Note: Let n be an integer, then (using prime factorisation) we can write

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r \quad (\text{we allow repeated primes; e.g. } p_1 = p_2.)$$

with $p_1 \leq p_2 \leq \ldots \leq p_r$. (E.g. $9 = 3 \cdot 3$). If n is a composite, then $r \geq 2$.

We can use the property above to prove that:

Lemma 2.32. *If n is composite number, then it has a prime factor p such that $p \leq \sqrt{n}$.*

Proof. Since n is composite,

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

where $r \geq 2$ and $p_1 \leq p_2$. Therefore,

$$p_1^2 \leq p_1 p_2 \leq p_1 \cdot p_2 \cdot \ldots \cdot p_r = n$$

Hence,

$$p_1 \leq \sqrt{n}.$$

□

Lemma 2.32 gives us a way to check whether a number is prime or not.

Example 2.33. Show that 89 is prime.

Solution. Notice that $89 < 11^2$. If 89 were composite, then it would have a prime factor p with

$$p \leq \sqrt{89} < 11.$$

Hence, to check that 89 is prime, we just need to check that for all primes $p < 11$, then $p \nmid 89$. All of the primes < 11 are: $2, 3, 5, 7$. Since 89 is not divisible by any of these, then it is prime.

Example 2.34. Find all prime numbers between 210 and 225.

Proof. A composite integer $n \leq 225$ must have a prime factor p with $p \leq \sqrt{n} \leq \sqrt{225} = 15$. So n is prime if and only if it is not divisible by all of the primes < 15: $2, 3, 5, 7, 11, 13$. We can now construct a table

n	$n \mid 2?$	$n \mid 3?$	$n \mid 5?$	$n \mid 7?$	$n \mid 11?$	$n \mid 13?$
210	2					
211	x	x	x	x	x	x
212	2					
213	x	3				
214	2					
215	x	x	5			
216	2					
217	x	x	x	7		
218	2					
219	x	3				
220	2					
221	x	x	x	x	x	13
222	2					
223	x	x	x	x	x	x
224	2					
225	x	3				

Hence, the prime numbers are 211 and 223. □

Finally there is one more tool we will need for spotting primes. Let $n > 0$ be an integer. Then,

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}), \qquad (\text{Equation 3})$$
$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots + b^{n-1}). \qquad (\text{If } n \text{ is odd})$$

Example 2.35. Let a, n be integers with $a \geq 2$ and $n \geq 1$. If n is composite, then $a^n - 1$ is composite.

Solution. Since n is composite, there is an integer $1 < d < n$ such that $d \mid n \implies n = qd$. Thus, using the Equation 3,

$$a^n - 1 = (a^d)^q - 1^q = (a^d - 1)\left((a^d)^{q-1} + (a^d)^{q-2} + \ldots + 1\right)$$

Hence, $(a^d - 1) \mid (a^n - 1)$. Moreover, since $1 < d < n$,

$$1 \leq a^1 - 1 < a^d - 1 < a^n - 1$$

Thus, $a^n - 1$ is composite.

2.5 Error detecting and error correcting codes

Q4 We would like to transmit a message consisting of a string of characters, but there is a chance that a character may be transmitted incorrectly.

a) Is there a way to encode the message so that errors of transmission can be detected? → Error-detecting code

b) Is there a way to encode a message so that the correct value can be inferred, even if errors may have been made? → Error-correcting code

We will assume throughout this section that at most one error will be made.

Example 2.36. a) A simple error detecting code is transmitting each character twice.

If one character is transmitted incorrectly, then the message will have one character which is not repeated.

E.g. Transmitting the word "share":

$$SS \quad \underbrace{CH}_{\text{Error. Correct character may be C or H.}} \quad AA \quad RR \quad EE$$

b) A simple error correcting code is transmitting each character three times.

If one character is transmitted incorrectly, then the message will have have one character which is not repeated three times, but it is still repeated twice so one can deduce the error.

E.g. Transmitting the word "share":

$$SSS \quad \underbrace{CHH}_{\text{Error. Correct character is H}} \quad AAA \quad RRR \quad EEE$$

These codes are extravagant, in the sense that the coded message is much longer than the original. One can use number theory to create more economical codes.

2.5.1 EAN-13 code

Error-detecting code used for bar codes in shops.

Transmitting the message.

The messages we will transmit are 12-character strings

$$a_1 a_2 \dots a_{12}$$

where each $a_i \in \{0, \dots 9\}$.

This message will be encoded as

$$\underbrace{a_1 a_2 \dots a_{12}}_{\text{Original message}} \quad \overbrace{a_{13}}^{\text{Redundant character}}$$

where

$$a_{13} = -(a_1 + 3a_2 + a_3 + 3a_4 + \dots + 3a_{12}) \mod 10.$$

For example, if we want to transmit the message:

$$3086\ 1230\ 0107$$

We need to find:

$$\begin{aligned} a_{13} &= -(3 + 3\cdot 0 + 8 + 3\cdot 6 + 1 + 3\cdot 2 + 3 + 3\cdot 0 + 0 + 3\cdot 1 + 0 + 3\cdot 7) \mod 10 \\ &= -3 \mod 10 \\ &= 7 \mod 10. \end{aligned}$$

Thus, the code that is transmitted is:

$$3086\ 1230\ 0107\ 7.$$

Error-detection.

Suppose we received the message

$$a_1 a_2 \dots a_{12} a_{13}.$$

This string has a checksum

$$s = a_1 + 3a_2 + a_3 + 3a_4 + \dots + 3a_{12} + a_{13}.$$

If the code was **transmitted correctly**, then because

$$a_{13} = -(a_1 + 3a_2 + \dots + 3a_{12}) \mod 10$$

we must have that $s = 0 \mod 10$.

If the code was **transmitted with a single error**: suppose a_k is replaced by c_k. Then, the checksum would be:

$$s = \begin{cases} a_1 + 3a_2 + \dots + c_k + \dots + 3a_{12} + a_{13} & \text{If } k \text{ is odd} \\ a_1 + 3a_2 + \dots + 3c_k + \dots + 3a_{12} + a_{13} & \text{If } k \text{ is even} \end{cases}$$

Subbing in the expression for a_{13} we have that

$$s = \begin{cases} c_k - a_k & \text{If } k \text{ is odd,} \\ 3(c_k - a_k) & \text{If } k \text{ is even.} \end{cases}$$

Since $-10 < b_i - a_i < 10$ and $\gcd(3, 10) = 1$, then s is not a multiple of 10 i.e. $s \neq 0 \mod 10$.

Thus, to check for errors we just need to compute the checksum:

$$\begin{cases} s = 0 \mod 10 & \text{Code is correct,} \\ s \neq 0 \mod 10 & \text{There is an error.} \end{cases}$$

Notice that we only know that there is an error, and we do not know where it is or how to correct it.

Note: The 3's are present in the expressions for a_{13} and s to check transposition errors: e.g. if a message $a_1a_2a_3\ldots$ gets transmitted as $a_2a_1a_3\ldots$.

2.5.2 Hamming Codes

Hamming codes are error correcting codes used when transmitting strings of $\underbrace{\text{binary digits}}_{\text{bits}}$.

For $m \geq 2$ then:

$$\begin{array}{c}\text{String of} \\ 2^m - m - 1 \text{ bits}\end{array} \xrightarrow{\text{represented/encoded as}} \text{String of } 2^m - 1 \text{ bits}$$

Note:

$$\lim_{m\to\infty} \frac{2^m - 1}{2^m - m - 1} = 1$$

and so at the limit of very large m, then the coded message is not much longer than the original. Hence, this is a very economical code.

2.5.3 [7, 4] Hamming Code

In the Hamming codes when $m = 3$ then:

$$\begin{array}{c}\text{String of} \\ 2^3 - 3 - 1 = 4 \\ \text{bits.}\end{array} \xrightarrow{\text{represented/encoded as}} \begin{array}{c}\text{String of} \\ 2^3 - 1 = 7 \\ \text{bits.}\end{array}$$

The $m = 3$ case is often called the $[4, 7]$ Hamming Code.

Encoding the message:

Let's write our original 4-bit message as:

$$b_3, b_5, b_6, b_7$$

with $b_i \in \{0, 1\}$ (We label the bits by all of the numbers $1, \ldots, 7$ which are not powers of 2).

Then we will encode this message as a 7-bit string:

$$b_1b_2 \quad \underbrace{b_3}_{\text{In our original message}} \quad b_4 \quad \underbrace{b_5b_5b_7}_{\text{In our original message}} .$$

and so we need to define b_1, b_2 and b_4. We do this as follows.

- Take the subscripts $1, \dots 7$ which are not powers of 2: $3, 5, 6, 7$ and write them in binary notation

$$3 = 011,$$
$$5 = 101,$$
$$6 = 110,$$
$$7 = 111.$$

- Consider the sets:

$A_0 = \{\text{subscripts above which (written in binary) have a 1 in position 0}\} = \{3, 5, 7\}$
$A_1 = \{\text{subscripts above which (written in binary) have a 1 in position 1}\} = \{3, 6, 7\}$
$A_2 = \{\text{subscripts above which (written in binary) have a 1 in position 2}\} = \{5, 6, 7\}$

Note: Binary numbers are read from right to left so, e.g. $3 = 011$ has a 1 in position 0 and a 0 in position 2.

- Define b_1, b_2, b_4 as:

$$b_1 = -(b_3 + b_5 + b_7) \mod 2 \quad \text{Sum of all } b_i \text{ for which } i \in A_0,$$

$$b_2 = -(b_3 + b_6 + b_7) \mod 2 \quad \text{Sum of all } b_i \text{ for which } i \in A_1,$$

$$b_4 = -(b_5 + b_6 + b_7) \mod 2 \quad \text{Sum of all } b_i \text{ for which } i \in A_2.$$

Example 2.37. Encode the message 1101.

Solution. We have $b_3 = 1, b_5 = 1, b_6 = 0, b_7 = 1$. Then, the coded message is

$$b_1 b_2\ 1\ b_4\ 101,$$

where

$$b_1 = -(b_3 + b_5 + b_7) = -(1 + 1 + 1) = 1 \mod 2$$
$$b_2 = -(b_3 + b_6 + b_7) = -(1 + 0 + 1) = 0 \mod 2$$
$$b_4 = -(b_5 + b_6 + b_7) = -(1 + 0 + 1) \mod 2 = 0 \mod 2.$$

Hence, the code to be transmitted is: 10 1 0 101.

Correcting Errors.

Suppose we received a message $b_1 b_2 \dots b_7$. To correct errors, we will again use checksums .

Consider the checksums:

$$s_0 = b_1 + (b_3 + b_5 + b_7) \mod 2$$

$$s_1 = b_2 + (b_3 + b_6 + b_7) \mod 2$$

$$s_2 = b_4 + (b_5 + b_6 + b_7) \mod 2$$

Note: s_0 is the sum of b_1, b_3, b_5, b_7. These are all of the b_i that have an index i which (written in binary) have a 1 in position zero.

Similarly, s_1 is the sum of all b_i that have an index i which (written in binary) have a 1 in position one.

Similarly for s_2.

If the code was **transmitted correctly**, then since

$$b_1 = -(b_3 + b_5 + b_7) \mod 2,$$

it must be that

$$s_0 = b_1 - b_1 = 0.$$

Similarly, $s_1 = 0 \mod 2$ and $s_2 = 0 \mod 2$.

Suppose that there was a **single error in the code**: b_k was incorrectly transmitted as c_k.

- If k (written in binary) does not have 1 in position zero, then $k \neq 1, 3, 5, 7$. Hence, b_1, b_3, b_5 and b_7 are all transmitted correctly. Since
$$s_0 = b_1 + b_2 + b_3 + b_7$$
then s_0 is unaffected by the error. I.e. $s_0 = 0 \mod 2$.

- If k (written in binary) has a 1 in position 0, then $k \in \{1, 3, 5, 7\}$ and so one of b_1, b_3, b_5 or b_7 are incorrect.

  Notice that
  $$s_0 = b_1 + b_3 + b_5 + b_7 - b_k + c_k \mod 2$$
  (e.g. if $k = 1$ then $s_0 = c_1 + b_3 + b_5 + b_7$.
  Since $b_1 + (b_3 + b_5 + b_7) = 0 \mod 2$, then
  $$s_0 = c_k - b_k \mod 2.$$
  Now, b_k is either 0 or 1 and $c_k \neq b_k$. In either case, $c_k - b_k = 1 \mod 2 \neq 0$.

- In summary, we have shown that if there are no errors then $s_0 = s_1 = s_2 = 0 \mod 2$.

  If there is one error where b_k is transmitted incorrectly as c_k, then
  $$s_0 = \begin{cases} 1 \mod 2 & \text{if } k \text{ (written in binary) has a 1 in position 0)} \\ 0 \mod 2 & \text{otherwise.} \end{cases}$$

- Similarly,
  $$s_1 = \begin{cases} 1 \mod 2 & \text{if } k \text{ (written in binary) has a 1 in position 1)} \\ 0 \mod 2 & \text{otherwise.} \end{cases}$$
  $$s_2 = \begin{cases} 1 \mod 2 & \text{if } k \text{ (written in binary) has a 1 in position 2)} \\ 0 \mod 2 & \text{otherwise.} \end{cases}$$

Thus, we can check if there is an error, and find which character b_k was transmitted incorrectly by computing the checksums; since there are only two options for digits in binary, we know how to correct the error.

Example 2.38. Suppose we receive a code 10 1 0 001. Check if there is an error and correct it if necessary.

Solution. We have:

$$\begin{aligned} b_1 &= 1 \\ b_2 &= 0 \\ b_3 &= 1 \\ b_4 &= 0 \\ b_5 &= 0 \\ b_6 &= 0 \\ b_7 &= 1. \end{aligned}$$

Let's compute the checksums:

$$\begin{aligned} s_0 &= b_1 + b_3 + b_5 + b_7 = 1+1+0+1 = 1 \mod 2 \\ s_1 &= b_2 + b_3 + b_6 + b_7 = 0+1+0+1 = 0 \mod 2 \\ s_2 &= b_4 + b_5 + b_6 + b_7 = 0+0+0+1 = 1 \mod 2 \end{aligned}$$

Since the checksums are not all $0 \mod 2$, then there is an error in some position k.

Since $s_0 = s_2 = 1 \mod 2 \neq 0 \mod 2$, k (written in binary) has a 1 in positions 0 and 2. Moreover, since $s_2 = 0 \mod 2$, k has a 0 in position 1.

Thus, $k = 101 = 5$. This tells us that b_5 was transmitted incorrectly. Since we received that $b_5 = 0$, the correct value should be $b_5 = 1$. Thus, the correct code is 10 1 0 101.

Note: The $m = 4$ case is be covered in your tutorial sheets!

2.6 Fermat's Theorem

The previous section discussed error detecting/correcting codes which answered the question: Can we encode a message so that someone who receives the message can detect/correct any errors of transmission?

These codes are not secret codes. If a message is intercepted, then it can be decoded very easily.

Our next goal is to learn about a code which does provide a level of secrecy: the RSA code. This code is based on Fermat's theorem .

Note: Let n be an integer. Then, what is $\gcd(0, n)$? Well, $n \mid n$ and $n \mid 0$ since $\frac{0}{n}$ is an integer. Hence, $\gcd(0, n) = n$. Therefore, as long as $n > 1$, then 0 is not coprime to n.

Theorem 2.39. *Let p be a prime number.*

a) If a is any integer not divisible by p then

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

b) If b is any integer then

$$b^p \equiv b \mod p.$$

Proof. a) Consider the following observations.

① Consider the set $\mathbb{Z}/p = \{0, 1, \ldots, p-1\}$. Since p is prime, the integers in the set $\mathbb{Z}/p$ coprime to p are all of the nonzero integers:

$$x_1 = 1,\ x_2 = 2\ ,\ \ldots\ ,\ x_{p-1} = p-1.$$

② Let a be any integer not divisible by p. Then, we can write

$$a = kp + r$$

where $1 \leq r \leq\leq p-1$. Hence, $r \in \mathbb{Z}/p$ and is nonzero. Therefore, r is coprime to p. Moreover, $a = r \mod p$.

Now consider the list

$$rx_1\ ,\ rx_2\ ,\ \ldots\ ,\ rx_{p-1} = 1r\ ,\ 2r\ \ldots\ ,\ (p-1)r \mod p.$$

Since r is coprime to p, Theorem 2.21 tells us that this list is just a reordering of the list

$$x_1\ ,\ x_2\ ,\ \ldots\ ,\ x_{p-1} = 1\ ,\ 2\ ,\ \ldots\ ,\ (p-1) \mod p.$$

Hence,

$$1r \cdot 2r \cdot \ldots \cdot (p-2)r \cdot (p-1)r = 1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) \mod p$$

Simplifying, we get

$$r^{p-1} \cdot (p-1)! = (p-1)! \mod p. \tag{24}$$

Since $(p-1)!$ is coprime to p, then by Proposition 2.18 there is an s such that $(p-1)! \cdot s = 1 \mod p$. Multiplying both sides of Equation (24) by s gives:

$$\begin{aligned} &r^{p-1}(p-1)! \cdot s = (p-1)! \cdot s \mod p \implies \\ &r^{p-1} = 1 \mod p \implies \\ &a^{p-1} = 1 \mod p. \qquad \text{(Since } a = r \mod p\text{)} \end{aligned}$$

b) Now let b be any integer.

If $p \mid b$, then $b = 0 \mod p$ and so

$$b^p = 0^p = 0 = b \mod p.$$

If, on the other hand, $p \nmid b$, then we can apply part (a)

$$b^p = b \cdot b^{b-1} = b \cdot 1 = b \mod p$$
$$\text{(since } b^{p-1} = 1 \mod p \text{ by (a).)}$$

□

Example 2.40. Consider the case $p = 5$. Then, part (a) of Fermat's theorem tells us that $2^{5-1} = 1 \mod 5$ and part (b) says that $2^5 = 2 \mod 5$.

Fermat's theorem gives us another (not entirely reliable) tool for check whether a number is prime.

Example 2.41. Show that $2^9 = 1 \mod 511$. Use Fermat's theorem to show that 511 is not prime.

Solution.

$$2^9 = 512 = 1 \mod 511.$$

By part b) of Fermat's theorem, if 511 were prime, we should have that

$$2^{511} = 2 \mod 511.$$

To compute 2^{511}, note that

$$511 = 9 \cdot 56 + 7$$

and so

$$2^{511} = (2^9)^{56} \cdot 2^7 = 2^7 = 128 \neq 2 \mod 511.$$

Therefore, 511 cannot be prime by Fermat's theorem.

Note: Let n be an integer. Fermat's theorem tells us that if

$$(\ n \text{ is prime }) \implies (\ a^n = a \mod n \text{ for all } a \in \mathbb{Z}\ ).$$

The converse

$$(\ n \text{ is prime }) \impliedby (\ a^n = a \mod n \text{ for all } a \in \mathbb{Z}\ )$$

is not true! So, in general, we are not able to use Fermat's theorem to show that a number is prime. We are only able to use Fermat's theorem to show that a number is not prime.

Example 2.42. Show that 561 is not prime but that $a^{561} = a \mod 561$ for any integer a.

Solution. The integer 561 has prime factorisation:

$$561 = 3 \cdot 11 \cdot 17$$

and so it is not prime.

We will show that $a^{561} = a \mod 561$ by showing that

$$\begin{aligned} a^{561} &= a \mod 3 \\ a^{561} &= a \mod 11 \\ a^{561} &= a \mod 17. \end{aligned}$$

(This implies that $a^{561} = a \mod 561$ by Theorem 13.2.)

① Let us first show $a^{561} = a \mod 3$.
If $3 \mid a$, then $a = 0 = a^{561} \mod 3$, and we are done.

If $3 \nmid a$, then Fermat's theorem (a) tells us that $a^2 = 1$. Hence,

$$a^{561} = a^{560} \cdot a = (\underbrace{a^2}_{=1 \mod 3})^{280} \cdot a = a \mod 3$$

as required.

② $a^{561} = a \mod 11$.

Similarly, if $11 \mid a$, then $a = 0 = a^{561} \mod 11$. If $11 \nmid a$, then Fermat's theorem (a) tells us that $a^10 = 1 \mod 11$. Hence,

$$a^{561} = a^{560} \cdot a = (\underbrace{a^{10}}_{=1 \mod 11})^{56} \cdot a = a \mod 11.$$

③ $a^{561} = a \mod 17$.

Finally, if $17 \mid a$ then $a = 0 = a^{561} \mod 17$. If $17 \nmid a$ then by Fermat's Theorem (a) $a^{16} = 1 \mod 17$ and

$$a^{561} = a^{560} \cdot a = (\underbrace{a^{16}}_{=1 \mod 17})^{35} \cdot a = a \mod 17.$$

Definition 2.43. A composite integer n such that $a^n = a \mod n$ for all $a \in \mathbb{Z}$ is called a Carmichael number .

Fermat's theorem can be used to prove the following result, which is the heart of the RSA code.

Theorem 2.44. *Let a be any integer. Let p and q be distinct primes and write $N = p \cdot q$. If e and f are positive integers such that*

$$ef \equiv 1 \mod (p-1)(q-1),$$

then

$$(a^e)^f \equiv a \mod N.$$

Proof. Since N has prime factorisation $N = p \cdot q$, Theorem 13.2 tells us that

$$(a^e)^f \equiv a \mod N$$

if and only if

$$\begin{cases} (a^e)^f \equiv a \mod p \\ (a^e)^f \equiv a \mod q. \end{cases}$$

① We first show that $(a^e)^f \equiv a \mod p$.

If $p \mid a$, then $a = 0 \mod p$, so that $a = 0 = (a^e)^f \mod p$ and we are done. On the other hand, if $p \nmid a$, then Fermat's theorem (a) tells us that $a^{p-1} = 1 \mod p$.

By definition of e and f,

$$ef \equiv 1 \mod (p-1)(q-1)$$

which means that there is an integer k with

$$ef = k(p-1)(q-1) + 1.$$

Hence,

$$(a^e)^f = a^{ef} = a^{k(p-1)(q-1)+1} = (\underbrace{a^{p-1}}_{=1 \mod p})^{k(q-1)} \cdot a = a \mod p$$

as required.

② Similarly, $(a^e)^f \equiv a \mod q$. Hence, the result follows. □

2.7 RSA code

Problem.

- Alice and Bob would like to communicate via an insecure network, so that messages can be read by an eavesdropper, Eve.
- To keep their messages private, Alice and Bob would like to encode them. But in order to agree on a coding system, they need to communicate via the network, so Eve will also know the coding system and will be able to easily decode the message.

In principle, there is no way around this. In practice, one can make it hard for Eve to figure out the coding system using the RSA code.

Setup.

- Alice and Bob exchange a list of $M+1$ codes indexed by integers $0 \leq n < M$ (so this list is also available to Eve).
- In order to agree on a coding system, Alice will send Bob a secret message consisting of an integer a with $0 \leq a < M$.

The question is: How to do this without Eve knowing the value of a?

Steps.

- Bob chooses:
  - Two primes $p, q \geq \sqrt{M}$,
  - A a positive integer e coprime to $(p-1)(q-1)$.
- Bob computes:
  - $N = pq$ [**Note:** $N = pq \geq M$].[5],
  - An integer f such that [6]

$$ef = 1 \mod (p-1)(q-1).$$

- Bob tells Alice (and Eve) the values of N and e but he keeps the values of p, q and f secret.
- Alice computes the integer[7]

$$c = a^e \mod N$$

[**Note:** $0 \leq c < N$].

5. Bob can check if the integers p and q are prime using Fermat's theorem or the other methods in section 4

6. Bob can use the Euclidean algorithm to check that e is coprime to $(p-1)(q-1)$. He can use reverse substitution to find f.

7. Alice can use binary expansion and repeated squaring to compute c.

- Alice tells Bob (and Eve) the value of c.
- Using Theorem 2.44, Bob can now decode the message by computing
$$c^f = (a^e)^f = a \mod N.$$

Example 2.45. Alice will send Bob an integer $2 \leq a < 324$.

a) Since $\sqrt{324} = 18$, Bob chooses prime numbers $p = 23, q = 29 \geq 18$.
   - Bob knows that these numbers are prime by applying Lemma 13.1: $23, 98 < 36$ and so if 23 or 29 were composite, they would have a prime factor $p' < 6$. All of the primes < 6 are: $2, 3, 5$. Since 23 and 29 are not divisible by any of these primes, they must be prime themselves.
   - Bob computes the product
$$N = pq = 23 \cdot 29 = 667.$$

b) Bob chooses the integer $e = 367$ which he checks is coprime to $(p-1)(q-1) = 616$ by running the Euclidean algorithm and finding $\gcd(616, 367) = 1$. By reverse substitution in the Euclidean algorithm, he finds that
$$367 \cdot 47 = 1 \mod 616$$
   and so he chooses $f = 47$.

c) Bob tells Alice (and Eve) the values: $N = 667$ and $e = 367$.

d) Alice wants to send Bob the integer $a = 63$, so she computes $63^{367} \mod 667$.
   - She can compute this by finding the binary expansion
$$367 = 2^8 + 2^6 + 2^5 + 2^3 + 2^2 + 2^1 + 2^0$$
     and using the method of successive squaring.
   - She finds that $c = 63^{367} = 38 \mod 667$.

   Alice tells Bob (and Eve) the value $c = 38$.

e) Bob decodes the message c by computing:
$$c^f = 38^{47} = 63 = a \mod 667.$$

   We can summarise the RSA code using the following table.

Information Involved	Alice Knows	Eve Knows	Bob Knows
p	×	×	✓
q	×	×	✓
N	✓	✓	✓
$(p-1)(q-1)$	×	×	✓
e	✓	✓	✓
f	×	×	✓
c	✓	✓	✓

Q5 Why is hard for Eve to decode the message?

A: Eve does not know the value of f, so she cannot compute c^f.

To compute f, she needs to first find the values of p and q from $N = pq$.

Ultimately, this strategy depends on the following observation. Consider the sets

$$A = \{(p,q) \mid p \text{ and } q \text{ are primes with } p < q\},$$
$$B = \{p \cdot q \mid p \text{ and } q \text{ are primes with } p < q\}.$$

Then, there is an easily computable bijection:

$$f\colon A \to B\colon (p,q) \mapsto pq.$$

This function has an inverse f^{-1}, but this inverse is actually hard to compute.

Definition 2.46. An easily computable bijection whose inverse is hard to compute is called a one way function .

The encryption methods we learn in this course can be boiled down to finding different one-way functions!

> **Note:** Actually, one should require $a \geq 2$ because Eve knows that $0^f = 0$ and $1^f = 1$, even if she does not know the value of f.

2.8 Euler's Theorem

Euler's theorem is a generalisation of Fermat's theorem. This result is helpful when computing powers $a^k \mod m$.

Let p be a prime and let a be any integer coprime to p.

Recall that Fermat's theorem proves that $a^{p-1} = 1 \mod p$. Moreover, notice that there are $p-1$ integers in $\mathbb{Z}/p$ which are corpime to p (since all nonzero integers in $\mathbb{Z}/p$ are coprime to p).

2.8.1 Euler's Phi Function

Definition 2.47. Let $\mathbb{Z}_+$ denote the set of all positive integers. Then, we can define a function

$$\phi\colon \mathbb{Z}_+ \to \mathbb{Z}_+\colon n \mapsto \#(\text{ integers in } \mathbb{Z}/n \text{ coprime to } n\ )$$

called Euler's phi function .

Example 2.48. a) $\phi(1) = 1$ because $\mathbb{Z}/1 = \{0\}$ and $\gcd(0,1) = 1$ so 0 is coprime to 1.

b) $\phi(4) = 2$ because $\mathbb{Z}/4 = \{0,1,2,3\}$ and

$$\gcd(0,4) = 4,$$
$$\gcd(1,4) = 1,$$
$$\gcd(2,4) = 2,$$
$$\gcd(3,4) = 1.$$

Hence, 1 and 3 are the only integers in $\mathbb{Z}/4$ coprime to 4.

c) For any prime p, $\phi(p) = p - 1$ since all nonzero integers in $\mathbb{Z}/p$ are coprime to p.

Theorem 2.49. *Let $n > 1$ be an integer and let $p_1, \ldots, p_r$ be the distinct prime factors of n. Then,*

$$\phi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Example 2.50. The integer $12 = 2^2 \cdot 3$ has prime factors $2, 3$. Hence,

$$\phi(12) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

Proof of Theorem 2.49. This is an application of the Inclusion-Exclusion Principle.

Let $n > 1$ have prime factors $p_1, \ldots, p_r$. For $i \in \{1, 2, \ldots, r\}$, let

$$\begin{aligned} A_i &= \{\text{integers in } \mathbb{Z}/n \text{ which are divisible by } p_i\} \\ &= \{\text{non-negative integers in } < n \text{ which are divisible by } p_i\} \quad (25) \end{aligned}$$

Let S be the set of integers coprime to n. Then, by definition, $\phi(n) = |S|$.

The integers coprime to n are integers which are not divisible by any of the primes $p_1, \ldots, p_r$. Therefore,

$$S = \mathbb{Z}/n - A_1 \cup \ldots \cup A_r$$

and so, by the subtraction principle,

$$\phi(n) = |S| = \underbrace{|\mathbb{Z}/n|}_{=n} - |A_1 \cup \ldots \cup A_r|. \tag{26}$$

The inclusion-exclusion principle tells us that

$$|A_1 \cup \ldots \cup A_r| = \sum_{i=1}^{r} |A_i| - \sum_{1 \le i < j \le r} |A_i \cap A_j| + \sum_{1 \le i < j < k \le r} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{r-1} |A_1 \cap \ldots \cap A_r|. \tag{27}$$

From Equation (25), recall from previous lectures that

$$|A_i| = \lfloor \frac{n}{p_i} \rfloor = \frac{n}{p_i}$$

since p_i is a factor of n.

Similarly,

$$\begin{aligned} A_i \cap A_j &= \{\text{integers in } \mathbb{Z}/n \text{ which are divisible by } p_i \text{ and } p_j\} \\ &= \{\text{non-negative integers} < n \text{ which are divisible by } p_i \cdot p_j.\} \end{aligned}$$

Hence,

$$|A_i \cap A_j| = \lfloor \frac{n}{p_i \cdot p_j} \rfloor = \frac{n}{p_i \cdot p_j}.$$

Likewise, the intersection of t sets has cardinality

$$\begin{aligned} |A_{i_1} \cap \ldots \cap A_{i_t}| &= |\{\text{integers in } \mathbb{Z}/n \text{ which are divisible by } p_{i_1} \cdot \ \ldots \ \cdot p_{i_t}\}| \\ &= \frac{n}{p_{i_1} \cdot \ \ldots \ \cdot p_{i_t}}. \end{aligned}$$

Subbing this into (27), we have

$$|A_1 \cup \ldots \cup A_r| = \sum_{i=1}^{r} \frac{n}{p_i} - \sum_{1 \le i < j \le r} \frac{n}{p_i \cdot p_j} + \sum_{1 \le i < j < k \le r} \frac{n}{p_i \cdot p_j \cdot p_k} + \ldots + (-1)^{r-1} \frac{n}{p_1 \cdot \ \ldots \ \cdot p_r}.$$

Subbing this into (26),

$$\begin{aligned} \phi(n) &= n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1 \le i < j \le r} \frac{n}{p_i \cdot p_j} - \sum_{1 \le i < j < k \le r} \frac{n}{p_i \cdot p_j \cdot p_k} + \ldots + (-1)^{r} \frac{n}{p_1 \cdot \ \ldots \ \cdot p_r} \\ &= n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right) \end{aligned} \tag{28}$$

as required. □

Corollary 2.51. *Let $n > 1$ be an integer with prime factorisation*

$$n = p_1^{\alpha_1} \cdot \ \ldots \ \cdot p_r^{\alpha_r}.$$

Then,

$$\phi_n = p_1^{\alpha_1 - 1} \cdot \ \ldots \ \cdot p_r^{\alpha_r - 1} \cdot (p_1 - 1) \ldots (p_r - 1).$$

Proof. Substitute

$$n = p_1^{\alpha_1} \cdot \ \ldots \ \cdot p_r^{\alpha_r}$$

into (28) and simplify. □

2.8.2 Euler's Theorem

We are finally ready to state Euler's theorem.

Theorem 2.52. *Let n be a positive integer and let a be any integer coprime to n. Then,*

$$a^{\phi(n)} = 1 \mod n.$$

Proof. Let $x_1 \, , \, x_2 \ \ldots \, , \, x_{\phi(n)}$ be the integers in $\mathbb{Z}/n$ which are coprime to n. Consider the list

$$ax_1 \, , \, ax_2 \ \ldots \, , \, ax_{\phi(n)}.$$

Since a is also coprime to n, Theorem 2.21 tells us that this list is just a reordering of the list

$$x_1 \, , \, x_2 \ \ldots \, , \, x_{\phi(n)}.$$

Hence,

$$x_1 \cdot x_2 \cdot \ \ldots \ \cdot x_{\phi(n)} = ax_1 \cdot ax_2 \cdot \ \ldots \ \cdot ax_{\phi(n)}$$

which implies

$$x_1 \cdot x_2 \cdot \ \ldots \ \cdot x_{\phi(n)} = a^{\phi(n)} \cdot (x_1 \cdot x_2 \cdot \ \ldots \ \cdot x_{\phi(n)}) \tag{29}$$

Notice that $x_1 \cdot \ \ldots \ \cdot x_{\phi(n)}$ is coprime to n, and so Proposition 2.18 tells us that there is a b such that

$$b \cdot (x_1 \cdot x_2 \cdot \ \ldots \ \cdot x_{\phi(n)}) = 1 \mod n.$$

Therefore, multiplying both sides of Equation (29) by b gives

$$1 = a^{\phi(n)} \mod n$$

as required. □

Example 2.53. Find the remainder of 7^{50} when dividing by 20.

Solution. First, note that $\gcd(7,20) = 1$ and so Euler's theorem tells us that

$$7^{\phi(20)} = 1 \mod 20.$$

Thus, we next need to find $\phi(20)$. Since $20 = 2^2 \cdot 5$, then by Corollay 16.1 we have:

$$\phi(20) = 2^{2-1} \cdot (2-1) \cdot (5-1) = 8.$$

Hence, $7^8 = 1 \mod 20$.

Finally, note that $50 = 8 \cdot 6 + 2$, and so

$$7^{50} = 7^{8\cdot 6+2} = (\underbrace{7^8}_{=1})^6 \cdot 7^2 = 7^2 = 9 \mod 20.$$

Example 2.54. Find the last two digits of 3^{2015}.

Solution. Finding the last two digits of an integer n amounts to computing the remainder of n when dividing by 100. Hence, we want to compute $3^{2015} \mod 100$.

First, sicen $\gcd(3,100) = 1$, then Euler's theorem tells us that $3^{\phi(100)} = 1 \mod 100$.

Therefore, we next need to compute $\phi(100)$. Since $100 = 2^2 \cdot 5^2$, then

$$\phi(100) = 2^{2-1} \cdot 5^{2-1} \cdot (2-1) \cdot (5-1) = 40$$

and so Euler's theorem tells us that

$$3^{40} = 1 \mod 100.$$

Thirdly, note that $2015 = 50 \cdot 40 + 15$ and so

$$3^{2015} = (\underbrace{3^{40}}_{=1})^{50} \cdot 3^{15} = 3^{15} \mod 100.$$

Finally, we compute 3^{15} by finding the binary expansion of 15 and then applying the method of successive squaring. Well,

$$15 = 2^3 + 2^2 + 2 + 1$$

so that

$$3^{15} = 3^8 \cdot 3^4 \cdot 3^2 \cdot 3$$

and now we compute each of these powers:

$$\begin{aligned}
3 &= 3 \mod 100 \\
3^2 &= 9 \mod 100 \\
3^4 = 9^2 &= 81 = -19 \mod 100 \\
3^8 = (-19)^2 &= 361 = 61 = -39 \mod 100.
\end{aligned}$$

Hence,

$$3^{15} = (-39) \cdot (-19) \cdot 9 \cdot 3 = 2007 = 07 \mod 100$$

and so the last two digits are 07.

2.8.3 Units

In Q44 of the tutorial exercises, we showed that every element $a \in \mathbb{Z}/15$ which is coprime to 15 has a multiplicative inverse .

(*Recall that a multiplicative inverse of $a \in \mathbb{Z}/m$ is an element $r \in \mathbb{Z}/m$ such that $ra = 1 \mod m$.*)

This fact is actually true more generally: An element in $a \in \mathbb{Z}/m$ has a multiplicative inverse if and only if it is coprime to m.

This is a consequence of Proposition 2.18 which states that there exists an integer r such that $ra = 1 \mod m$ if and only if a and m is coprime.

Definition 2.55. Let m be a positive integer.

a) An element $a \in \mathbb{Z}/m$ is a unit if and only if it has a multiplicative inverse.

b) Define the group of units as the subset $(\mathbb{Z}/m)^\times \subset \mathbb{Z}/m$:

$$\begin{aligned}(\mathbb{Z}/m)^\times &:= \{\text{Elements in } \mathbb{Z}/m \text{ which are units}\} \\ &= \{\text{Elements in } \mathbb{Z}/m \text{ which are coprime to } m\}.\end{aligned}$$

Example 2.56. Consider $\mathbb{Z}/14 = \{0, 1, \ldots, 13\}$.

$(\mathbb{Z}/14)^\times = \{\text{Elements in } \mathbb{Z}/14 \text{ which are coprime to } 14\} = \{1, 3, 5, 9, 11, 13\}$.

So $|(\mathbb{Z}/14)^\times| = 6$.

From the definition of Euler's phi function,

$$\begin{aligned}\phi(m) &= \#\,(\text{Elements in } \mathbb{Z}/m \text{ which are coprime to } m) \\ &= \#\,(\text{Units in } \mathbb{Z}/m) \\ &= |(\mathbb{Z}/m)^\times|.\end{aligned}$$

Example 2.57. $\phi(14) = 6 = |(\mathbb{Z}/14)^\times|$.

Example 2.58. How many units are there in $\mathbb{Z}/300$? How many elements does the group of units have?

Solution. The number of units in $\mathbb{Z}/300$ is the same as the number of elements in $\mathbb{Z}/300$ which are coprime to 300. This is given by $\phi(300)$.

Since $300 = 3 \cdot 2^2 \cdot 5^2$, then

$$\phi(300) = 2 \cdot 5 \cdot (2-1) \cdot (3-1) \cdot (5-1) = 2 \cdot 5 \cdot 2 \cdot 4 = 80.$$

Since the group of units is the set of all units, then it has 80 elements.

Moreover, Euler's theorem gives us a way to find multiplicative inverses of units.

Example 2.59. Find the multiplicative inverse of 3 in $\mathbb{Z}/14$.

Solution. Since $\gcd(3,14) = 1$, Euler's theorem tells us that $3^{\phi(14)} = 1 \mod 14$.

Moreover, $14 = 7 \cdot 2$ and so $\phi(14) = (2-1)(7-1) = 6$ and so,

$$\begin{aligned} 3^6 &= 1 \mod 14 \implies \\ 3 \cdot 3^5 &= 1 \mod 14. \end{aligned}$$

Hence, 3^5 is the inverse of 3 in $\mathbb{Z}/14$. We therefore just need to compute 3^5.

The binary expansion of 5 is $5 = 2^2 + 1 = 4 + 1$ and so $3^5 = 3^4 \cdot 3$.

Using successive squaring:

$$\begin{aligned} 3 &= 3 \mod 14 \\ 3^2 &= 9 = -5 \mod 14 \\ 3^4 &= (-5)^2 = 25 = 11 = -3 \mod 14. \end{aligned}$$

Hence, the inverse of 3 in $\mathbb{Z}/14$ is:

$$3^5 = -3 \cdot 3 = -9 = 5 \mod 14.$$

Hence, the multiplicative inverse of $3 \in \mathbb{Z}/14$ is 5.

From example 2.59, we know that $3 \in \mathbb{Z}/14$ is a unit since it is coprime to 14 and that its inverse is $3^5 = 3^{\phi(14)-1}$. This is actually true more generally:

> If $a \in \mathbb{Z}/m$ is a unit, then $a^{\phi(m)-1} \in \mathbb{Z}/m$ is its multiplicative inverse.

2.9 Fields

We will see that if every nonzero element in $\mathbb{Z}/m$ is a unit, then $\mathbb{Z}/m$ is a finite field .

Our goal today is to understand the basics of finite fields , as they can be used in cryptography to construct various one-way functions.

2.9.1 Some intuition

Fields are sets on which the addition, subtraction, multiplication and division have been defined and behave nicely.

Example 2.60. The set of real numbers $\mathbb{R}$ is a field.

The abstract definition of a field extracts "nice" arithmetic properties of $\mathbb{R}$ which we would like all fields to satisfy.

- We can add and multiply numbers in $\mathbb{R}$. Formally, what this means is: Given any three numbers $a, b \in \mathbb{R}$, there are two well-defined

rules:

$$\begin{aligned}\mathbb{R}\times\mathbb{R} &\to \mathbb{R}\\ (a,b) &\mapsto a+b\\ (a,b) &\mapsto a\cdot b\end{aligned}$$

which send a pair (a,b) to numbers in $\mathbb{R}$ represented by the symbols $a+b$ and $a\cdot b$.

For example,

$$\begin{aligned}\mathbb{R}\times\mathbb{R} &\to \mathbb{R}\\ (3,7) &\mapsto 3+7=10\\ (3,7) &\mapsto 3\cdot 7=21\end{aligned}$$

- Moreover, $\mathbb{R}$ has two distinguished elements $0,1\in\mathbb{R}$ which satisfy

(F1) $0+a=a$ for all $a\in\mathbb{R}$,

(F2) $1\cdot a=a$ for all $a\in\mathbb{R}$.

- Nonzero numbers in $\mathbb{R}$ have additive and multiplicative inverses. Let $a\in\mathbb{R}$ be any nonzero number. Then,

(F3) a has an additive inverse: There is an element $-a\in\mathbb{R}$ such that

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

e.g. $7+(-7)=0$.

(F4) a has a multiplicative inverse: There is an element $a^{-1}\in\mathbb{R}$ such that

$$a\cdot a^{-1}=1$$

e.g. $7\cdot(1/7)=1$.

[**Note:** We can define subtraction by a as addition by $(-a)$ and division by a as multiplication by a^{-1}.]

- Finally, addition and multiplication behave nicely.

(F5) Addition and multiplication are commutative:

- $a+b=b+a$ for all $a,b\in\mathbb{R}$,
- $a\cdot b=b\cdot a$ for all $a,b\in\mathbb{R}$.

(F6) Addition and multiplication are associative:

- $(a+b)+c=a+(b+c)$ for all $a,b,c\in\mathbb{R}$,
- $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ for all $a,b,c\in\mathbb{R}$.

(F7) Multiplication distributes over addition:

- $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$ for all $a,b,c\in\mathbb{R}$.

Example 2.61. • $\mathbb{Q}$ and $\mathbb{C}$ are fields (addition and multiplication function as in $\mathbb{R}$).

- $\mathbb{Z}$ is not a field.

  The crucial difference is that not every element has a multiplicative inverse. For example, there is no integer n such that $3n = 1$.

- $\mathbb{N}$ is not a field.

  The crucial differences here are that not every element has a multiplicative or an additive inverse. For example, there is no integer n such that $3 + n = 0$.

2.9.2 Field Axioms

Definition 2.62 (Field)**.** Let F be a set with at least two distinct elements $0, 1 \in F$ together with two well-defined rules:

- $F \times F \to F \colon (a, b) \mapsto a + b$,
- $F \times F \to F \colon (a, b) \mapsto a \cdot b$,

which send every pair $(a, b) \in F \times F$ to well-defined elements in $a + b, a \cdot b \in F$.

Then, we say that F is a field if it satisfies the following axioms:

(F1) $0 + a = a$ for all $a \in F$.

(F2) $1 \cdot a = a$ for all $a \in F$.

(F3) Every $a \in F$ has an additive inverse: there is an element $-a \in F$ such that $a + (-a) = 0$.

(F4) Every nonzero $a \in F$ has a multiplicative inverse: there is an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

(F5) Addition and multiplication are commutative:

- $a + b = b + a$ for all $a, b \in F$,
- $a \cdot b = b \cdot a$ for all $a, b \in F$.

(F6) Addition and multiplication are associative:

- $(a + b) + c = a + (b + c)$ for all $a, b, c \in F$,
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in F$.

(F7) Multiplication distributes over addition:

- $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in F$.

Example 2.63. Consider the set S be the set

$$S = \{0, 1, \alpha\}$$

where addition and multiplication are defined by the following tables.

$+$	0	1	α
0	0	1	α
1	1	α	0
α	α	0	1

$\times$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	1

Then, S is a field. Exercise: Check that axioms 1-7 hold for S .

Example 2.64. The set of 2×2 matrices

$$M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d, \in \mathbb{R} \right\}$$

is not a field.

- Multiplication is not commutative:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$$

- Not every element has a multiplicative inverse:

$$\begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$$

  has determinant zero, and so is not invertible.

In summary, a field F is a set where addition, multiplication, subtraction and division are defined and behave "nicely".

2.9.3 When is $\mathbb{Z}/m$ a field?

Theorem 2.65. *Let m be a positive integer. Then, $\mathbb{Z}/m$ is a field if and only if m is prime.*

Proof. Exercise: Check that for any integer $m > 1$, then $\mathbb{Z}/m$ satisfies all axioms (F1)–(F7) except maybe (F4).

Thus, we just need to show that $\mathbb{Z}/m$ satisfies (F4) if and only if m is prime.

Recall that (F4) states that every nonzero element in $\mathbb{Z}/m$ has a multiplicative inverse.

($\implies$) Suppose that every nonzero element in $a \in \mathbb{Z}/m$ has a multiplicative inverse. Then, for every $a \in \mathbb{Z}/m$, there is an $r \in \mathbb{Z}/m$ such that

$$ra = 1 \mod m.$$

By Proposition 2.18, this means that a is coprime to m. Hence, m is coprime to every integer in $\mathbb{Z}/m$. In other words, integers in $\{2, \ldots, m-1\}$ do not divide m. This means that the only factors of m are 1 and itself. I.e. m is prime.

($\impliedby$) Suppose that m is prime, then every nonzero integer in $\mathbb{Z}/m$ is coprime to m. By Proposition 2.18, then every nonzero integer in $\mathbb{Z}/m$ is a unit (has a multiplicative inverse). Hence, (F4) is satisfied. □

Notation 2.66. Let p be a prime. We will often write $\mathbb{F}_q := \mathbb{Z}/p$.

2.9.4 Properties of Fields

Definition 2.67. A finite field is a field F which has finitely many elements.

For example, $S = \{0, 1, \alpha\}$ in example 2.63 has $|S| = 3$ and so is a finite field. Similarly, $\mathbb{F}_p$ has $|\mathbb{F}_p| = p$ elements, and so is a finite field.

Definition 2.68. The order of a field F is $|F|$.

Example 2.69. a) The order of S in example 2.63 is $|S| = 3$.

b) The order of $\mathbb{F}_p = \mathbb{Z}/p = \{0, \dots p-1\}$ is p.

The last property of fields we would like to discuss is a generalisation of Fermat's theorem to any finite field. However, we will first need a lemma.

Lemma 2.70. *Let F be a field, and let $a, x, y \in F$ be nonzero elements. Then,*

a) $a \cdot x \neq 0$,

b) $a \cdot x = a \cdot y$ *if and only if* $x = y$.

Proof. a) Suppose that $a \cdot x = 0$. Since F is a field and a is nonzero, we can divide by a. Dividing both sides of the equation by a gives us $x = 0$, which is a contradiction since we assumed $x \neq 0$.

b) ($\implies$) Suppose $a \cdot x = a \cdot y$. Then, as before, we can divide by a. Dividing both sides of the equation by a gives us $x = y$.

($\impliedby$) If $x = y$, then multiplying both sides by a gives us $a \cdot x = a \cdot y$.

□

Theorem 2.71 (Generalisation of Fermat's theorem)**.** *Let F is a field of order q.*

a) If $a \in F$ is nonzero, then $a^{q-1} = 1$ in F.

b) If $b \in F$ is any element of F, ten $a^q = a$.

Proof. a) Since F has order q, it has q elements, of which one is 0. Hence, there are $q - 1$ nonzero elements in F and we can list them as:

$$x_1, \dots, x_{q-1}. \tag{30}$$

Let $a \in F$ be nonzero. Then, we can make a new list

$$a \cdot x_1, \dots, a \cdot x_{q-1}. \tag{31}$$

By Lemma 2.70, (31) is a list of $q - 1$ distinct nonzero elements in F. In other words, 31 is a list of all the nonzero elements in F. Therefore, it must be a reordering of (30).

Thus,

$$x_1 \cdot \dots \cdot x_{q-1} = a x_1 \cdot \dots \cdot a x_{q-1} \implies$$
$$x_1 \cdot \dots \cdot x_{q-1} = a^{q-1} \cdot (x_1 \cdot \dots \cdot x_{q-1})$$

Since the product $x_1 \cdot \ldots \cdot x_{q-1}$ is a nonzero element in F, we can divide both sides by this product to get

$$1 = a^{q-1}$$

as required.

b) There are two cases to consider.

If $b = 0$, then $b^q = 0^q = 0 = b$ and we are done.

If $b \neq 0$, then part (a) tells us that $b^{q-1} = 1$. Multiplying both sides by b gives $b^q = b$, as required.

□

2.10 Primitive Elements and one-way functions

In this section, we will explain how we can generate a one-way function using finite fields.

2.10.1 One-way functions

Example 2.72. a) In $\mathbb{F}_{13}$ the powers 2: $2^0, 2^1, \ldots, 2^{11}$ are

$$\begin{aligned}
2^0 &= 1 \mod 13\\
2^1 &= 2 \mod 13\\
2^2 &= 4 \mod 13\\
2^3 &= 8 \mod 13\\
2^4 &= 3 \mod 13\\
2^5 &= 6 \mod 13\\
2^6 &= 12 \mod 13\\
2^7 &= 11 \mod 13\\
2^8 &= 9 \mod 13\\
2^9 &= 5 \mod 13\\
2^{10} &= 10 \mod 13\\
2^{11} &= 7 \mod 13.
\end{aligned}$$

Notice that every nonzero element in $\mathbb{F}_{13}$ appears exactly once in the list above. (I.e. every nonzero element in $\mathbb{F}_{13}$ is a power of 2,)

Hence, we can write down a bijection

$$\begin{aligned}
\{0, 1, \ldots, 11\} &\to \mathbb{F}_{13} - \{0\}\\
i &\mapsto 2^i
\end{aligned}$$

This bijection is easy to compute, but its inverse is hard to compute. Hence, it is a one-way function.

b) In $\mathbb{F}_{17}$ this is not true. The powers of 2: $2^0, 2^1, \ldots, 2^{15}$ are:

$$\begin{aligned}
2^0 &= 1 \mod 17\\
2^1 &= 2 \mod 17\\
2^2 &= 4 \mod 17\\
2^3 &= 8 \mod 17\\
2^4 &= 16 \mod 17\\
2^5 &= 15 \mod 17\\
2^6 &= 13 \mod 17\\
2^7 &= 9 \mod 17\\
2^8 &= 1 \mod 17\\
2^9 &= 2 \mod 17\\
2^{10} &= 4 \mod 17\\
2^{11} &= 8 \mod 17\\
2^{12} &= 16 \mod 17\\
2^{13} &= 15 \mod 17\\
2^{14} &= 13 \mod 17\\
2^{15} &= 9 \mod 17
\end{aligned}$$

Notice that in this case some numbers appear twice (e.g. 1) and some numbers in $\mathbb{F}_{13} - \{0\}$ don't appear at all (e.g. 3).

Hence, the function

$$\begin{aligned}\{0, 1, \ldots, 15\} &\to \mathbb{F}_{17} - \{0\}\\ i &\mapsto 2^i\end{aligned}$$

is neither injective nor surjective.

On the other hand, we can check that the function

$$\begin{aligned}\{0, 1, \ldots, 15\} &\to \mathbb{F}_{17} - \{0\}\\ i &\mapsto 3^i\end{aligned}$$

is bijective.

Q6 What makes $2 \in \mathbb{F}_{13}$ and $3 \in \mathbb{F}_{17}$ special?

A: They are **primitive elements**.

2.10.2 Primitive Elements

We will say that elements in $a \in \mathbb{F}_q$ which generate bijections

$$\begin{aligned}\{0, 1, \ldots, q-2\} &\to \mathbb{F}_q - \{0\}\\ i &\mapsto a^i\end{aligned}$$

are primitive elements . More concisely,

Definition 2.73. Let F be a finite field of order q. A nonzero element $a \in F$ is primitive if all of the nonzero elements in F can be listed without repetition as

$$1, a^1, a^2, \ldots, a^{q-2}$$

Example 2.74. a) $2 \in \mathbb{F}_{13}$ is primitive, since from example 2.72 we see that every nonzero element in $\mathbb{F}_{13}$ appears in the list $2^0, 2^1, \ldots, 2^{11}$ exactly once.

b) $2 \in \mathbb{F}_{17}$ is not primitive since we cannot get a $1 \in \mathbb{F}_{17}$ appears twice as 2^0 and 2^8 in $\mathbb{F}_{17}$.

c) Exercise: Check that $3 \in \mathbb{F}_{17}$ is primitive.

Q7 Why do we only take powers up to $q-2$? E.g. in $\mathbb{F}_{13}$ we took powers up to 11 and in $\mathbb{F}_{17}$ we took powers up to 15.

A: Since a is a nonzero element, the generalisation of Fermat's theorem tells us that $a^{q-1} = 1$ in F.

Hence, the list of powers a^k larger than $q-2$:

$$a^{q-1}\ ,\ a^q\ ,\ a^{q+1}\ ,\ \ldots$$

is the same as

$$\underbrace{a^{q-1}}_{1}\ ,\ \underbrace{a^{q-1}}_{1} \cdot a\ ,\ \underbrace{a^{q-1}}_{1} \cdot a^2\ ,\ \ldots$$

which simplifies to

$$1, a^1, a^2, \ldots$$

and so for $k \geq q-1$, powers a^k start repeating.

Proposition 2.75. *Let a be a nonzero element in a field F of order q. Let k be any integer and let r be the remainder of k when dividing by $(q-1)$. Then,*

$$a^k = a^r.$$

Proof. Using the division algorithm, we can always write any integer as $k = n \cdot (q-1) + r$. Therefore,

$$a^k = a^{n\cdot(q-1)+r} = (\underbrace{a^{q-1}}_{=1})^n \cdot a^r = a^r.$$

□

Q8 How to find primitive elements? Do they always exist?

In Example 2.72, we found primitive elements by brute force by computing all the powers of $2 \in \mathbb{F}_{13}$ and showing that they satisfy the definition of a primitive element. There is a more efficient way of doing this, which we will learn in later sections.

For now, what we will show is that once we have found one primitive element in F, then we can find all of them.

Theorem 2.76. *Let F be a field of order q. Suppose that $a \in F$ is a primitive element. Let $k_1, k_2, \ldots, k_t$ be all of the integers in $\{0, 1, \ldots, q-1\}$ which are coprime to $q-1$. Then, the complete set of primitive elements in F is:*

$$a^{k_1}, \ldots, a^{k_t}.$$

Example 2.77. Find all of the primitive elements in $\mathbb{F}_{13}$.

Solution.

From Example 2.72, we know that $2 \in \mathbb{F}_{13}$ is primitive.

The field $\mathbb{F}_{13}$ has $q = 13$, so to find all of the primitive elements we consider the set

$$\{0, 1, \ldots, q-1 = 12\}$$

and choose all integers in this set which are coprime to $q - 1 = 12$. These are: $1, 5, 7, 11$.

Hence, by Theorem 2.76, the complete set of primitive elements in $\mathbb{F}_{13}$ is:

$$2^1, 2^5, 2^7, 2^{11} \mod 13.$$

We can compute these powers in the following way:

$$\begin{aligned}
2^2 &= 4 \mod 13 \\
2^4 &= 16 = 3 \mod 13 \\
2^5 &= 2^4 \cdot 2 = 3 \cdot 2 = 6 \mod 13 \\
2^7 &= 2^5 \cdot 2^2 = 6 \cdot 4 = -2 = 11 \mod 13 \\
2^{11} &= 2^7 \cdot 2^4 = (-2) \cdot 3 = -6 = 7 \mod 13.
\end{aligned}$$

Hence, the primitive elements in $\mathbb{F}_{13}$ are

$$2, 6, 11, 7.$$

2.10.3 Bonus: Proof of Theorem 2.76

In this section, we present a proof of the theorem 2.76. First, we will need the following proposition.

Proposition 2.78. *Let k be an integer, and let F be a field of order q. Suppose that $a \in F$ is a primitive element. Then, $a^k \in F$ is primitive if and only if k is coprime to $q-1$.*

Proof. ($\implies$) Suppose that $a^k \in F$ is primitive. Then,

$$1, a^k, (a^k)^2, \ldots, (a^k)^{q-1}$$

are all of the nonzero elements in F. Therefore, there must be an m such that $(a^k)^m = a$. In other words, $a^{km} = a$.

Using the division algorithm, we can write

$$km = n \cdot (q-1) + r$$

with $0 \leq r \leq q-2$. By the generalisation of Fermat's theorem,

$$a = a^{km} = (\underbrace{a^{q-1}}_{=1})^n \cdot a^r = a^r.$$

Now, we know that a is primitive, so that assignment

$$\{0, \ldots, q-2\} \to F \colon a \mapsto a^i$$

is injective. Hence, $a^r = a = a^1$ if and only if $r = 1$. Thus,

$$km = n \cdot (q-1) + 1$$

which tells us that $km \equiv 1 \mod (q-1)$. By proposition 11.2, this can only happen if k and $q-1$ are coprime.

($\Longleftarrow$) Suppose that k and $q-1$ are coprime.

① By definition a^k is primitive if

$$a, a^k, (a^k)^2, \ldots, (a^k)^{q-2} \tag{32}$$

is a list of $q-1$ distinct nonzero elements in F.

② Since $a \neq 0$, then $a^k \neq 0$, so all we need to do is show that the elements in the list (32) are distinct.

Suppose that there are integers $1 \leq s, t \leq q-2$ such that

$$(a^k)^s = (a^k)^t. \tag{33}$$

In order to prove that the elements in (32) are distinct, we want to show that $k = t$.

Well, (33) tells us that $a^{ks} = a^{kt}$. Since F is a field, we can divide both sides by a^{kt}, so we get

$$\begin{aligned} \frac{a^{ks}}{a^{kt}} = 1 &\implies \\ a^{kt} \cdot a^{-kt} = 1 &\implies \\ a^{k(s-t)} = 1 = a^0. & \end{aligned}$$

We can use the division algorithm to write

$$k(s-t) = n \cdot (q-1) + r.$$

with $r \in \{0, 1, \ldots, q-2\}$. Hence we get by Lemma 2.75 that

$$a^r = a^{k(s-t)} = a^0.$$

But since a is primitive, the assignment

$$\{0, 1, \ldots, q-2\} \to F \colon i \mapsto a^i$$

is injective, and so we must have $r = 0$. In other words,

$$k(s-t) = n \cdot (q-1).$$

However, k and $(q-1)$ are coprime, hence it $q-1$ must divide $s-t$. That is,

$$s - t = n' \cdot (q-1).$$

In other words,

$$s = t \mod (q-1).$$

But note that $s, t \leq q-1$, so actually $s = t$. □

Theorem 2.76 Let F be a field of order q. Suppose that $a \in F$ is a primitive element. Let $k_1, k_2, \ldots, k_t$ be all of the integers in $\{0, 1, \ldots, q-1\}$ which are coprime to $q-1$. Then, the complete set of primitive elements in F is:

$$a^{k_1}, \ldots, a^{k_t}.$$

Proof. By assumption a is primitive, so all of the nonzero elements of F are

$$1, a^1, \ldots, a^{q-1}.$$

Each a^k above is primitive if and only if k is coprime to $q-1$ by Proposition 2.78. Hence, the statement follows. □

2.11 Diffie-Hellman Key Exchange Process

Let $a \in F$ be a primitive elemenot in a field of order q. Then, from the previous section we learned that there is a one-way function

$$\begin{aligned} \{0, 1, \ldots, q-2\} &\to \mathbb{F}_q - \{0\} \\ i &\mapsto a^i. \end{aligned}$$

In this section we will learn how to use this function to encode secret messages. The process of doing so is called the Diffie-Hellman Key Exchange Process.

Problem.

- Alice and Bob would like to communicate via an insecure network, so that messages can be read by an eavesdropper, Eve.
- To keep their messages private, Alice and Bob would like to encode them. But in order to agree on a coding system, they need to communicate via the network, so Eve will also know the coding system and will be able to easily decode the message.

Setup.

- Alice and Bob exchange a list of $q-1$ codes indexed by nonzero elements in a field F of order q (so this list is also available to Eve).
- In order to agree on a coding system, Alice and Bob need to secretly agree on a nonzero element $k \in F$, which is called a (secret) key .

Steps.

- Alice and Bob publicly agree on a primitive element $g \in F$ (so Eve also knows the value of g).
- Alice chooses a positive integer a and tells Bob (and Eve) the value of $A = g^a$.
- Bob chooses a positive integer b and tells Alice (and Eve) the value of $B = g^b$

- The secret key Alice and Bob will agree on is $k = g^{ab} \in F$.
- Alice finds the secret key by computing

$$B^a = (g^b)^a = g^{ab} = k.$$

- Likewise, Bob finds the secret key by computing

$$A^b = (g^a)^b = g^{ab} = k.$$

Alice and Bob have therefore agreed on a secret key, without telling Eve what it is.

Example 2.79. Alice and Bob have agreed on the primitive element $3 \in \mathbb{F}_{17}$. Alice chose the integer $a = 6$ and Bob sends Alice the value $B = 5$. Compute the key Alice and Bob have agreed on.

Example 2.80. Alice and Bob have agreed on the primitive element $3 \in \mathbb{F}_{17}$. Alice chose the integer $a = 6$ and Bob sends Alice the value $B = 5$. Compute the key Alice and Bob have agreed on.

Solution. The secret key is

$$g^{ab} = (g^b)^a = B^a = 5^6 \mod 17$$

We can compute this power in the following way.

$$\begin{aligned} 5^2 &= 25 = 8 \mod 17 \\ 5^3 &= 40 = 6 \mod 17 \\ 5^6 &= 6^2 = 2 \mod 17. \end{aligned}$$

Hence, $g^{ab} = 2$.

In summary:

Information involved	Known by Alice	Known by Bob	Known by Eve
F	✓	✓	✓
g	✓	✓	✓
a	✓	×	×
b	×	×	✓
g^a	✓	✓	✓
g^b	✓	✓	✓
g^{ab}	✓	✓	×

Q9 Why is hard for Eve to determine the secret key?

A: Eve needs to work out the value of g^{ab}, but the information which is publicly available to Eve are the values g, g^a, g^b.

To workout g^{ab}, Eve would have to workout the values of a or b from g^a or g^b. But this is hard to do since the function $a \mapsto g^a$ is a one-way function.

2.12 Roots of Unity

We learned how to encrypt messages by choosing primitive elements in finite fields. But we still have to answer the following question:

Q10 How to find primitive elements? Do they always exist?

To answer this question, we will introduce *roots of unity*.

Definition 2.81. Let n be a positive integer and let F be a field. Then, $a \in F$ is an *nth root of unity* if $a^n = 1$.

Example 2.82. a) $-1 \in \mathbb{R}$ is a 2nd root of unity since $(-1)^2 = 1$.

b) $e^{\frac{2\pi i}{3}} \in \mathbb{C}$ is a 3rd root of unity since

$$\left(e^{\frac{2\pi i}{3}}\right)^3 = e^{2\pi i} = 1.$$

c) $e^{\frac{2\pi i}{3}} \in \mathbb{C}$ is also a 6th root of unity since

$$\left(e^{\frac{2\pi i}{3}}\right)^6 = e^{4\pi i} = \left(e^{2\pi i}\right)^2.$$

d) Let F be a field of order q and let $a \in F$ be nonzero. From the generalisation of Fermat's theorem, then $a^{q-1} = 1$ in F. Hence, every nonzero element in F is a $(q-1)$th root of unity.

For example, in $\mathbb{F}_{13}$, $3^{12} = 1$. Hence, $3 \in \mathbb{F}_{13}$ is a 12th root of unity in $\mathbb{F}_{13}$.

Definition 2.83. Let n be a positive integer and let F be a field. Then, a nth root of unity $a \in F$ is *primitive* if $a^m \neq 1$ for all $0 < m < n$.

Example 2.84. $e^{\frac{2\pi i}{3}} \in \mathbb{C}$ is a primitive 3rd root of unity since:

$$\left(e^{\frac{2\pi i}{3}}\right)^1 = \frac{1}{2} + \frac{\sqrt{3}\cdot i}{2} \neq 1$$
$$\left(e^{\frac{2\pi i}{3}}\right)^2 = \left(e^{\frac{4\pi i}{3}}\right) = -\frac{1}{2} - \frac{\sqrt{3}\cdot i}{2} \neq 1.$$
$$\left(e^{\frac{2\pi i}{3}}\right)^3 = 1.$$

However, it is not a primitive 6th root of unity since $\left(e^{\frac{2\pi i}{3}}\right)^3 = 1$.

Example 2.85. Consider the field $\mathbb{F}_{17}$, and $2 \in \mathbb{F}_{17}$. By Fermat's theorem we know that $2^{16} = 1 \mod 17$, so 2 is a 16th root of unity in $\mathbb{F}_{17}$.

However, $2^8 = 1 \mod 17$, and so 2 is also an 8th root of unity. Hence, 2 is not a primitive 16th root of unity.

We can compute

$$\begin{aligned}
2^1 &= 2 \mod 17\\
2^2 &= 4 \mod 17\\
2^3 &= 8 \mod 17\\
2^4 &= 16 \mod 17\\
2^5 &= 15 \mod 17\\
2^6 &= 13 \mod 17\\
2^7 &= 9 \mod 17\\
2^8 &= 1 \mod 17
\end{aligned}$$

and check that 2 is a primitive 8th root of unity, since $2^m \neq 1$ for all $0 < m < 8$.

Example 2.86. Check by computing powers

$$\begin{aligned}
2, 2^2, \ldots, 2^{10} &\mod 13\\
3, 3^2, \ldots, 3^{15} &\mod 17
\end{aligned}$$

that:

a) $2 \in \mathbb{F}_{13}$ is a primitive 12th root of unity.

b) $3 \in \mathbb{F}_{17}$ is a primitive 16th root of unity.

Theorem 2.87. *For every prime q, there always exists a primitive $(q-1)$th root of unity in $\mathbb{F}_q$.*

2.12.1 Key Properties of Roots of Unity

Proposition 2.88. *Every nth root of unity is a primitive mth root of unity for some $m \leq n$.*

Proof. Suppose that $a \in F$ is an nth root of unity, then $a^n = 1$. Looking at the powers

$$a^1, a^2, \ldots, a^n$$

we can take the minimum m such that $a^m = 1$. Then, a will be a primitive mth root of unity. □

Example 2.89. Let's consider $5 \in \mathbb{F}_{11}$. By Fermat's theorem, we know that $5^{10} = 1$, so it is a 10th root of unity. Find m such that 5 is a primitive mth root of unity.

Solution. We can find m by computing powers of 5 until we reach the first m such that $5^m = 1 \mod 11$.

$$\begin{aligned}
5^1 &= 5 \mod 11\\
5^2 &= 3 \mod 11\\
5^3 &= 4 \mod 11\\
5^4 &= 9 \mod 11\\
5^5 &= 1 \mod 11.
\end{aligned}$$

Hence, of the indices

$$1, \ldots, 10$$

the minimum m such that $5^m = 1$ is $m = 5$. We can check by the computation above that $5 \in \mathbb{F}_{11}$ is a primitive 5th root of unity.

Proposition 2.90. *Let F be a field of order q. Let $a \in F$ be a primitive nth root of unity. Then, $a^i = a^j$ if and only if $i = j \mod n$.*

Proof. ($\implies$) Suppose that $a^i = a^j$.

① Since F is a field, we can divide both sides by a^j. This gives us that $\frac{a^i}{a^j} = 1$. That is,

$$a^{i-j} = 1.$$

② Using the division algorithm, we can write

$$i - j = k \cdot n + r$$

with $0 \leq r < n$. So,

$$1 = a^{i-j} = a^{k \cdot n} \cdot a^r = (\underbrace{a^n}_{=1})^k \cdot a^r = a^r.$$

since a is a nth root of unity

③ Now, $0 \leq r < n$.

Since a is a primitive nth root of unity then $a^r \neq 1$ if $0 < r < n$. So, it must be that $r = 0$. In other words,

$$i - j = k \cdot n \implies i = j \mod n.$$

($\impliedby$) Suppose that $i = j \mod n$. Then,

$$i - j = k \cdot n$$

so that

$$a^{i-j} = a^{k \cdot n} = (\underbrace{a^n}_{=1})^k = 1.$$

since a is a nth root of unity

Multiplying both sides of this equation by a^j gives

$$a^i = a^j.$$

□

2.13 Roots of Unity and Primitive Elements

We are finally ready to connect primitive roots of unity with primitive elements in a field F, and answer the question:

Q11 Do primitive elements always exist? How to find them?

Theorem 2.91. *In a field F of order q, the primitive elements are precisely the primitive $(q-1)$th primitive roots of unity.*

Proof. ① We first prove: Every primitive element in F is a primitive $(q-1)$th root of unity.

Assume that $a \in F$ is primitive. By (the generalisation of) Fermat's theorem, $a^{q-1} = 1$, and so a is a $(q-1)$th root of unity.

By definition of primitive element, we know that the powers

$$1, a, a^2, \ldots, a^{q-2}$$

are all distinct elements in F. Therefore, $a^m \neq 1$ for all $1 \leq m < q-1$. Hence, a is a primitive $(q-1)$th root of unity.

② Every primitive $(q-1)$th root of unity is a primitive element in F.

Suppose $a \in F$ is a primitive $(q-1)$th root of unity. Then, by Proposition 2.90,

$$1, a, a^2, \ldots, a^{q-1}$$

are all distinct and so a is a primitive element in F. □

The **key takeaways** from this theorem are:

- In a field F of order q we have:

  $$\{\text{primitive elements}\} = \{\text{primitive } (q-1)\text{th roots of unity}\}.$$

- By Theorem 1, $(q-1)$th roots of unity always exist in $\mathbb{F}_q$, so primitive elements always exist. This answers the first part of Q1.
- Finding primitive elements in F amounts to finding a primitive $(q-1)$th roots of unity.

The following theorem is our key tool for finding primitive nth roots of unity.

Theorem 2.92. *Let F be a field, and let $a \in F$ be an nth root of unity.*

Then, a is a primitive nth root of unity if and only if $a^{n/p} \neq 1$ for every prime factor p of n.

Proof. ($\Longrightarrow$) Suppose that a is a primitive nth root of unity. By definition, $a^m \neq 1$ for all $0 < m < n$.

Let p be a prime factor of n. Since $0 < n/p < n$, then $a^{n/p} \neq 1$.

($\Longleftarrow$) Assume that $a^{n/p} \neq 1$ for every prime factor p of n.

Since a is an nth root of unity by assumption, then, proposition 2.88 gives us that there is an $m \leq n$ such that a is a primitive mth root of unity.

This implies that

$$a^m = 1 = a^n.$$

Since a is a primitive mth root of unity, then proposition 2.90 tells us that

$$n = m = 0 \mod m.$$

In other words,

$$n = k \cdot m$$

with $k \geq 1$ (since we assumed m, n are both positive).

We have two cases to consider: $k = 1$ or $k > 1$.

① If $k = 1$, then $n = m$ and a is a primitive $m = n$th root of unity, as required.

② If $k > 1$, then it has at least one prime factor.

Let p be a prime factor of k. Then, p is a prime factor of n and

$$\frac{n}{p} = \frac{k}{p} \cdot m.$$

Hence,

$$a^{\frac{n}{p}} = a^{\frac{k}{p} \cdot m} = (\underbrace{a^m}_{=1})^{\frac{k}{p}} = 1$$

which is a contradiction, since we assumed that $a^{n/p} \neq 1$. Thus, the case $k > 1$ is impossible.

Therefore, the only option is $k = 1$, and we already know that in this case a is a primitive nth root of unity. □

Example 2.93. Show that

a) $5 \in \mathbb{F}_{23}$ is a primitive element.

b) $2 \in \mathbb{F}_{23}$ is not a primitive element,

Solution.

a) ① $\mathbb{F}_{23}$ is a field of order $q = 23$.

② By Theorem 2.91, $5 \in \mathbb{F}_{23}$ is a primitive element if and only if it is a primitive $(q-1) = 22$nd root of unity. So we need to check if 5 is a primitive 22nd root of unity.

③ Notice that $22 = 2 \cdot 11$, and the prime factors of 22 are 11 and 2.

By Theorem 2.92, 5 is a primitive 22nd root of unity if and only if

$$5^{22/2} = 5^{11} \neq 1$$
$$5^{22/11} = 5^2 \neq 1$$

in $\mathbb{F}_{23}$.

We can compute these powers in the following way.

$$5 = 5 \mod 23$$
$$5^2 = 25 = 2 \mod 23 \implies 5^2 \neq 1 \mod 23$$
$$5^4 = 2^2 = 4 \mod 23$$
$$5^8 = 4^2 = 16 = -7 \mod 23$$
$$5^{10} = 2 \cdot (-7) = -14 = 9 \mod 23$$
$$5^{11} = 5 \cdot 9 = 45 = -1 = 22 \mod 23 \implies 5^{11} \neq 1 \mod 23$$

and so 5 is a primitive 22nd root of unity $\implies$ it is a primitive element in $\mathbb{F}_{23}$.

b) Similar to a), $2 \in \mathbb{F}_{23}$ is a primitive element if and only if it is a primitive $(q-1) = 22$nd root of unity. Hence, we just need to show that 2 is not a primitive 22nd root of unity.

Notice that 2 is a primitive 22nd root of unity if and only if

$$2^{22/2} = 2^{11} \neq 1$$
$$2^{22/11} = 2^2 \neq 1$$

in $\mathbb{F}_{23}$.

We can compute 2^{11}:

$$\begin{aligned}
&2 = 2 \mod 23\\
&2^2 = 4 \mod 23\\
&2^4 = 16 = -7 \mod 23\\
&2^8 = (-7)^2 = 49 = 3 \mod 23\\
&2^{10} = 4 \cdot 3 = 12 \mod 23\\
&2^{11} = 2 \cdot 12 = 24 = 1 \mod 23.
\end{aligned}$$

Hence, 2 is not a primitive 22nd root of unity $\implies$ it is not a primitive element in $\mathbb{F}_{23}$.

Example 2.94. a) Show that 11 is a primitive element in $\mathbb{F}_{13}$.

b) What are all of the primitive elements in $\mathbb{F}_{13}$.

Solution.

a) ① $\mathbb{F}_{13}$ is a field of order $q = 13$.

② By Theorem 2.91, $11 \in \mathbb{F}_{13}$ is a primitive element if and only if it is a primitive $(q-1) = 12$th root of unity. So we just need to check if 11 is a primitive 12th root of unity.

③ Notice that $12 = 3 \cdot 2^2$, and the prime factors of 12 are 2 and 3.

By Theorem 2.92, 11 is a primitive 12th root of unity if and only if

$$11^{12/2} = 11^6 \neq 1$$
$$11^{12/3} = 11^4 \neq 1$$

in $\mathbb{F}_{13}$.

We can compute these powers in the following way.

$$\begin{aligned}
&11 = 11 = -2 \mod 13\\
&11^2 = 4 \mod 13\\
&11^4 = 4^2 = 16 = 3 \mod 13 \implies 11^4 \neq 1 \mod 13\\
&11^3 = 5 \mod 13\\
&11^6 = 11^2 \cdot 11^4 = 4 \cdot 3 = 12 \mod 13 \implies 11^6 \neq 1 \mod 13.
\end{aligned}$$

and so 11 is a primitive 12th root of unity $\implies$ it is a primitive element in $\mathbb{F}_{13}$.

b) To compute all of the primitive elements in $\mathbb{F}_{13}$, we use Theorem 2.76.

① The integers in the set $\{0, 1, \ldots, q-1 = 12\}$ which are coprime to $q - 1 = 12$ are: $1, 5, 7, 11$.

Hence, the complete set of primitive elements in $\mathbb{F}_{13}$ is:

$$11^1, 11^5, 11^7, 11^{11} \mod 13.$$

We can compute these in the following way:

$$\begin{aligned}
11^2 &= 4 \mod 13 \\
11^4 &= 3 \mod 13 \\
11^5 &= 11 \cdot 3 = 33 = 7 \mod 13 \\
11^7 &= 11^2 \cdot 11^5 = 4 \cdot 7 = 28 = 2 \mod 13 \\
11^{11} &= 11^4 \cdot 11^7 = 3 \cdot 2 = 6 \mod 13.
\end{aligned}$$

Hence, the primitive elements in $\mathbb{F}_{13}$ are

$$11, 7, 2, 6.$$