

# Combinatorics

Jacob Green  
Department of Mathematical Sciences, The University of Bath

November 11, 2024

## Abstract

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

**Keywords:** Combinatorics, Probability

## Preface

### Notation

- $\mathbb{N} = \{1, 2, \dots\}$  and  $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
- $[n] = \{1, \dots, n\}$
- if  $a$  is defined to be  $b$  we may say  $a := b$  (but I will often forget)
- $A^k = \overbrace{A \times \dots \times A}^{k \text{ times}}$  for a set  $A$ ,  $\times$  being the Cartesian product.

# Contents

<b>1</b>	<b>Elementary Combinatorics</b>	<b>3</b>
1.1	Fundamental Principles . . . . .	3
1.2	Binomial Coefficients . . . . .	7
1.3	The Pigeonhole Principle . . . . .	9
1.4	The Principle of Inclusion-Exclusion . . . . .	11
1.5	Generating Functions . . . . .	13
1.6	Miscellaneous Topics . . . . .	14
1.7	Additional Problems . . . . .	15
<b>2</b>	<b>The Probabilistic Method</b>	<b>16</b>
2.1	Introducing the Probabilistic Method with Ramsey Bounds . . . . .	16
2.2	Linearity of Expectation . . . . .	17
2.3	Alteration . . . . .	18
2.4	Lovász Local Lemma . . . . .	19
<b>3</b>	<b>Solutions</b>	<b>20</b>

# 1 Elementary Combinatorics

In combinatorics we are concerned with counting the number of objects from a collection. For example, we may count the positive integers divisible by 3 that are less than 1000. Here the objects are positive integers are the objects and the collection is those objects that are both divisible by 3 and less than 1000.

As a set is just a collection of objects, we will often phrase things set theoretically.

## 1.1 Fundamental Principles

To begin counting anything interesting, we'll need the following principles. The first two let us count things inductively (e.g. counting the number of wines by counting in threes or counting the number of wine & cheese pairings by counting the wines and the cheeses). The final simply says it doesn't matter what order we count each element (e.g. wine) in. These are essentially common sense principles, and you have certainly used these in your day to day life. Regardless, I will prove these. That way these notes are built on a rigorous set theoretic basis.

### Theorem 1.1 (addition principle)

Let  $n \in \mathbb{N}$ . Let  $A_1, \dots, A_n$  be finite sets. One has<sup>a</sup>

$$A_1, \dots, A_n \text{ disjoint} \implies |A_1 \cup \dots \cup A_n| = |A_1| + \dots + |A_n|$$

<sup>a</sup> $A_1, \dots, A_n$  are said to be disjoint if  $\cap_{i=1}^n A_i = \emptyset$

To prove this, we simply count both sides one term at a time.

*Proof.* Let  $x \in \cup_{i=1}^n A_i$ . Then  $x \in A_i$  for exactly one  $1 \leq i \leq n$  and hence

$$|A_1| + \dots + |A_n| = \sum_{x \in A_1} 1 + \dots + \sum_{x \in A_n} 1 = \sum_{x \in \cup_{i=1}^n A_i} 1 = |\cup_{i=1}^n A_i|$$

by counting both sides term by term. □

### Theorem 1.2 (multiplication principle)

Let  $n \in \mathbb{N}$ . Let  $A_1, \dots, A_n$  be finite sets. One has

$$|A_1 \times \dots \times A_n| = |A_1| \times \dots \times |A_n|$$

This time we count terms in each slot recursively.

*Proof.* Consider an arbitrary element  $x = (x_1, \dots, x_n) \in A_1 \times \dots \times A_n$  and let  $1 \leq i \leq n$ . Then fixing  $x_j, j \neq i$  we have  $|A_i|$  possible choices for  $x_i$ . Hence, we have

$$|A_1 \times \dots \times A_n| = \sum_{i=1}^n \sum_{x \in A_i} |\cap_{j \neq i} A_j| = \sum_{i=1}^n |A_i| \sum_{x \in A_i} |\cap_{j \neq i} A_j| = \dots = |A_1| \times \dots \times |A_n|$$

by repeated application of this reasoning. □

### Theorem 1.3 (bijection principle)

Let  $A$  and  $B$  be sets. If there is a bijection<sup>a</sup>  $\pi : A \rightarrow B$  then  $|A| = |B|$

<sup>a</sup>A bijection is a one-to-one mapping

*Proof.* This is a truism. □

The addition principle can be thought of as emptying two containers of  $n$  and  $m$  wine bottles and containing how many bottles you have in total ( $n + m$ ), whereas the multiplication principle can be thought of as counting the number of ways of pairing  $b$  boys with  $g$  girls. The bijection principle says if we take  $s$  students and select them one by one at random,  $t$  times, we'll always have selected  $t$  students. We will often look for such interpretations in combinatorics.

With just these principles, we can count all the following quantities.

**Problem 1.1 ( $k$ -words with repetitions)**

How many words length  $k$  can be formed from an alphabet with  $n$  letters.

*Solution.* To count the number of words with repetitions allowed, we sample with replacement to get

$$\underbrace{n \times \cdots \times n}_{k \text{ times}} = n^k$$

$k$ -words (or  $k$ -sequences or  $k$ -tuples) on  $n$  symbols by the multiplication principle. □

**Problem 1.2 ( $k$ -words without repetitions)**

How many words length  $k$  with distinct letters can be formed from an alphabet with  $n$  letters.

*Solution.* For  $k$ -words without repetition, we sample without replacement for each letter to get

$$n \times (n - 1) \times \cdots \times (n - k + 1) =: n^{\underline{k}}$$

$k$ -words without repetition on  $n$  symbols by the multiplication principle.<sup>1</sup> □

Note a word is just a  $k$ -tuple of letters. Often times we will be able to phrase new objects in terms of the old and we care a great deal about doing so. Learning combinatorics is quite different to other fields of mathematics. Often, say in analysis, there will be a classic style of proof which will build the core results. Then we may use these core results, in conjunction with some manipulation, to prove new results. Then these new results to prove others and so on so forth, building a great theory of analysis. In combinatorics, often times the proof of a new result will be entirely novel, depending on little known theory (outside of what an undergraduate may have encountered) but will rely on a great onslaught of techniques, applied in a creative manner. Learning combinatorics is not learning definitions, lemmas, theorems and piecing them all together to prove related results. Instead it is learning to apply, and more importantly spot ways of applying, core techniques to novel problems.

If we were to consider words of length  $n$  on  $n$  symbols without repetition, then we would be *permuting* (i.e. reordering/relabelling) the  $n$  symbols. Hence we have  $n \times (n - 1) \times \cdots \times 1 =: n!$  *permutations* on  $n$  symbols. Using this notation we have  $n^{\underline{k}} = n!/(n - k)!$ .

Suppose we wish to count the number of subsets length 2 on  $n$  symbols. We would have  $n(n - 1)$  ways of choosing 2 unique elements (i.e. 2-words without repetition), but we have counted the reorderings and hence overcounted by doing this. We know, by the multiplication principle, that the number of reorderings times the number of ways to select two unique elements will be  $n(n - 1)$ , hence as there's  $2! = 2$  ways to order 2 symbols (as chosen or reversed) we have  $\frac{1}{2}n(n - 1)$  subsets size 2 of  $[n]$ . We extend this logic to count  $k$ -subsets.

**Problem 1.3 ( $k$ -subsets)**

How many subsets size  $k$  are there of a set size  $n$ ?

---

<sup>1</sup>We call  $n^{\underline{k}}$  the falling factorial of  $n$

*Solution.* Let  $x$  be the desired quantity. For each subset size  $k$ , we may reorder its elements in  $k!$  ways and we may select  $k$  unique elements by counting  $k$ -words on  $n$  symbols without repetition, thus

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

and dividing by  $k!$  gives  $x = n!/k!(n-k)! =: \binom{n}{k}$  □

We call  $\binom{n}{k}$  the *binomial coefficient*, and would say this as “ $n$  choose  $k$ ” (as this counts the ways of choosing  $k$  things from  $n$  things). We will dedicate an entire section (in fact, next section) to these.

In this next problem we will first encounter the idea of “stars and bars” counting, which gives us a way of counting the ways to group  $n$  indistinguishable objects into  $k$  groups. This has many novel uses, like the one we’re about to encounter.

#### Problem 1.4 ( $k$ -multisubsets)

How many multisubsets<sup>a</sup> of size  $k$  are there in a set of  $n$  objects?

<sup>a</sup>a multiset is a set that allows repetition, see <https://en.wikipedia.org/wiki/Multiset>

*Solution.* Let  $X = \{x_1, \dots, x_n\}$ . We call the number of times  $x_i, 1 \leq i \leq n$  appears in a multisubset of  $X$  the *multiplicity* of  $x_i$ . We know that the size of a multiset is the sum of its multiplicities, thus it suffices to count solutions  $(\ell_1, \dots, \ell_n)$  of nonnegative integers to

$$\ell_1 + \dots + \ell_n = k$$

which by setting  $\ell'_i := \ell_i + 1$  is the same as counting positive integer solutions to

$$\ell'_1 + \dots + \ell'_n = k + n$$

Now write this as

$$\underbrace{1 + \dots + 1}_{\ell'_1 \text{ times}} + \dots + \underbrace{1 + \dots + 1}_{\ell'_n \text{ times}} = k + n$$

We are tasked with dividing up the  $k + n$  ones into  $n$  groups, which can be done by inserting  $n - 1$  stars in between two ones (not the ends as we require  $n$  nonempty collections of ones) to signify the beginning of a new group. This gives  $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$  possibilities. □

#### Problem 1.5 ( $k$ -partitions with a given sizing)

How many ways are there to divide a set partition a set  $X$  of size  $n$  into sets  $X_1, \dots, X_k$  with size  $n_1, \dots, n_k$  respectively (where  $n_1 + \dots + n_k = n$ )?

*Solution.* There are

$$\binom{n - n_1 - \dots - n_{i-1}}{n_i}$$

ways of choosing the  $X_i$  once  $X_1, \dots, X_{i-1}$  have been chosen, and

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

So all together one obtains

$$\binom{n}{n_1} \binom{n-n_1}{n_2} \dots \binom{n-(n_1+\dots+n_{k-1})}{n_k} = \frac{n!}{n_1! \dots n_k!} =: \binom{n}{n_1, \dots, n_k}$$

such partitions.<sup>2</sup> □

<sup>2</sup>The quantity  $\binom{n}{n_1, \dots, n_k}$  is called the multinomial coefficient

## Exercises

### Exercise 1.1

In how many ways can  $n$  people be seated at a circular table with  $n$  seats, where we do not classify between seatings that can be obtained from one another by rotating the table?

### Exercise 1.2

How many subsets are there of the set  $\{1, 2, \dots, n\} =: [n]$ ? How many are of even size?

### Exercise 1.3

There are  $2n$  people at a party. How many ways can the  $2n$  people split into  $n$  pairs?

### Exercise 1.4

A robot is placed on the bottom left of an  $n \times n$  chessboard. The robot has two moves, go vertically up one square or horizontally along (to the right) one square. How many sequences of moves can the robot make to get to the top right square?

## 1.2 Binomial Coefficients

### Lemma 1.1 (addition formula)

Let  $n \in \mathbb{N}$  and  $1 \leq k \leq n$ . The identity

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

holds.

*Proof 1.* A simple algebraic verification works, I leave this to the reader.  $\square$

We can also prove this identity with the technique of “double counting”. Intuitively, this is just saying that if we can count things in two ways they must be equal. For example, if we had an  $n \times n$  grid full of numbers, we could count the sum of all the numbers by summing along the rows or the columns. For certain selections of numbers, this can yield interesting equalities.

*Proof 2.* We count the  $k$ -subsets of  $[n]$  in two ways. First, all at once, getting  $\binom{n}{k}$  such sets. Secondly, by considering separately the cases when 1 is in our subset and isn't. This gives  $\binom{n-1}{k-1}$  choices with 1 and  $\binom{n-1}{k}$  choices without, giving us the desired equality.  $\square$

### Theorem 1.4 (binomial theorem)

For all integers  $n \geq 0$  and  $x, y \in \mathbb{C}$ , one has

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

*Proof 1.* We first use a straight forward induction argument. Observe, assuming the hypothesis for some  $n \geq 0$  (and noting it trivially holds for  $n = 0$ ),

$$\begin{aligned} (x + y)^{n+1} &= (x + y)(x + y)^n \\ &= (x + y) \sum_{k=0}^n \binom{n}{k} x^k y^{n-k} \\ &= \sum_{k=0}^n \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^n \binom{n}{k} x^k y^{n-k+1} \\ &= \sum_{k=0}^{n+1} \left( \binom{n}{k-1} + \binom{n}{k} \right) x^k y^{n-k+1} \quad (\dagger) \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{(n+1)-k} \end{aligned}$$

where  $(\dagger)$  follows from an index shift ( $k \rightarrow k-1$ ) and defining  $\binom{n}{k} := 0$  for  $k > n$  or  $k < 0$ .  $\square$

As before, we can double count ourselves a proof of this theorem.

*Proof 2.* Consider the coefficient of  $x^k y^{n-k}$  of

$$(x + y)^n = \overbrace{(x + y) \cdots (x + y)}^{n \text{ times}}$$

When computing this expansion, we are multiplying exactly one of  $x$  or  $y$  from each  $(x + y)$  term on the RHS. Our entire expansion will be the sum of all such choices. Thus, to compute the coefficient of  $x^k y^{n-k}$  in  $(x + y)^n$ , it suffices to count the number of ways to choose exactly  $k$   $x$ s out the  $n$  possible choices. This is clearly  $\binom{n}{k}$  and hence the result follows.  $\square$



As an immediate corollary we have the following.

**Corollary 1.1 (sum and alternating sum of binomial coefficients)**

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad \text{and} \quad \sum_{k=0}^n (-1)^k \binom{n}{k} = 0$$

*Proof 1.* Take  $x = y = 1$  and  $x = 1, y = -1$  in the Binomial Theorem.  $\square$

We may also take a more combinatorial approach to proving these identities.

*Proof 2.* There are  $2^n$  subsets of  $[n]$  by counting directly (see exercise 1.2) and by counting each of the subsets size  $k$  in groups we get  $\sum_{k=0}^n \binom{n}{k}$ , giving the first equivalence. For the second, note there are an equal number of odd and even subsets of  $[n]$  (also exercise 1.2) so we have

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = \sum_{k=0}^n \sum_{k=0,2|k}^n \binom{n}{k} - \sum_{k=0,2 \nmid k}^n \binom{n}{k} = 0$$

giving the latter equivalence.  $\square$

Let us recall the following lemma from (elementary) complex analysis, concerning sums of powers of roots of unity. If you are not yet familiar with these tools please skip the next lemma and problem.

**Lemma 1.2 (sums of powers of roots of unity)**

Let  $1, \xi_1, \dots, \xi_{n-1}$  be the  $n$ -roots of unity, that is the solutions to  $z^n = 1, z \in \mathbb{C}$ . Then, one has

$$1 + \sum_{j=1}^{n-1} \xi_j^\ell = \begin{cases} n : \ell \equiv 0 \pmod{n} \\ 0 : \ell \not\equiv 0 \pmod{n} \end{cases}$$

*Proof.* Write  $\xi_j = \exp(2\pi i j/n)$ . If  $\ell = mn, m \in \mathbb{Z}$ , then  $\xi_j^\ell = \exp(2\pi i m) = 1$  and hence

$$1 + \sum_{j=1}^{n-1} \xi_j^\ell = n$$

Conversely, if  $\ell = mn + r, m \in \mathbb{Z}, 0 < r < n$  then  $\xi_j^\ell = \exp(2\pi i(mn + r)j/n) = \exp(2\pi i r j/n)$  and

$$1 + \sum_{j=1}^{n-1} \xi_j^\ell = \sum_{j=0}^{n-1} (\exp(2\pi i r/n))^j = \frac{1 - \exp(2\pi i r)}{1 - \exp(2\pi i r/n)} = 0$$

where we used the standard result for the sum of a geometric series in equality 2.  $\square$

With this, we can prove the following result. Generalising further the previous problem.

**Problem 1.6 (sums of binomial multiples)**

Compute the following quantity.

$$\sum_{k=0}^n \binom{mn}{mk}$$

*Solution.* Let  $\xi_0, \dots, \xi_{m-1}$  be the  $m^{\text{th}}$  roots of unity, with  $\xi_0 = 1$ . Then, by our previous lemma and the Binomial theorem, we can deduce

$$\sum_{k=0}^n \binom{mn}{mk} = \sum_{k=0}^{mk} \binom{nm}{k} \left( \frac{1}{m} \sum_{\ell=0}^{m-1} \xi_\ell^k \right) = \frac{1}{m} \sum_{\ell=0}^{m-1} \sum_{k=0}^{mn} \binom{mn}{k} \xi_\ell^k = \frac{1}{m} \sum_{\ell=0}^{m-1} (1 + \xi_\ell)^{mn}$$

The term of the RHS can be further simplified, I elect to leave it here.  $\square$

THINGS TO ADD:

- VANDERMONDE'S
- HOCKEYSTICK LEMMA

**Proposition 1.1 (Vandermonde's Identity)**

Fix  $n, a, b, \in \mathbb{N}$ . Then

$$\sum_{k=0}^n \binom{a}{k} \binom{b}{n-k} = \binom{a+b}{n}$$

As at this point you'd expect, we have two proofs. One algebraic, one via double counting. The motivation for this first proof comes from the fact we are taking a sum of the form  $\sum_{k=0}^n a_k b_{n-k}$ , which should remind us of the multiplication of polynomials.

*Proof 1.* □

A nice way to think about this double counting proof is to count the ways of forming a committee of  $n$  people from  $a$  boys and  $b$  girls, choosing  $k$  boys at a time.

*Proof 2.* We count the number of ways to choose subsets size  $n$  from  $[a+b]$  in two ways. The first, directly, gives  $\binom{a+b}{n}$  choices. The second, is by counting the number of ways to choose such a subset with exactly  $0 \leq k \leq n$  elements in  $[a]$ . We have  $\binom{a}{k}$  ways of choosing the  $k$  elements in  $[a]$ , and  $\binom{b}{n-k}$  ways of choosing the remaining  $n-k$  elements from  $[a+b] \setminus [a]$ . Thus, summing over  $0 \leq k \leq n$  we obtain the desired equality. □

## Exercises

**Exercise 1.5**

How many words length  $n$  can be formed from an alphabet of  $\ell$  letters  $\mathcal{A} = \{A_1, \dots, A_\ell\}$  such that the first letter  $A_1$  occurs an even number of times?

## 1.3 The Pigeonhole Principle

If I have 5 pigeons and 4 containers, each only able to fit one pigeon, can I fit all the pigeons into my containers? Of course not! It turns out this common-sense principle allows us to discover many, many, combinatorial facts...

**Theorem 1.5 (pigeonhole principle)**

Given a set  $X$  of size  $n$ , any partition of  $X$  into  $m < n$  subsets  $X_1, \dots, X_m$  must have at least one  $X_i$  with  $|X_i| > 1$ .

We prove this with the following simple contradiction.

*Proof.* Suppose each  $|X_i| \leq 1$ , then  $|X| = |\cup_{i=1}^m X_i| = \sum_{i=1}^m |X_i| \leq m < n$ . Absurd! □

We can slightly better than this. What if my containers can fit 2 pigeons and I only have 2 this time. Then I still can't fit my pigeons into my containers. Formally,

**Theorem 1.6 (full pigeonhole principle)**

Given a set  $X$  of size  $n = km + 1$ , any partition of  $X$  into  $m$  subsets  $X_1, \dots, X_m$  must have at least one  $X_i$  with  $|X_i| > k$ .

Another simple, almost identical, contradiction will kill this.

*Proof.* Suppose each  $|X_i| \leq k$ , then  $|X| = |\cup_{i=1}^m X_i| = \sum_{i=1}^m |X_i| \leq km < n$ . Absurd! □

We also have a infinite pigeonhole principle. If I can only fit a finite number of pigeons into each container then, assuming I only have finitely many containers, I cannot fit an infinite number of pigeons into my containers.

**Theorem 1.7 (infinite pigeonhole principle)**

Given a set  $X$  of infinite cardinality, any partition of  $X$  into finitely many sets  $X_1, \dots, X_m$  must have some  $X_i$  also of infinite cardinality.

Again, a simple contradiction will prove this.

*Proof.* Suppose each  $|X_i| = n_i < \infty$ . Then  $|X| = |\cup_i^m X_i| = \sum_{i=1}^m |X_i| = \prod_{i=1}^m n_i < \infty$ . Absurd!  $\square$

**Problem 1.7 (monotone subsequences)**

How large must a sequence of distinct real numbers be to guarantee the existence of a monotone subsequence size  $n + 1$ ,  $n \in \mathbb{N}$ ?

*Solution.*  $\square$

**Exercises**

## 1.4 The Principle of Inclusion-Exclusion

It is often much easier to count how many objects have properties  $A$  AND  $B$  than  $A$  OR  $B$ . Thankfully we have the following principle to relate the two.

### Proposition 1.2 (2 variable inclusion exclusion principle)

Let  $A$  and  $B$  be finite sets. Then,

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

For an intuitive argument, just draw a venn diagram. To find the count  $|A \cup B|$  we can count the entire circles of  $A$  and  $B$  individually, but when doing this we count the  $A \cap B$  section twice so we must subtract off one lot of it.

We prove this by showing for each  $x \in A \cup B$ ,  $x$  is counted exactly once in the RHS.

*Proof.* Write  $|A \cup B| = \sum_{x \in A \cup B} 1$ . WLOG take  $x \in A$ , then either  $x \in B$  or  $x \notin B$ . In the former case,  $x \in A \cap B$  gives a count of exactly 1 on the RHS for  $x$  and in the latter case  $x \notin A \cap B$  affirms the same result. Hence  $|A| + |B| - |A \cap B| = \sum_{x \in A \cup B} 1 = |A \cup B|$ .  $\square$

It turns out this property can be generalised for  $n$  finite sets.

### Theorem 1.8 (inclusion exclusion principle)

Let  $n \in \mathbb{N}$  and  $A_1, \dots, A_n$  be finite sets. Then,

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\ell=1}^n (-1)^{\ell-1} \sum_{I \subseteq [n], |I|=\ell} \left| \bigcap_{i \in I} A_i \right|$$

We have two proofs for this. A bashy induction will work, but there is also a clever little trick we can do with indicator functions.

*Proof 1.* We work via induction.  $\square$

*Proof 2.* Suppose (reasonably) that all of our subsets lie in some space  $\Omega$  and denote  $A^c := \Omega \setminus A$  for  $A \subseteq \Omega$ . Then,

$$\mathbf{1} \left[ \bigcup_{i=1}^n A_i \right] = \mathbf{1} \left[ \left( \bigcap_{i=1}^n A_i^c \right)^c \right] = 1 - \mathbf{1} \left[ \bigcap_{i=1}^n A_i^c \right] = 1 - \prod_{i=1}^n (1 - \mathbf{1}[A_i])$$

Where  $\mathbf{1}[A] = 1$  if  $x \in A$  and 0 elsewhere (we call this the indicator function). Now, expanding the product we see

$$\mathbf{1} \left[ \bigcup_{i=1}^n A_i \right] = \sum_{\ell=1}^n \sum_{I \subseteq [n], |I|=\ell} \prod_{i \in I} (-\mathbf{1}[A_i])$$

which, summing both sides over  $x \in \Omega$ , gives the result.  $\square$

Recall (see any elementary number theory text) that for primes  $p, q$  and  $n \in \mathbb{N}$ , one has  $p, q \mid n \Leftrightarrow pq \mid n$ . Thus, it is easy to count how many naturals below  $n$  are divisible by  $p$  and  $q$  (simply those divisible by  $pq$ ), and by the inclusion exclusion principle it must also be easy to count how many naturals below  $n$  are divisible by  $p$  or  $q$ .

Recall (again, see any elementary number theory text) that *Euler's totient function*  $\phi : \mathbb{N} \rightarrow \mathbb{N}$  has  $\phi(n) = |\{1 \leq i \leq n : \gcd(i, n) = 1\}|$ . That is,  $\phi$  counts the number of integers at most  $n$  which are coprime to  $n$ . We will count this quantity directly, working with the reasoning outlined above.

**Proposition 1.3 (explicit form of Euler's  $\phi$ -function)**

Let  $n \in \mathbb{N}$ . Then, letting  $\phi$  be Euler's totient function,

$$\phi(n) = n \prod_{\substack{p|n, \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

*Proof.* Factorise  $n = p_1^{\ell_1} \cdots p_k^{\ell_k}$  into primes. Then we have  $1 \leq x \leq n$  coprime to  $n$  if and only if  $p_1, \dots, p_k \nmid x$ . Define  $A_p := \{1 \leq x \leq n : p \mid x\} \subseteq [n]$ . By the inclusion exclusion principle we may compute, where compliments are taken with respect to  $[n]$ ,

$$\phi(n) = \left| \bigcap_{i=1}^k A_{p_i}^c \right| = n - \left| \bigcup_{i=1}^k A_{p_i} \right| \quad (1)$$

$$= n - \sum_{m=1}^k (-1)^{m-1} \sum_{I \subseteq [k], |I|=m} \left| \bigcap_{i \in I} A_{p_i} \right| \quad (2)$$

$$= n - \sum_{m=1}^k (-1)^{m-1} \sum_{I \subseteq [k], |I|=m} \frac{n}{\prod_{i \in I} p_i} \quad (3)$$

$$= n \sum_{m=0}^k (-1)^m \sum_{I \subseteq [k], |I|=m} \frac{1}{\prod_{i \in I} p_i} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Where in (1) we used DeMorgan's laws, (2) the inclusion exclusion principle and in (3) the fact that  $|\cap_{p \in P} A_p| = n / \prod_{p \in P} p$  when  $p \in P$  are primes dividing  $n$  (easily seen with  $pq \mid n \Leftrightarrow p, q \mid n$ ).  $\square$

We can also use the inclusion exclusion principles to count the number of permutations of  $[n]$  with no fixed point, the so called *dearrangements* of  $[n]$ . A fixed point of a permutation  $\pi : [n] \rightarrow [n]$  is simply an  $x \in [n]$  with  $\pi(x) = x$ .

**Proposition 1.4 (dearrangements)**

The number of permutations of  $[n]$  with no fixed point is

$$n! \sum_{k=0}^n \frac{(-1)^k}{k!}$$

*Proof.* This is another direct application of the inclusion exclusion principle. Let  $A_i$  be the set of permutations on  $[n]$  with  $i$  a fixed point. Then we compute

$$\left| \bigcap_{i=1}^n A_i^c \right| = n! - \left| \bigcup_{i=1}^n A_i \right| = n! - \sum_{k=1}^n \sum_{I \subseteq [n], |I|=k} \left| \bigcap_{i \in I} A_i \right| = n! - \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} (n-k)! = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$$

using the fact there are  $\binom{n}{k}$  subsets  $I \subseteq [n]$  of size  $k$  and  $(n-k)!$  permutations with  $k$  elements fixed.  $\square$

If we take the limit  $n \rightarrow \infty$ , we see that the probability of a (uniformly) random permutation of  $[n]$  having no fixed points tends to  $1/e$ .

## 1.5 Generating Functions

### Exercises

## 1.6 Miscellaneous Topics

### Exercises

## 1.7 Additional Problems



## **2 The Probabilistic Method**

### **2.1 Introducing the Probabilistic Method with Ramsey Bounds**

#### **Exercises**

## 2.2 Linearity of Expectation

### Exercises

## 2.3 Alteration

### Exercises

## 2.4 Lovas  Local Lemma

### Exercises

### 3 Solutions

Here I list the exercise solutions in a random order. I will store which exercises have a solution in the README of this repository.