Summations

Evan Chen

October 13, 2016

> Mathematicians just love sigma notation for two reasons. First, it provides a convenient way to express a long or even infinite series. But even more important, it looks really cool and scary, which frightens nonmathematicians into revering mathematicians and paying them more money.
>
> — *Calculus II for Dummies*

Acknowledgments

Thanks to Zack Chroman, Michael Diao, Steven Hao, Ryan Kim, Kevin Qian, Colin Tang, Michael Tang, Tyler Zhu, for helpful suggestions and comments.

Contents

§1 Introduction

This is a handout about how to deal with complicated sums. Broadly, sums on olympiad contests fall into a few different categories:

- Purely **algebraic** sums, like $\sum_n \frac{1}{n(n+1)}$, which are mostly exercise in algebraic manipulation. These are the kind you would get in a lecture named "sums and products".
- Sums which are **combinatorial**, involving expressions like $\binom{n}{k}$. You would see this in lectures named "combinatorial sums" and "counting in two ways", or perhaps "generating functions".
- Sums which are **number theoretic**, involving functions like φ, μ, or which involve expressions like $\sum_{d|n}$, or which ask you to take a sum modulo p. Often appears in "multiplicative number theory".

I think it is preferable to avoid separating the learning of these apparently disjoint topics, hence the unified handout. There are some connected themes which underlie all three; in particular, one of the big ideas which runs through the entire handout is the concept of **swapping the order of summation**.

Theorem 1.1 (Swapping the order of summation)
Let $f(a,b)$ be a function. Then

$$\sum_{a\in A}\sum_{b\in B} f = \sum_{b\in B}\sum_{a\in A} f.$$

This seemingly obvious fact is a nontrivial step in more than 50% of summation problems (in the same way that cyclic quadrilaterals is used in more than 50% of geometry problems). We will see this key idea again and again in the examples that follow. Thus **any time you see a double sum**, you should always consider computing the sum in the reversed order. In fact, even if you only have a single $\sum$ you should consider rewriting the expression as a double sum (e.g. a generating function) so that the above theorem applies. You might also need to change the variables before this step; for example we also have

$$\sum_{a\geq 0}\sum_{b\geq 0} f = \sum_{k\geq 0}\sum_{\substack{a,b\\ a+b=k}} f.$$

§2 Algebraic manipulation

These are the most low-tech problems, and often appear on short-answer contests as a result. These techniques apply to all sums, and especially to those which don't have N or C flavor.

Examples of things you can do:

- Look at **telescoping sequences**. The classic example that everyone knows of is

$$\sum_{n=1}^{100} \frac{1}{n(n+1)}.$$

- Generalizing the above point, looking at **partial fractions** is very often a good thing to do if your expression has polynomial denominators.
- Try to **factor the expression**. In particular, one can factor through double sums:

$$\sum_{a\in A}\sum_{b\in B} a^2(b+1) = \left(\sum_{a\in A} a^2\right)\left(\sum_{b\in B}(b+1)\right).$$

- Try **swapping the order of summation**. (This is so important we're saying it again.)

§2.1 Telescoping and partial fractions

I won't provide too many examples here (though there are plenty in the practice problems!) since this is a topic that often appears at the AIME level anyways. So here is my token example.

Example 2.1 (Stanford 2011)
Evaluate the sum

$$\sum_{n\geq 1} \frac{7n+32}{n(n+2)} \cdot \left(\frac{3}{4}\right)^n.$$

Solution. Again, since we have a polynomial denominator, our first reflex is to decompose its partial fractions. This gives us

$$\frac{7n+32}{n(n+2)} = \frac{16}{n} - \frac{9}{n+2}.$$

Suddenly we're done, because the sum telescopes according to the fact that $9 = (3/4)^2 \cdot 16$:

$$\sum_{n\geq 1} \frac{16}{n}\left(\frac{3}{4}\right)^n - \frac{16}{n+2}\left(\frac{3}{4}\right)^{n+2}.$$

We see the trailing terms in the sum tend to zero as $n \to \infty$. So the answer is $\frac{16}{1}\cdot\frac{3}{4} + \frac{16}{2}\cdot\frac{9}{16} = 12 + \frac{9}{2} = \frac{33}{2}$. □

§2.2 Swapping the order of summation

For a less contrived example, we now prove linearity of expectation, which is the key result from [2].

The motivating example which I always present is that this allows one to compute the expected number of fixed points in a random permutation of $\{1, \dots, n\}$:

Example 2.2
A random permutation of $\{1, \dots, n\}$ has an average of one fixed point.

To see this, let's look at the case $n = 4$:

	W	X	Y	Z	Σ
1	**W**	**X**	**Y**	**Z**	4
2	**W**	**X**	Z	Y	2
3	**W**	Y	X	**Z**	2
4	**W**	Y	Z	X	1
5	**W**	Z	X	Y	1
6	**W**	Z	**Y**	X	2
7	X	W	**Y**	**Z**	2
8	X	W	Z	Y	0
9	X	Y	W	**Z**	1
10	X	Y	Z	W	0
11	X	Z	W	Y	0
12	X	Z	**Y**	W	1
13	Y	W	X	**Z**	1
14	Y	W	Z	X	0
15	Y	**X**	W	**Z**	2
16	Y	**X**	Z	W	1
17	Y	Z	W	X	0
18	Y	Z	X	W	0
19	Z	W	X	Y	0
20	Z	W	**Y**	X	1
21	Z	**X**	W	Y	1
22	Z	**X**	**Y**	W	2
23	Z	Y	W	X	0
24	Z	Y	X	W	0
Σ	6	6	6	6	24

The idea is as follows: nominally, to compute the expected value, one is supposed to compute the number of fixed points in each row, and then take the average. However, the number of fixed points per row is chaotic. It would be much simpler to take the sum in each column, and take the average of *those* instead: in which case we see the answer is $\frac{1}{n!}n \cdot (n-1)! = 1$.

The following theorem generalizes this:

Example 2.3 (Linearity of Expectation)

Let X and Y be random variables (not necessarily independent). Then $\mathbb{E}[X+Y] = \mathbb{E}[X] + \mathbb{E}[Y]$.

As described in [2] the proof of this is just a "double summation". We do this formally here:

Proof. For simplicity we do the case where X, Y take nonnegative integer values; for the general case one should use $\int$ rather than $\sum$. By definition, we have

$$\mathbb{E}[X+Y] = \sum_{n \ge 0} nP(X+Y=n) = \sum_{n \ge 0} \sum_{a+b=n} nP(X=a, Y=b).$$

Unfortunately[1] we can't write $P(X=a, Y=b) = P(X=a)P(Y=b)$ since X and Y need not be independent. So instead we write $n = a+b$ and then replace $\sum_{n \ge 0} \sum_{a+b=n}$

[1]This was wrong in an earlier published version. Thanks to SH for noticing.

with $\sum_{a,b}$ This lets us split the sum into two parts, which we sum in two different orders. Here is the calculation:

$$\begin{aligned}
\mathbb{E}[X+Y] &= \sum_{n\geq 0} \sum_{a+b=n} (a+b)P(X=a,Y=b) \\
&= \sum_{a,b\geq 0} (a+b)P(X=a,Y=b) \\
&= \sum_{a\geq 0}\sum_{b\geq 0} aP(X=a,Y=b) + \sum_{b\geq 0}\sum_{a\geq 0} bP(Y=b,X=a) \\
&= \sum_{a\geq 0} aP(X=a) + \sum_{b\geq 0} bP(Y=b) \\
&= \mathbb{E}[X] + \mathbb{E}[Y].
\end{aligned}$$

□

Thus we see that:

> **Every application of linearity of expectation is philosophically an application of switching the order of summation.**

Finally, let's look at some number-theoretic examples. First, we prove the following lemma which we will revisit later.

Lemma 2.4 ($\varphi * \mathbf{1} = \mathrm{id}$)
Let $n \geq 1$ be an integer. Then

$$\sum_{d\mid n} \varphi(d) = n.$$

Proof. We will give a more pedestrian proof later on in "multiplicative number theory", and so for now let's present the nice combinatorial proof: look at the fractions

$$\frac{1}{n}, \quad \frac{2}{n}, \quad \frac{3}{n}, \quad \dots, \quad \frac{n}{n}.$$

Suppose we reduce all the fractions to simplest form. Then for every $d \mid n$, there are exactly $\varphi(d)$ fractions with denominator d. (If you don't see why, try writing out the case $n = 15$.) Since there are n fractions total, we're done. □

Now I can present my favorite example which illustrates just how useful swapping the order of summation can be.

Example 2.5 (AMSP 2011 NT3 Exam)
Let n be a positive integer. Prove that

$$\sum_{k\geq 1} \varphi(k) \left\lfloor \frac{n}{k} \right\rfloor = \frac{1}{2}n(n+1).$$

Proof. The key idea is to rewrite the floor as a sum involving divisors:

$$\sum_{k\geq 1} \varphi(k) \left\lfloor \frac{n}{k} \right\rfloor = \sum_{k\geq 1} \varphi(k) \sum_{\substack{m\leq n \\ k\mid m}} 1 = \sum_{k\geq 1} \sum_{\substack{m\leq n \\ k\mid m}} \varphi(k).$$

Thus we're computing the sum of $\varphi(k)$ over several pairs of integers (k, m) for which $k \mid m$, $m \le n$. For example, if $n = 6$, the possible pairs (k, m) are given be the following table:

$$(k,m) \in \left\{ \begin{array}{cccccc} (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ & (2,2) & & (2,4) & & (2,6) \\ & & (3,3) & & & (3,6) \\ & & & (4,4) & & \\ & & & & (5,5) & \\ & & & & & (6,6) \end{array} \right\}$$

Nominally, we're supposed to be summing by the rows of this table (i.e. fix k and run the sum over corresponding m). However, by interchanging the order of summation we can instead consider this as a sum over the columns: if we instead pick the value of m first, we see that

$$\sum_{k \ge 1} \sum_{\substack{k \mid m \\ m \le n}} \varphi(k). = \sum_{m=1}^{n} \sum_{k \mid m} \varphi(k).$$

But we know how to evaluate the inner sum by the lemma! We get

$$\sum_{m=1}^{n} \sum_{k \mid m} \varphi(k) = \sum_{m=1}^{n} m = \frac{1}{2} n(n+1). \qquad \square$$

§2.3 Finite Fourier analysis

A classic MathCounts-flavored problem goes as follows: we wish to compute

$$\sum_{k \ge 0} \binom{1000}{2k}.$$

In order to do this, we use the fact that

$$\begin{aligned} (1+1)^{1000} &= \sum_{n \ge 0} \binom{1000}{n} \\ (1-1)^{1000} &= \sum_{n \ge 0} \binom{1000}{n} (-1)^n. \end{aligned}$$

Adding these together, we get that twice the desired sum is 2^{1000} hence the answer is 2^{999}. The key fact we used was that

$$\frac{1^n + (-1)^n}{2} = \begin{cases} 1 & n \text{ even} \\ 0 & n \text{ odd}. \end{cases}$$

This trick can be generalized using a so-called **roots of unity filter**. To motivate it, we consider the following example problem.

Example 2.6 (Classical application of roots of unity filter)
Compute

$$\sum_{k \ge 0} \binom{1000}{3k}.$$

Solution. We can rewrite the sum as

$$\sum_{n\geq 0} \binom{1000}{n} f(n)$$

where

$$f(n) = \begin{cases} 1 & n \equiv 0 \pmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

So we want the mod 3 analog of the parity detector $1^n + (-1)^n$ we had earlier.

The trick, which gives it the name "roots of unity filter", is that we can take

$$f(n) = \frac{1}{3}\left(1^n + \omega^n + \omega^{2n}\right)$$

where $\omega = \exp\left(\frac{2}{3}\pi i\right)$ is a cube root of unity, satisfying the relation $\omega^2 + \omega + 1 = 0$. Thus, we have

$$\sum_{n\geq 0} \binom{1000}{n} f(n) = \frac{1}{3} \sum_{n\geq 0} \binom{1000}{n} (1 + \omega^n + \omega^{2n}).$$

We can swap the order of summation now (never gets old, does it?) and instead consider

$$\sum_{n\geq 0} \binom{1000}{n} f(n) = \frac{1}{3} \sum_{n\geq 0} \binom{1000}{n} + \frac{1}{3} \sum_{n\geq 0} \binom{1000}{n} \omega^n + \frac{1}{3} \sum_{n\geq 0} \binom{1000}{n} \omega^{2n}.$$

(This doesn't look like the previous examples of swapping the order of summation, but perhaps I could instead write $\sum_{n\geq 0} \sum_{k=0}^{2} \binom{1000}{n} \omega^{nk} = \sum_{k=0}^{2} \sum_{n\geq 0} \binom{1000}{n} \omega^{nk}$. The point is we are exchanging an 1000×3 sum with a 3×1000 sum.) Thus by the binomial theorem the expression in question is

$$\begin{aligned} \sum_{n\geq 0} \binom{1000}{n} f(n) &= \frac{1}{3}\left[(1+1)^{1000} + (1+\omega)^{1000} + (1+\omega^2)^{1000}\right] \\ &= \frac{1}{3}\left[2^{1000} + (-\omega^2)^{1000} + (-\omega)^{1000}\right] \\ &= \frac{1}{3}\left[2^{1000} + \omega + \omega^2\right] \\ &= \frac{1}{3}\left[2^{1000} - 1\right]. \end{aligned}$$

□

§2.4 Problems

Problem 2.7 (Putnam 2011)**.** Let $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ be sequences of positive real numbers such that $a_1 = b_1 = 1$ and $b_n = b_{n-1}a_n - 2$ for $n = 2, 3, \ldots$. Assume that the sequence (b_j) is bounded. Prove that

$$S = \sum_{n=1}^{\infty} \frac{1}{a_1 \cdots a_n}$$

converges, and evaluate S.

Problem 2.8 (Putnam 2013)**.** Let $a_0, a_1, \ldots, a_n, x$ be real numbers, where $0 < x < 1$, satisfying

$$\frac{a_0}{1-x} + \frac{a_1}{1-x^2} + \cdots + \frac{a_n}{1-x^{n+1}} = 0.$$

Prove that for some $0 < y < 1$ we have

$$a_0 + a_1 y + a_2 y^2 + \cdots + a_n y^n = 0.$$

Problem 2.9 (Putnam 2015)**.** Let T be the set of triples of positive integers whose lengths are the sides of a triangle. Compute

$$\sum_{(a,b,c)\in T} \frac{2^a}{3^b 5^c}.$$

Problem 2.10. How many nonempty subsets of $\{1, 2, \dots, 1000\}$ have sum divisible by 3?

§3 Sums modulo a prime

Sometimes you have a sum which you'd like to evaluate modulo p instead of computing altogether. Most of the same strategies from before still apply, and so these problems are not actually too different from before.

However, when working in $\mathbb{F}_p$ instead of $\mathbb{R}$, you can take advantage of the fact that there are only finitely many elements to get some useful symmetry. A simple manifestation of this is

Lemma 3.1 (Fermat's little theorem)
Let p be a prime. Then $a^{p-1} \equiv 1 \pmod p$ whenever $\gcd(a, p) = 1$.

Proof. Multiplication by a exhibits a bijection from $\{1, \dots, p-1\}$ to itself. Now take the products to get $a^{p-1}(p-1)! \equiv (p-1)! \pmod p$, and cancel the resulting $(p-1)!$. □

I'm sure you've already seen this lemma before, but I included the proof anyways because its main idea of exploiting the fact that $\mathbb{F}_p$ is finite is often useful.

Similarly, a sum or product from 1 to $p-1$ will often cancel out in spectacular ways, such as:

Lemma 3.2 (Wilson's theorem)
For any prime p,

$$(p-1)! \equiv -1 \pmod p.$$

Exercise 3.3. Prove this theorem if you don't already know how.

The next lemma is somewhat less well-known than it deserves to be.

Lemma 3.4 (Sums of powers modulo p)
Let p be a prime and m an integer. Then

$$1^m + 2^m + \cdots + (p-1)^m \equiv \begin{cases} 0 \pmod p & \text{if } p-1 \nmid m \\ -1 \pmod p & \text{if } p-1 \mid m. \end{cases}$$

Proof. Suffices to show the case $p-1 \nmid m$ since the other is obvious. Let g be a primitive root modulo p (see [1]), then the above sum equals

$$1 + g^m + \cdots + g^{(p-2)m} \equiv \frac{g^{(p-1)m} - 1}{g^m - 1} \pmod p$$

which is okay since the denominator isn't zero. But the numerator vanishes. □

Here is another example.

Example 3.5 (Wolstenholme's theorem)
Let $p > 3$ be a prime. Then

$$(p-1)!\left(\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{p-1}\right) \equiv 0 \pmod{p^2}.$$

Note the presence of $(p-1)!$ is just a formality to ensure the left-hand side is an integer; it makes more sense to just evaluate $S = 1^{-1} + 2^{-1} + \cdots + (p-1)^{-1} \pmod{p^2}$.

Proof. Let $S = 1^{-1} + 2^{-1} + \cdots + (p-1)^{-1} \pmod{p^2}$. It's already clear (by say Lemma 0.3.4 with $m = -1$) that $p \mid S$, but we in fact want $p^2 \mid S$. We exploit the symmetry by pairing up the opposite terms:

$$2S = \sum_{k\geq 1}^{p-1} \frac{1}{k} + \frac{1}{p-k} = \sum_{k=1}^{p-1} \frac{p}{k(p-k)}.$$

So just as before we see that S is divisible by p, but this time we know information mod p^2: it now suffices to show that

$$\frac{1}{p} \cdot 2S = \sum_{k=1}^{p-1} \frac{1}{k(p-k)}$$

is zero modulo p as well. But

$$\sum_{k=1}^{p-1} \frac{1}{k(p-k)} \equiv \sum_{k=1}^{p-1} \frac{1}{k(-k)} = -\sum_{k=1}^{p-1} k^{-2} \pmod{p}$$

and we're done by Lemma 0.3.4 applied at $m = -2$. (Where did we use $p > 3$?) □

Finally, here is a weird trick which is often useful when faced with $\frac{1}{k}$ expressions modulo p. Look through the problems for a few examples.

Lemma 3.6 (Harmonic modulo p trick)
For any integer $k = 1, 2, \ldots, p-1$, we have

$$\frac{1}{k} \equiv (-1)^{k-1} \cdot \frac{1}{p}\binom{p}{k} \pmod{p}.$$

Exercise 3.7. Check this.

This is often useful because it reduces a computation involving k^{-1}'s modulo p to a computation involving $\binom{p}{k}$ mod p^2; the latter is often easier to deal with.

§3.1 Problems

Problem 3.8 (ELMO 2009, John Berman)**.** Let p be an odd prime and x be an integer such that $p \mid x^3 - 1$ but $p \nmid x - 1$. Prove that p divides

$$(p-1)!\left(x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots - \frac{x^{p-1}}{p-1}\right).$$

Problem 3.9. Let $p > 5$ be a prime. Prove that

$$\frac{1}{1^3} + \frac{1}{2^3} + \cdots + \frac{1}{(p-1)^3} \equiv 0 \pmod{p^2}.$$

Problem 3.10 (OMO 2013 W42, Victor Wang)**.** Find the remainder when

$$\prod_{i=0}^{100} (1 - i^2 + i^4)$$

is divided by 101.

§4 Multiplicative number theory

Earlier we saw that that $\sum_{d|n} \varphi(d) = n$. In this section we'll develop a more general theory which can handle these divisor-based sums.

To get a grasp of what we're doing, let's redo the example from above. The key idea is rooted in the standard MathCounts formula for the sum of the prime factors of $n = p_1^{e_1} \dots p_k^{e_k}$: it is equal to

$$\sum_{d|n} d = \left(1 + p_1 + p_1^2 + \cdots + p_1^{e_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{e_2}\right) \dots \left(1 + p_k + p_k^2 + \cdots + p_k^{e_k}\right).$$

Indeed, if we expand the right-hand side, each factor appears exactly once.

But in fact, φ has a special property: if m and n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$. (Proof: Chinese remainder theorem.) So we can copy the work above to get

$$\sum_{d|n} \varphi(d) = \left(\varphi(1) + \varphi(p_1) + \cdots + \varphi(p_1^{e_1})\right) \dots \left(\varphi(1) + \varphi(p_k) + \cdots + \varphi(p_k^{e_k})\right).$$

But now we're done, because it's easy to see that $\varphi(1) + \varphi(p) + \cdots + \varphi(p^e) = p^e$ when p is a prime, and thus the right-hand side is n.

In this short section we will grow this idea into its full generality. In what follows, $\mathbb{N}$ denotes the positive integers.

§4.1 Multiplicative functions

Definition 4.1. An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$. It is

- **multiplicative** if $f(mn) = f(m)f(n)$ for **relatively prime** m and n.
- **completely multiplicative** if $f(mn) = f(m)f(n)$ for **any** m and n.

Example 4.2 (Completely multiplicative functions)
The following are examples of completely multiplicative functions.

- The identity function id.
- The Dirichlet delta function, $\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & n \geq 2. \end{cases}$
- The constant function $\mathbf{1}$, given by $\mathbf{1}(n) = 1$.

Example 4.3 (Multiplicative functions)
The following are examples of multiplicative functions which are not completely multiplicative.

- Euler's φ. For example, $\varphi(15) = \varphi(3)\varphi(5)$. But not $\varphi(9) = \varphi(3)\varphi(3)$.
- The Möbius function μ, defined by
$$\mu(n) = \begin{cases} (-1)^m & \text{if } n \text{ has } m \text{ prime factors, all distinct} \\ 0 & n \text{ is not squarefree.} \end{cases}$$
For example, $\mu(10) = 1$, $\mu(105) = -1$, but $\mu(12) = 0$.
- σ is the sum of divisors function. For example $\sigma(6) = 1 + 2 + 3 + 6 = 12$.
- τ is the divisor counting function. For example $\tau(6) = 4$.

Of course, the product of two multiplicative functions is also multiplicative.

The nice property of multiplicative functions is that it is **sufficient to determine their values on prime powers**. For example, we have formulas like
$$\varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\dots\left(p_m^{e_m} - p_m^{e_m-1}\right)$$
when $n = p_1^{e_1}\dots p_m^{e_m}$. This is one way you can prove the formula above: the Chinese remainder theorem implies quickly that φ is multiplicative, and it is straightforward to compute $\varphi(p^k) = p^k - p^{k-1}$, hence the result.

§4.2 Dirichlet convolution

Now given two arithmetic functions f and g, we define the **Dirichlet convolution** as
$$(f * g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{de=n} f(d)g(e).$$
This is more frequent than you might expect:

Example 4.4 (Examples of Convolution)
Verify that

- $\mathbf{1} * \mathbf{1} = \tau$.
- $\mathbf{1} * \mathrm{id} = \sigma$.
- $\mathrm{id} * \mathrm{id} = n \cdot \tau$.
- $\mathbf{1} * \phi = \mathrm{id}$ (previous example).
- $\delta * f = f$ for any f.

Here are some properties of $*$:

- The identity of $*$ is the Dirichlet delta function.
- Clearly $*$ is commutative.

- The operation $*$ is associative because
$$((f*g)*h)(n) = (f*(g*h))(n) = \sum_{d_1d_2d_3=n} f(d_1)g(d_2)h(d_3).$$
- It distributes over addition: $f*(g+h) = f*g + f*h$.
- Most important: the **convolution of two multiplicative functions is also multiplicative**.

Thus we have an operation on the set of multiplicative functions.

Exercise 4.5. Check that convolutions of multiplicative functions are multiplicative. (Mimic the proof of φ we used earlier.)

The upshot of this is that we can now use our theory to completely eradicate our earlier example.

Example 4.6 ($\varphi * \mathbf{1} = \mathrm{id}$)
Let $n \geq 1$ be an integer. Then
$$\sum_{d|n} \varphi(d) = n.$$

Proof. Rephrasing the problem, we wish to show that
$$\varphi * \mathbf{1} = \mathrm{id}.$$
It is true for prime powers $n = p^e$, because the left-hand side is $1 + (p-1) + (p^2-p) + \cdots + (p^e - p^{e-1}) = p^e$. But since both the LHS and RHS are multiplicative, this implies the problem. □

§4.3 Möbius inversion

We now know that given a multiplicative function f, we have a good handle on
$$g(n) = \sum_{d|n} f(d)$$
because g is the Dirichlet convolution $f * \mathbf{1}$. However, occasionally we instead have g and want to recover f. The way to do this is through Möbius inversion.

Lemma 4.7 (Möbius is inverse of 1)
We have $\mu * \mathbf{1} = \delta$.

Exercise 4.8. Prove this. (Check on prime powers.)

Theorem 4.9 (Möbius inversion formula)
Let f and g be *any* arithmetic functions (possibly not multiplicative). Then
$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d)g(n/d).$$
In other words, if $g = f * \mathbf{1}$ then $f = g * \mu$.

Proof. Assume $g = f * \mathbf{1}$. Then

$$g * \mu = (f * \mathbf{1}) * \mu = f * (\mathbf{1} * \mu) = f * \delta = f. \qquad \square$$

Here is a silly application from the IMO Shortlist.

Example 4.10 (Shortlist 1989)
Define a sequence $(a_n)_{n \ge 1}$ by $\sum_{d|n} a_d = 2^n$. Show that n divides a_n.

Solution. By Möbius inversion, $a_n = \sum_{d|n} \mu(n/d) 2^d$. Now just let $n = p_1^{e_1} \dots p_r^{e_r}$ and bash. Details omitted. $\square$

§4.4 Problems

Problem 4.11. Prove that for any integer $n \ge 1$,

$$\sum_{d|n} (\tau(d))^3 = \left(\sum_{d|n} \tau(d) \right)^2.$$

Problem 4.12 (Bulgaria 1989)**.** Let $\Omega(n)$ denote the number of prime factors of n, counted with multiplicity. Evaluate

$$\sum_{n=1}^{1989} (-1)^{\Omega(n)} \left\lfloor \frac{1989}{n} \right\rfloor.$$

Problem 4.13. Prove that for all positive integers n,

$$\mu(n) = \sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \cos\left(\frac{2\pi k}{n} \right).$$

§5 Generating functions

> A generating function is a device somewhat similar to a bag. Instead of carrying many little objects detachedly, which could be embarrassing, we put them all in a bag, and then we have only one object to carry, the bag.
> — George Pólya

The idea of generating functions is as follows: given a sequence a_n we want to understand we consider the formal series

$$A(x) = \sum_{n \ge 0} a_n x^n.$$

This gives us another sum that we can work with. Reasons why this could be helpful:

- $A(x)$ may often have a nice closed form, like $1 + x + x^2 + \dots = \frac{1}{1-x}$, and as Pólya has said this makes it much easier to work with.
- Often a_n is itself a sum, and now we can change the order of summation. See Snake Oil below.

§5.1 Toy applications

Example 5.1 (The Classic)
We have
$$\sum_{n \ge 0} \binom{1000}{n} = 2^{1000}.$$

Proof. Let $a_n = \binom{1000}{n}$, for example. Of course, by the binomial theorem we have attached generating function
$$A(x) = \sum_{n \ge 0} a_n x^n = \sum_{n \ge 0} \binom{1000}{n} x^n = (1+x)^{1000}.$$
Plugging in $x = 1$, for example, then implies the usual identity $\sum_{n \ge 0} \binom{1000}{n} = 2^{1000}$. □

Example 5.2 (The Derivative of the Classic)
We have
$$\sum_{n \ge 0} n \binom{1000}{n} = 1000 \cdot 2^{999}.$$

Proof. Take the derivative of the previous example
$$\sum_{n \ge 1} \binom{1000}{n} n x^{n-1} = 1000(1+x)^{999}.$$
This time, the we obtain $\sum_{n \ge 0} n\binom{1000}{n} = 1000 \cdot 2^{999}$. □

Exercise 5.3. Compute $\sum_{n \ge 0} n^2 \binom{1000}{n}$.

§5.2 Linear recurrences

Let's now use generating functions to derive the closed form of the Lucas numbers L_n, which are defined by
$$L_0 = 2, \quad L_1 = 1, \quad L_{n+2} = L_{n+1} + L_n.$$
For concreteness, the first few terms are $2, 1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$.

Theorem 5.4 (Explicit form for Lucas numbers)
Let $\alpha = \frac{1}{2}(1+\sqrt{5})$ and $\beta = \frac{1}{2}(1-\sqrt{5})$. Then
$$L_n = \alpha^n + \beta^n.$$

Proof. We consider the generating function
$$L(x) = 2 + x + 3x^2 + 4x^3 + 7x^4 + \ldots.$$

We aim to find its compact form. Write

$$\begin{aligned} L(x) &= 2 + x + 3x^2 + 4x^3 + 7x^4 + \dots \\ xL(x) &= 2x + x^2 + 3x^3 + 4x^4 + \dots \\ x^2L(x) &= 2x^2 + x^3 + 3x^4 + \dots. \end{aligned}$$

Thus we can deduce

$$L(x) - xL(x) - x^2L(x) = 2 - x$$

and consequently

$$(1 - x - x^2)L(x) = 2 - x \implies L(x) = \frac{2-x}{1-x-x^2}.$$

Now, what can we do with this? Answer: use *partial fractions* again. The denominator factors into $(1-\alpha x)(1-\beta x)$, and from this we deduce

$$L(x) = \sum_{n \ge 0} L_n x^n = \frac{1}{1-\alpha x} + \frac{1}{1-\beta x} = \sum_{n \ge 0} \left(\alpha^n + \beta^n\right) x^n.$$

So we're done upon equating coefficients. □

Philosophically, what's happened is that by considering a sum, we could compactify all the information about L_n into a single rational expression, which we could then use partial fractions on.

Exercise 5.5. In the same way, derive Binet's formula: if F_n is the nth Fibonacci number then

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n).$$

As an intermediate step, you should find the generating function $\frac{x}{1-x-x^2}$ for the Fibonacci numbers.

In principle, every linear recurrence can be solved in this way. For more details see for example [5].

§5.3 Common generating functions

So far, we know that $\frac{1}{1-x} = 1 + x + x^2 + \dots$ and $(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \dots$. It turns out we can get more formulas to add to our arsenal using the following:

Theorem 5.6 (Generalized binomial theorem)
Let r be *any* real number (not necessarily an integer). Then

$$(1+x)^r = \sum_{n \ge 0} \binom{r}{n} x^n \quad \text{where} \quad \binom{r}{n} = \frac{r(r-1)\dots(r-n+1)}{n!}.$$

Proof. For concreteness, let's show the coefficient of x^3 is $\frac{r(r-1)(r-2)}{3!}$. Suppose

$$(1+x)^r = \sum_{k \ge 0} a_k x^k = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \dots.$$

Take the triple derivative:

$$r(r-1)(r-2) \cdot (1+x)^{r-3} = 6a_3 + 24a_4 x + 60a_5 x^2 + \dots$$

Now if we compare the constant terms we get $a_3 = \frac{1}{6}r(r-1)(r-2)$. □

This generalized binomial theorem has several applications, described below.

- For example, if we set $r = -1$ we obtain
$$\frac{1}{1+x} = \sum_{n\geq 0} \binom{-1}{n} x^n = \sum_{n\geq 0} \frac{(-1)(-2)\dots(-n)}{n!} x^n = \sum_{n\geq 0} (-x)^n.$$

- More generally:
Exercise 5.7. Prove that for an *integer* m, we have $\binom{-m-1}{k} = (-1)^k \binom{m+k}{k}$. Deduce that
$$\frac{1}{(1-x)^{m+1}} = \binom{m}{m} x^0 + \binom{m+1}{m} x^1 + \binom{m+2}{m} x^2 + \dots = \sum_{k\geq 0} \binom{k+m}{m} x^k$$

- A second interesting example is $r = -\frac{1}{2}$. For convenience, we will look at $(1-4x)^{-\frac{1}{2}}$ rather than $(1-x)^{-\frac{1}{2}}$. Note that
$$\begin{aligned}
(1-4x)^{-\frac{1}{2}} &= \sum_{k\geq 0} (-4)^k \binom{-1/2}{k} x^k \\
&= \sum_{k\geq 0} (-4)^k \frac{\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\dots\left(-\frac{2k-1}{2}\right)}{k!} x^k \\
&= \sum_{k\geq 0} 2^k \cdot \frac{1\cdot 3\cdot\dots\cdot(2k-1)}{k!} x^k = \sum_{k\geq 0} 2^k \cdot \frac{(2k-1)!!}{k!} x^k \\
&= \sum_{k\geq 0} \frac{(2k)!/k!}{k!} x^k = \sum_{k\geq 0} \binom{2k}{k} x^k.
\end{aligned}$$
Thus we get the generating function for $\binom{2k}{k}$. Here we have used the well-known fact that
$$2^k k!(2k-1)!! = (2k)!$$
If you haven't seen this before, try to prove it!

- Finally, let's integrate both sides of $(1-4x)^{-\frac{1}{2}} = \sum_{k\geq 0} \binom{2k}{k} x^k$. This tells us that
$$\sum_{k\geq 0} \frac{1}{k+1} \binom{2k}{k} x^{k+1} = \frac{1/4}{-\frac{1}{2}} (1-4x)^{\frac{1}{2}} + C$$
for some constant C; by comparing the constant terms, we get $C = \frac{1}{2}$. Dividing by x we derive
$$\sum_{k\geq 0} \frac{1}{k+1} \binom{2k}{k} x^k = \frac{1-\sqrt{1-4x}}{2x}.$$
The numbers $C_k = \frac{1}{k+1}\binom{2k}{k}$ are the infamous **Catalan numbers**.

In Table 1 we collect the fruits of our labors above. Notice that in particular we can handle both of

- sequences of the form $\binom{n}{*}$ (where the top is fixed while the bottom moves)
- sequences of the form $\binom{*}{n}$ (where the bottom is fixed while the top moves).

These formulas will be indispensable later on.

Here is an application of the formulas.

$$(1+x)^n = \sum_{k\geq 0} \binom{n}{k} x^k$$
$$\frac{1}{(1-x)^{m+1}} = \sum_{k\geq 0} \binom{k+m}{m} x^k$$
$$\frac{x^m}{(1-x)^{m+1}} = \sum_{k\geq 0} \binom{k}{m} x^k$$

$$\frac{1}{\sqrt{1-4x}} = \sum_{k\geq 0} \binom{2k}{k} x^k$$
$$\frac{1-\sqrt{1-4x}}{2x} = \sum_{k\geq 0} C_k x^k$$
$$e^x = \sum_{k\geq 0} \frac{1}{k!} x^k$$

Table 1: Table of common generating functions

Example 5.8 (HMMT 2007 Combinatorics #9)
Let S be the set of triples (i,j,k) of positive integers which satisfy $i+j+k=17$. Compute
$$\sum_{(i,j,k)\in S} ijk.$$

Solution. The point is to notice that one can consider the quantity
$$F(x) = \left(\sum_{i\geq 0} ix^i\right)\left(\sum_{j\geq 0} jx^j\right)\left(\sum_{k\geq 0} kx^k\right)$$
and that we merely want the coefficient of x^{17}. But
$$F(x) = \left(\frac{x}{(1-x)^2}\right)^3 = x^3 \frac{1}{(1-x)^6}$$
so we need the x^{14} coefficient of $\frac{1}{(1-x)^6}$ which we know is $\binom{19}{5}$. □

§5.4 Snake Oil method

The so-called Snake Oil method, so dubbed by [4], is a powerful way to force a combinatorial sum into a generating-function double sum. It serves as a "miracle cure" for a whole class of problems, hence the name.

Here's how it works: suppose we have a sum we want to evaluate in terms of n, perhaps of the form
$$a_n = \sum_k F(k,n)$$
for some function F. It would suffice to evaluate the generating function
$$A(x) = \sum_{n\geq 0} a_n x^n = \sum_{n\geq 0}\sum_k F(k,n)x^n.$$
Since this is a double sum, we can now **swap the order of summation** and obtain
$$A(x) = \sum_k \sum_{n\geq 0} F(k,n)x^n.$$
With any luck the interchanged sum will be significantly easier to evaluate. This works best if F is the product of several functions that we know the generating functions of (like in table above).

Let's see an example:

Example 5.9 ([4])
For $n \ge 0$, compute
$$\sum_{k \ge 0} \binom{n+k}{2k} 2^{n-k}.$$

Proof. As described above, we let
$$\begin{aligned}
A(x) &= \sum_{n \ge 0} \left[\sum_{k \ge 0} \binom{n+k}{2k} 2^{n-k} \right] x^n = \sum_{k \ge 0} \sum_{n \ge 0} \binom{n+k}{2k} 2^{n-k} x^n \\
&= \sum_{k \ge 0} 2^{-k} \sum_{n \ge 0} \binom{n+k}{2k} (2x)^n = \sum_{k \ge 0} x^k \sum_{n \ge 0} \binom{(n-k)+2k}{2k} (2x)^{n-k} \\
&= \sum_{k \ge 0} x^k \sum_{a \ge 0} \binom{a+2k}{2k} (2x)^a = \sum_{k \ge 0} x^k \left(\frac{1}{1-2x} \right)^{2k+1} \\
&= \sum_{k \ge 0} \frac{1}{1-2x} \left(\frac{x}{(1-2x)^2} \right)^k = \frac{1}{1-2x} \frac{1}{1 - \frac{x}{(1-2x)^2}} = \frac{1-2x}{(1-2x)^2 - x} \\
&= \frac{1-2x}{1-5x+4x^2} = \frac{1-2x}{(1-4x)(1-x)} = \frac{1/3}{1-x} + \frac{2/3}{1-4x} \\
&= \sum_{n \ge 0} \left(\frac{1}{3} + \frac{2}{3} 4^n \right) x^n.
\end{aligned}$$
Hence by matching the nth coefficients we obtain
$$\sum_{k \ge 0} \binom{n+k}{2k} 2^{n-k} = \frac{1}{3} + \frac{2}{3} \cdot 4^n.$$
□

Example 5.10 ([4])
For $n \ge 0$, compute
$$\sum_{k \ge 0} \binom{k}{n-k}.$$

Solution. Snake Oil:
$$\begin{aligned}
\sum_{n \ge 0} \left[\sum_{k \ge 0} \binom{k}{n-k} \right] x^n &= \sum_{k \ge 0} \sum_{n \ge 0} \binom{k}{n-k} x^n \\
&= \sum_{k \ge 0} x^k \sum_{k \le n \le 2k} \binom{k}{n-k} x^{n-k} \\
&= \sum_{k \ge 0} x^k \cdot (1+x)^k = \frac{1}{1-x(1+x)} \\
&= \frac{1}{1-x-x^2}.
\end{aligned}$$
Thus the sum in question is the Fibonacci number F_{n+1}. □

The snake oil method relies on having the free variable appearing in only one place. So the following example doesn't succumb immediately to Snake Oil:

Prove that for $n \ge 0$ we have

$$\sum_{i=0}^{n} \binom{n}{i}\binom{2n}{n-i} = \binom{3n}{n}.$$

However, it is a special case of Vandermonde convolution, which *does* succumb to Snake Oil. So if a free variable appears in many places, this is often a hint to try and consider generalizations of the identity.

§5.5 Problems

Problem 5.11 ([3]). Prove that for every integer $n \ge 0$,

$$\sum_{a+b=n} \binom{2a}{a}\binom{2b}{b} = 4^n.$$

Problem 5.12 ([3]). For integers $m, n \ge 0$, prove that

$$\sum_{a+b=m} (-1)^a \binom{n}{a}\binom{n+b-1}{b} = \begin{cases} 1 & m = 0 \\ 0 & m > 0. \end{cases}$$

Problem 5.13 ([6]). Let $m \le n$ be positive integers. Compute

$$\sum_{k=m}^{n} \binom{n}{k}\binom{k}{m}.$$

Problem 5.14 ([4]). For $m, n \ge 1$ compute

$$\sum_{k \ge 0} \binom{n+k}{m+2k}\binom{2k}{k}\frac{(-1)^k}{k+1}.$$

§6 Author's Pick

Problem 6.1 (AMSP 2011 NT3 Exam). Let μ be the Möbius function. For $n \ge 1$, evaluate

$$\sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor.$$

Problem 6.2 (USAMO 2010/5, Titu Andreescu). Let $q = \frac{3p-5}{2}$ where p is an odd prime, and let

$$S_q = \frac{1}{2 \cdot 3 \cdot 4} + \frac{1}{5 \cdot 6 \cdot 7} + \cdots + \frac{1}{q(q+1)(q+2)}.$$

Prove that if $\frac{1}{p} - 2S_q = \frac{m}{n}$ for integers m and n, then $m - n$ is divisible by p.

Problem 6.3 (Princeton Individual Finals 2015, Xiaoyu Xu). Let p be an odd prime. Prove that $p^2 \mid 2^p - 2$ if and only if

$$\frac{1}{1 \cdot 2} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(p-2)(p-1)} \equiv 0 \pmod{p}.$$

Problem 6.4 (Reed Dawson, [4]). For $n \geq 0$, compute

$$\sum_{k \geq 0} \binom{2k}{k} \binom{n}{k} \left(-\frac{1}{4}\right)^k.$$

Problem 6.5 (NIMO 24.8, Evan Chen). For a complex number $z \neq 3,4$, let $F(z)$ denote the real part of $\frac{1}{(3-z)(4-z)}$. Compute

$$\int_0^1 F\left(\frac{\cos 2\pi t + i \sin 2\pi t}{5}\right) \, dt.$$

Problem 6.6 (NIMO 14.8, Evan Chen). Let x be a positive real number. Define

$$A = \sum_{k=0}^{\infty} \frac{x^{3k}}{(3k)!}, \quad B = \sum_{k=0}^{\infty} \frac{x^{3k+1}}{(3k+1)!}, \quad \text{and} \quad C = \sum_{k=0}^{\infty} \frac{x^{3k+2}}{(3k+2)!}.$$

Given that $A^3 + B^3 + C^3 + 8ABC = 2014$, compute ABC.

Problem 6.7 (OMO 2013 F24, Evan Chen). The real numbers $a_0, a_1, \ldots, a_{2013}$ and $b_0, b_1, \ldots, b_{2013}$ satisfy

$$a_n = \frac{1}{63}\sqrt{2n+2} + a_{n-1} \quad \text{and} \quad b_n = \frac{1}{96}\sqrt{2n+2} - b_{n-1}$$

for every integer $n = 1, 2, \ldots, 2013$. If $a_0 = b_{2013}$ and $b_0 = a_{2013}$, compute

$$\sum_{k=1}^{2013} \left(a_k b_{k-1} - a_{k-1} b_k\right).$$

Problem 6.8 (Shortlist 2014 N6). Let $a_1 < a_2 < \cdots < a_n$ be pairwise coprime positive integers with a_1 being prime and $a_1 \geq n+2$. On the segment $I = [0, a_1 a_2 \cdots a_n]$ of the real line, mark all integers that are divisible by at least one of the numbers a_1, …, a_n. These points split I into a number of smaller segments. Prove that the sum of the squares of the lengths of these segments is divisible by a_1.

Problem 6.9 (OMO 2014 S25, Michael Kural). Compute

$$\sum_{n=1}^{\infty} \frac{\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}}{\binom{n+100}{100}}.$$

Problem 6.10 (OMO 2015 F30, Michael Kural). Ryan is learning number theory. He reads about the *Möbius function* $\mu : \mathbb{N} \to \mathbb{Z}$, defined by $\mu(1) = 1$ and $\mu(n) = -\sum_{d|n, d \neq n} \mu(d)$ for $n > 1$. However, Ryan doesn't like negative numbers, so he invents his own function: the *dubious function* $\Delta : \mathbb{N} \to \mathbb{N}$, defined by the relations $\Delta(1) = 1$ and

$$\Delta(n) = \sum_{\substack{d|n \\ d \neq n}} \Delta(d)$$

for $n > 1$. Help Ryan determine the value

$$\sum_{k=0}^{\infty} \frac{\Delta(15^k)}{15^k}.$$

§7 Hints

2.7 Telescoping. $S = 3/2$.

2.8 By contradiction and intermediate value theorem. Expand the geometric series and swap the order of summation.

2.9 $\frac{17}{21}$. Ravi substitution.

2.10 Roots of unity filter on $-1 + (1+x)(1+x^2)(1+x^3)\dots(1+x^{1000})$.

3.8 Lemma 0.3.6.

3.9 Repeat the proof of Wolstenholme by adding opposite terms.

3.10 Answer is 9. Write as $\frac{i^6+1}{i^2+1}$ for $i \neq \pm 10$. Pair up and cancel all the other remaining terms and cancel.

4.11 Both sides are multiplicative, so check it on prime powers.

4.12 You will need to compute $\sum_{d|n}(-1)^{\Omega(d)}$. Then swap the order of summation with the floor again.

4.13 Let $F(n)$ be the right-hand side. Show that $F * \mathbf{1} = \delta$.

5.11 Square of $\frac{1}{\sqrt{1-4x}}$.

5.12 Product of $(1+(-x))^n$ and $\frac{1}{(1-x)^n}$.

5.13 Snake Oil. $\binom{n}{m}2^{n-m}$.

5.14 Snake Oil. $\binom{n-1}{m-1}$.

6.1 It equals 1. Switch order of summation with floor as before. Use the fact that $\sum_{d|n}\mu(d) = \delta(n)$.

6.2 Partial fractions.

6.3 Partial fractions, plus Lemma 0.3.6.

6.4 $2^{-2n}\binom{2n}{n}$. Snake Oil.

6.5 Don't be scared by the integral. Partial fractions then geometric series. Switch the sum and integral.

6.6 Answer is 183. Show that $A^3+B^3+C^3-3ABC = 1$. Roots of unity filter with e^x.

6.7 Look at $(a_n - a_{n-1})(b_n + b_{n-1})$.

6.8 Don't be scared that this is an N6. Let $p = a_1$ and look at intervals of the form $[cp, cp+p]$. Break the sum into several organized parts, and show that each part has sum zero. You will likely need Lemma 0.3.4.

6.9 $\frac{100}{9801}$. Swap the order of summation, and telescope the inverted $\binom{*}{100}$ binomial coefficients into $\binom{*}{99}$. Then telescope again.

6.10 Answer: $\frac{11}{7}$. Let $f(i,j) = \Delta(3^i 5^j)$. Find a recurrence for f, and deduce that the corresponding two-variable generating function obeys $F(x,y) = \frac{1}{2}\left(1 + \frac{1}{1-2x-2y+2xy}\right)$. Compute the s^0 coefficient of $F(s, \frac{1}{15s})$.

References

[1] **Orders Modulo a Prime**, by Evan Chen. http://web.evanchen.cc/handouts/ORPR/ORPR.pdf

[2] **Expected Uses of Probability**, by Evan Chen. http://web.evanchen.cc/handouts/ProbabilisticMethod/ProbabilisticMethod.pdf

[3] **Topics in Generating Functions**, by Qiaochu Yuan. https://math.berkeley.edu/~qchu/TopicsInGF.pdf.

[4] **generatingfunctionology**, by Herbert Wilf. https://www.math.upenn.edu/~wilf/DownldGF.html.

[5] **IMOmath: Recurrence Equations**, by Milan Novaković. http://www.imomath.com/index.php?options=356&lmm=0

[6] **IMOmath: The Method of Snake Oil**, by Milan Novaković. http://www.imomath.com/index.php?options=357&lmm=0