REU 2006 · Discrete Math · Lecture 1

Instructor: László Babai
Scribe: Travis Schedler
Editors: Eliana Zoque and Elizabeth Beazley

June 20, 2006. Last updated June 21, 2006 at 12:07 a.m.
NOT FULLY PROOF-READ

Laci's email is laci@cs.uchicago.edu. His office is in Ryerson 164. It is best if you ask questions after class or email him for an appointment.

1.1 The Limit of a Sequence

Let us begin by discussing some familiar series.

Example 1.1.1.

$$\zeta(1) := \sum_{k=1}^{\infty} \frac{1}{k} = \infty, \tag{1.1.1}$$

that is, the sum diverges.

Example 1.1.2. (Euler 1700's)

$$\zeta(2) := \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}. \tag{1.1.2}$$

This can be proved, as is done in Honors Analysis, using Parseval's theorem from Fourier analysis. Another proof using contour integrals is often presented in a course on complex analysis.

However, just proving that the sum $\zeta(2)$ converges can be done in one line, by comparing with a telescoping series:

$$\zeta(2) = \sum_{k=1}^{\infty} \frac{1}{k^2} < 1 + \sum_{k=2}^{\infty} \frac{1}{k(k-1)} = 1 + \sum_{k=2}^{\infty} \left(\frac{1}{k-1} - \frac{1}{k} \right) = 2. \tag{1.1.3}$$

Definition 1.1.3. In general, the **zeta function**, $\zeta(s)$, is defined for $s > 1$ by

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}. \tag{1.1.4}$$

Exercise 1.1.4. $\zeta(s) < \infty$ for all $s > 1$.

Exercise 1.1.5 (*). $\lim_{s \to 1^+} (s-1)\zeta(s) = 1$.

This uses the standard

Definition 1.1.6. $\lim_{x \to x_0} f(x) = L$ means $(\forall \epsilon > 0)(\exists \delta > 0)(\forall x)(|x - x_0| < \delta \Rightarrow |f(x) - L| < \epsilon)$.

Here the quantifiers are:

$$(\exists x) \text{ means "there exists } x \text{ such that";} \tag{1.1.5}$$
$$(\forall x) \text{ means "for all } x\text{".} \tag{1.1.6}$$

If $L = \infty$, then

Definition 1.1.7. $\lim_{x \to x_0} f(x) = \infty$ means $(\forall k)(\exists \delta > 0)(\forall x)(|x - x_0| < \delta \Rightarrow f(x) > k)$.

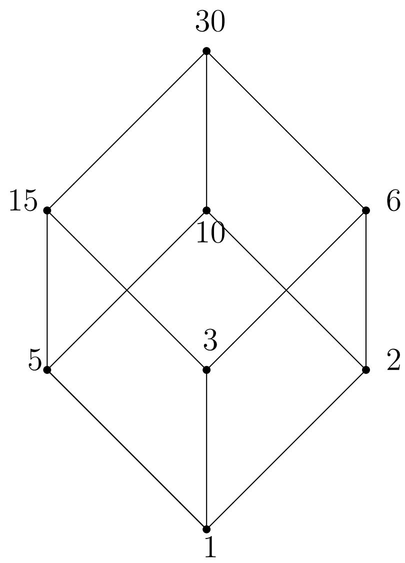
If L is finite, and $x_0 = \infty$, then

Definition 1.1.8. $\lim_{x \to \infty} = L$ means $(\forall \epsilon > 0)(\exists M)(\forall x)(x > M \Rightarrow |f(x) - L| < \epsilon)$.

Quantified formulas like this can be viewed as a game between the universal player that wants to make it false, and the existential player that wants to make it true. The formula is true if the existential player has a winning strategy and false if the universal player has a winning strategy.

There is a philosophy that says that each quantifier alternation in a definition results in an order of magnitude increase in the difficulty of the concept defined. As we see above, this fundamental definition in calculus involves three alternating quantifiers: this is one reason why calculus is difficult. It is peculiar that in games such as chess, people deal with unlimited alternation; yet when it comes to mathematics, very few will comprehend concepts defined by several alternations of quantifiers.

Now let's move on to a game some of you may be familiar with: **The Divisor Game**. Consider the divisor diagram for 30:



In this game, players alternate picking divisors of 30 and thereby erase that divisor and all of its divisors from the divisor diagram. They can only pick divisors that are not already erased (*i.e.*, are not divisors of a number already picked). The loser is the player that ends up having to pick 30.

As a special case, consider replacing the number 30 with a prime power p^k so that the diagram is just a line. Then the first player can always win by choosing the divisor p^{k-1}.

Exercise 1.1.9. Prove that for ANY number $n > 1$, in the Divisor Game played on the divisors of n, the first player has a winning strategy.

This is a proof of existence. It remains an **open problem** to find an explicit winning strategy for any number n. This is open even for numbers of the form $p^k q^\ell$ where p, q are distinct primes.

For some special cases, you can actually write down an algorithm that expresses a winning strategy.

Exercise 1.1.10. Find explicit winning strategies for numbers of the form $p^k \cdot q$, $p^k \cdot q^k$, pqr, and $pqrs$, where p, q, r, and s are distinct primes.

Note that the divisor diagram for 30, as a graph, is a three-dimensional cube. If we pick the product of n distinct primes, its diagram will be an n-cube. That is, square-free numbers have divisor diagrams which are hypercubes of dimension = the number of prime factors. Even for these we do not know any general explicit strategy.

1.2 Arithmetic Functions

Let's continue our exploration of divisors by studying some functions.

Definition 1.2.1. For any number $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where the p_i are distinct primes, let $d(n)$ be the number of positive divisors of n (including n).

For example, $d(30) = 8$. In general, the divisors of n are the numbers $p_1^{\ell_1} \cdots p_r^{\ell_r}$ for $0 \le \ell_i \le k_i$. One sees therefore that

$$d(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1). \tag{1.2.1}$$

We see that

Corollary 1.2.2. If $\gcd(a, b) = 1$, then $d(ab) = d(a)d(b)$.

On the other hand, for $a = p^k, b = p^\ell$, $d(a) = k + 1, d(b) = \ell + 1$, and $d(ab) = k + \ell + 1 < (k + 1)(\ell + 1)$. This motivates the following:

Definition 1.2.3. An **arithmetic function** is a function $f : \mathbb{Z}^+ \to \mathbb{C}$.

Definition 1.2.4. A **multiplicative function** is an arithmetic function such that $(\forall a, b \in \mathbb{Z}^+)(\gcd(a, b) = 1 \Rightarrow f(ab) = f(a)f(b))$.

Example 1.2.5. Examples of multiplicative functions include $d(n)$ and Euler's φ-function, which is discussed later.

Examples of **totally multiplicative** functions ($f(ab) = f(a)f(b)$ for all a, b): the identity function id, given by $\mathrm{id}(n) = n$; the one function $1(n) = 1, \forall n$, or more generally, $f(n) = n^k$ for any $k \ge 0$. Any totally multiplicative function is multiplicative, but not vice-versa.

Definition 1.2.6. $\sigma(n) =$ the sum of the divisors of n.

This is also multiplicative!

Definition 1.2.7. $\nu(n) =$ the number of distinct prime divisors of n. Specifically, $\nu(n) = r$ if $n = \prod_{i=1}^{r} p_i^{k_i}$.

Now, $\nu(n)$ is not multiplicative, but rather *additive*:

Definition 1.2.8. A function is **additive** if $(\forall a, b)(\gcd(a, b) = 1 \Rightarrow f(ab) = f(a) + f(b))$.

Observation 1.2.9. If $f(x)$ is additive, then $e^{f(x)}$ is multiplicative.

Note that $\nu(n)$ is not **totally additive**. One standard example of a totally additive function is $k \log n$. But there are other totally additive functions, such as:

Definition 1.2.10. $\nu^*(n) =$ the total number of prime divisors $= \sum k_i$.

Example 1.2.11. As another example, consider $\mathrm{gab}(n) := \prod p_i$ (for $n = \prod p_i^{k_i}$), which is multiplicative.

1.3 Asymptotics and Primes

Definition 1.3.1. Two sequences $\{a_n\}$ and $\{b_n\}$ are **asymptotically equal**, denoted $a_n \sim b_n$, if $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$.

Example 1.3.2. For example, $5n^3 + 3n^2 - \pi n^{3/2} + \sqrt{\log n} \sim 5n^3$.

Observation 1.3.3. $a_n \sim b_n$ and $b_n \sim c_n$ implies $a_n \sim c_n$, since $\frac{a_n}{c_n} = \frac{a_n}{b_n}\frac{b_n}{c_n}$.

Example 1.3.4 (Stirling's Formula).

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}. \tag{1.3.1}$$

Exercise 1.3.5. Show that

$$\binom{2n}{n} \sim c \cdot d^n \cdot n^b. \tag{1.3.2}$$

Also determine what c, d, and b are.

Another important question in mathematics is determining the frequency of prime numbers. To this end, we make the following definition:

Definition 1.3.6. $\pi(x) =$ the number of primes $\leq x$.

Example 1.3.7. For example, $\pi(10) = 4$: namely $2, 3, 5, 7$. Also, $\pi(100) = 25$ and $\pi(\pi) = 2$.

We now state one of the most beautiful results of all of mathematics:

Theorem 1.3.8 (Prime Number Theorem).

$$\pi(x) \sim \frac{x}{\ln x}. \tag{1.3.3}$$

This was conjectired by Gauss in the early 19th century and proved by Jacques Hadamard and Pierre de la Vallée-Poussin in 1894. (De la Vallée-Poussin was Belgian; Hadamard was French. In Hadamard's name, the "H" in the front and the "d" at the end are silent, presumably to confuse foreigners.) That is, the frequency of primes up to x is asymptotically $1/\ln x$:

$$\frac{\pi(x)}{x} \sim \frac{1}{\ln x}. \tag{1.3.4}$$

Example 1.3.9. The probability that a random 100-digit integer is prime, is about $\dfrac{1}{\ln 10^{100}} = \dfrac{1}{100 \ln 10} \approx \dfrac{1}{230}$.

Let us denote the n-th prime number by p_n.

Exercise 1.3.10. The Prime Number Theorem is equivalent to the asymptotic relation $p_n \sim n \ln n$.

Exercise 1.3.11. $\prod_{p<x} p$ is approximately equal to e^x; the exact meaning of this statement is that the logarithms of the two sides are asymptotically equal:

$$\sum_{p \le x} \ln p \sim x. \tag{1.3.5}$$

Using the Prime Number Theorem, one sees that

$$\sum_{p \text{ prime}} \frac{1}{p} = \infty. \tag{1.3.6}$$

In fact,

$$\sum_{p \le x} \frac{1}{p} \sim \ln \ln x. \tag{1.3.7}$$

This latter equation follows from the integral comparison test of calculus, using the version $p_n \sim n \ln n$ of PNT. We shall, however, prove the divergence of the series $\sum 1/p$ without using the PNT (below).

For the proof we shall need to know the rate at which the harmonic series $\sum 1/n$ diverges.

$$\sum_{k=1}^{n} \frac{1}{k} < 1 + \int_1^n \frac{dx}{x} = 1 + \ln n. \tag{1.3.8}$$

Similarly, we have the following comparison:

Exercise 1.3.12. $\sum_{k=1}^{n} \frac{1}{k} > \ln n$.

Corollary 1.3.13.

$$\ln n < \sum_{k=1}^{n} \frac{1}{k} < 1 + \ln n. \tag{1.3.9}$$

We can then use the Sandwich Theorem, (also known as the Two Policemen Theorem in Hungary, since "if two police officers converge to the station, then the suspect between them also converges to the station"), to show that the asymptotic equality

$$\sum_{k=1}^{n} \frac{1}{k} \sim \ln n. \tag{1.3.10}$$

Now let's compare this with the sum $\sum'$ of $\frac{1}{n}$ over all integers without the digit 8:

Exercise 1.3.14. $\sum' \frac{1}{n} < \infty$.

Exercise 1.3.15. In fact, $\sum'' \frac{1}{n} < \infty$, where the sum is over all integers without the string 2006.

Here is an interesting result:

Theorem 1.3.16 (Dirichlet's Theorem). *The sequence $an + b$ contains infinitely many prime numbers unless* $\gcd(a, b) \neq 1$.

Now we come to the first nontrivial proof:

Theorem 1.3.17.

$$\sum_{p \le n} \frac{1}{p} \ge \ln \ln n - 1. \tag{1.3.11}$$

Proof. We have

$$\ln n < \sum_{k=1}^{n} \frac{1}{k} < \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} = \prod_{p \le n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) = \sum{}''' \frac{1}{m}, \tag{1.3.12}$$

where the $\sum'''$ is the sum over all integers of which all prime divisors are $\le n$. To show the first equality, we use the geometric series $\dfrac{1}{1-x} = 1 + x + x^2 + \dots$. This equality then explains the second $<$ sign.

Next, taking ln of the above inequality, we have $\ln \ln n < -\sum_{p \le n} \ln\left(1 - \dfrac{1}{p}\right)$. We can now use the Taylor series, which says that $-\ln(1-x) = x + \dfrac{x^2}{2} + \dfrac{x^3}{3} + \dots$, if $|x| < 1$. So we get

$$\ln \ln n < \sum_{p \le n} \frac{1}{p} + \frac{1}{2} \sum_{p \le n} \frac{1}{p^2} + \frac{1}{3} \sum_{p \le n} \frac{1}{p^3} + \dots. \tag{1.3.13}$$

Using that $\sum_{p \le n} \dfrac{1}{p^2} < 1$ and similarly for p^3, etc., one gets

$$\ln \ln n < \sum_{p \le n} \frac{1}{p} + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots < \sum_{p \le n} \frac{1}{p} + 1. \tag{1.3.14}$$

This completes the proof. □

The following similar statement is more difficult to prove:

Exercise 1.3.18 (*).

$$\sum_{p \le n} \frac{1}{p} \sim \ln \ln n \tag{1.3.15}$$

Interlude: Paul Erdős and Paul Turán were both famous as high school students for sending in the most elegant solutions to problems designed for high schoolers. These problem contests promised to publish the most elegant solutions together with the authors' photographs, which provided great incentive to solve them. In college, Erdős was really intrigued to learn why the sum of the reciprocals of the primes diverges, since his father, who was also a mathematician, could not tell him. Erdős thus sought Turán, and upon recognizing his face from the contest photos exclaimed, "You are Turán! Tell me why the sum of the reciprocals of the primes diverges!" Thenceforth Erdős became the magician of prime numbers.

Around the end of World War II was a bad time to be in Hungary. Turán and Erdős were Jewish and were in danger. Anticipating this, Erdős had already left Hungary for the United States, but Turán remained in Hungary. Somehow he managed to escape from a cell and survive for a few days while the Nazis were driven out by the Soviets, but then he was captured by the Soviets and asked for his ID, which was a problem since it had been confiscated by the Nazis. However, he did carry a reprint of a paper published with Erdős in a Soviet journal, which he showed the officer instead. This publication by two Jewish Hungarians in a Soviet journal impressed the officer enough that he let Turán go. Subsequently Turán wrote to Erdős to tell him of his new, unexpected application of number theory.

Question 1.3.19. How fast can ν grow?

Let's consider $1, \dots, x$ with $1 < n < x$. To maximize ν, we want n to be a product of the primes up to some y. That is, $n := 2 \cdot 3 \cdot 5 \cdots = \prod_{p<y} p \le x$. Here we have by Exercise 1.3.11 that $\prod_{p<y} p \approx e^y$. Thus we should take $n := \prod_{p \le \ln x} p$, and then the Prime Number Theorem says that $\nu(n) = \pi(\ln x) \sim \dfrac{\ln x}{\ln \ln x}$.

Definition 1.3.20. $a_n \lesssim b_n$ if $a_n \sim \min\{a_n, b_n\}$.

This is called an **asymptotic inequality**. The discussion above motivates the following exercise:

Exercise 1.3.21. $\nu(n) \lesssim \dfrac{\ln n}{\ln \ln n}$

One may also show that the average value of $\nu(n)$ for $n \le x$ is $\ln \ln x$. Let's explore what this means and how to prove it. We will make use of δ-notation:

Definition 1.3.22.

$$\delta(\text{statement}) = \begin{cases} 1, & \text{if "statement" is TRUE;} \\ 0, & \text{otherwise.} \end{cases} \tag{1.3.16}$$

By definition we can thus see that

$$\nu(k) = \sum_p \delta(p \mid k), \tag{1.3.17}$$

where "$p \mid k$" means "p divides k", i.e. p is a divisor of k. Now, if n is an integer, then

$$\frac{1}{n}\sum_{k=1}^{n}\nu(k) = \frac{1}{n}\sum_{k=1}^{n}\sum_{p\leq n}\delta(p \mid k) = \frac{1}{n}\sum_{p\leq n}\sum_{k=1}^{n}\delta(p \mid k) = \frac{1}{n}\sum_{p\leq n}\frac{n}{\lfloor p\rfloor}, \tag{1.3.18}$$

where $\lfloor\cdot\rfloor$ is the **floor** or **greatest integer** function, returning the greatest integer $\leq$ the quantity inside.

Combining the above equalities with Theorem 1.3.17, we then have

$$\ln\ln n \sim \left(\sum_{p\leq n}\frac{1}{p}\right) - 1 = \frac{1}{n}\left(\sum_{p\leq n}\left(\frac{n}{p} - 1\right)\right) < \frac{1}{n}\sum_{k=1}^{n}\nu(k) < \frac{1}{n}\sum_{p\leq n}\frac{n}{p} = \sum_{p\leq n}\frac{1}{p} \sim \ln\ln n. \tag{1.3.19}$$

By the Two Policemen Theorem, all quantities in the above equation are asymptotic. In other words, we have just proved the following theorem about the average value of $\nu(n)$:

Theorem 1.3.23.

$$\frac{1}{n}\sum_{k=1}^{n}\nu(k) \sim \ln\ln n. \tag{1.3.20}$$

Exercise 1.3.24.

$$\frac{1}{n}\sum_{k=1}^{n}\nu^*(k) \sim \ln\ln n. \tag{1.3.21}$$

Exercise 1.3.25 (*). Prove that $\nu^*(n) \leq \log_2 n$.

Note that $\nu^*(n)$ can be as large as $\log_2(n)$, since $\nu^*(2^r) = r$.

Question 1.3.26. What can we say about the behavior of ν around the mean: does it deviate much?

The **standard deviation** is defined to answer precisely such questions. Hardy and Ramanujan computed the **variance** of ν, which is the square of the standard deviation:

Theorem 1.3.27. *(Hardy-Ramanujan)*

$$\frac{1}{n}\sum_{k=1}^{n}\big(\nu(k) - \ln\ln n\big)^2 \sim \ln\ln n. \tag{1.3.22}$$

Corollary 1.3.28. The standard deviation of $\nu(n)$ is $\sqrt{\ln\ln n}$.

Exercise 1.3.29 (*). Turán came up with a beautiful elementary proof of this Corollary. Now that you know it exists, you can find it!

In 1949, Erdős attended a lecture by Kac in which a conjecture was posed about the distribution of primes. After the lecture, Erdős approached Kac and said he thought he could prove the result, but just needed to know one thing. (This "one thing" was the Central Limit Theorem, which any mathematician would know.) After this and other contributions, they proved the result and published it in a joint paper. The theorem says that the distribution of primes is asymptotically normal, if you recenter the bell curve to have mean $\ln\ln n$ and standard deviation $\sqrt{\ln\ln n}$. One can get this bell curve by scaling x and renormalizing the function $\frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$.

Theorem 1.3.30. *(Erdős-Kac)*

$$\Pr_{k \le n}\left(\frac{\nu(k) - \ln\ln n}{\sqrt{\ln\ln n}} < x\right) \sim \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt. \tag{1.3.23}$$

This says that the ν function behaves as the sum of small independent quantities. This makes sense because the event of being divisible by 2, 3, 5, etc., are basically independent. But how far can that go? Only up to log, and so the proof of this is quite difficult: even taking the larger prime numbers into account, as a whole, it still behaves as if divisibility were independent events.

1.4 More Arithmetic Functions

Definition 1.4.1. We define **Euler's φ function** as follows:

$$\varphi(n) = \#\{k : 1 \le k \le n \text{ and } \gcd(k, n) = 1\}. \tag{1.4.1}$$

Note that we have the following equality:

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{1.4.2}$$

Example 1.4.2. $\varphi(p) = p - 1$ and $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

Exercise 1.4.3. φ is multiplicative. That is, if $\gcd(a, b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$.

As a result, we conclude that if $n = \prod_{i=1}^{r} p_i^{k_i}$, then

$$\varphi(n) = \prod_{i=1}^{r} p_i^{k_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \tag{1.4.3}$$

Now, $\Pr_{1 \le k \le n}(\gcd(k, n) = 1) = \frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right)$.

Question 1.4.4. Can the product $\prod_{p|n}\left(1-\frac{1}{p}\right)$ be less than $\frac{1}{100}$?

Since $n := \prod_{p\le x} p \approx e^x$, then we see that

$$\frac{\varphi(n)}{n} = \prod_{p\le x}\left(1-\frac{1}{p}\right) \tag{1.4.4}$$

Exercise 1.4.5 (Important Exercise!). Does

$$\prod_{p}\left(1-\frac{1}{p}\right) = 0\ ? \tag{1.4.5}$$

Exercise 1.4.6. Show that

$$\lim_{n\to\infty}\frac{\sum_{k=1}^{n}\varphi(k)}{n^2} = \frac{3}{\pi^2} = \frac{1}{2\zeta(2)}. \tag{1.4.6}$$

HINT: Prove this under the assumption that the limit exists.

Definition 1.4.7. Define $F(n) := \sum_{k|n}\varphi(k)$.

Example 1.4.8. For example, $F(6) = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(6) = 1+1+2+2 = 6$. Also, $F(7) = \varphi(1)+\varphi(7) = 1+6 = 7$.

Exercise 1.4.9. Show $F(n) = n$.

Definition 1.4.10. Define $f(n) := \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$

If we have a function g such that

$$f(n) = \sum_{d|n} g(d), \tag{1.4.7}$$

then $1 = f(1) = g(1)$. Furthermore, $0 = f(p) = g(1) + g(p)$ implies that $g(p) = -1$ for any prime p. Similarly, $0 = f(pq) = g(1)+g(p)+g(q)+g(pq) = 1-2+g(pq)$ implies $g(pq) = 1$. One also obtains $g(pqr) = -1$ and $g(p^2) = 0$ in a similar manner.

So in fact g is the **Moebius function**, μ ("mu"), which is defined as follows:

Definition 1.4.11.

$$\mu(n) := \begin{cases} (-1)^{\nu(n)}, & \text{if } n \text{ is square-free,} \\ 0, & \text{otherwise.} \end{cases} \tag{1.4.8}$$

We can then see that

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{1.4.9}$$

The above observation naturally leads to *Moebius Inversion*.

Theorem 1.4.12. *Suppose $F : \mathbb{Z}^+ \to \mathbb{C}$ and $G(n) := \sum_{d|n} F(d)$. Then*

$$F(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) G(d). \tag{1.4.10}$$

Exercise 1.4.13. If F is multiplicative, show that so is G, and vice-versa.

Exercise 1.4.14. Deduce from Moebius inversion that

1. $\varphi(n) = n \prod \left(1 - \frac{1}{p}\right)$;
2. φ is multiplicative.

Exercise 1.4.15. Contemplate

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n}. \tag{1.4.11}$$

Is there any convergence?

Recall the definition of the zeta function, $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Exercise 1.4.16. Show that $\zeta(s)(\zeta(s) - 1) = \sum \frac{\sigma(n)}{n^s}$, recalling that $\sigma(n)$ is the sum of divisors.

Exercise 1.4.17. $\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$.

Exercise 1.4.18. $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$.

Exercise 1.4.19. $(\zeta(s))^2 = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}$.

Definition 1.4.20. A *partition* of a positive integer n is a representation of n as a sum of positive integers: $n = x_1 + \cdots + x_k$, where $x_1 \leq \cdots \leq x_k$.

Example 1.4.21. A partition here is something like $7 = 1 + 1 + 2 + 3$. For other examples, refer to Handout 2, Definition 2.2.14.

Definition 1.4.22. Define the **partition function**, $p(n)$, to be the number of partitions of n.

A very nontrivial result of Hardy-Ramanujan describes the growth of $p(n)$:

Theorem 1.4.23 (Hardy-Ramanujan Formula).

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\sqrt{\frac{2}{3}}\pi\sqrt{n}}. \tag{1.4.12}$$

The important thing is the form $\frac{c_1}{n} e^{c_2\sqrt{n}}$. This theorem is difficult, but the following exercise should take only 15 minutes:

Exercise 1.4.24. Prove that there exists c, d such that $e^{c\sqrt{n}} < p(n) < e^{d\sqrt{n}}$, for large n.

As a step toward proving the Hardy-Ramanujan Formula, we shall show next time that

$$p(n) < e^{\sqrt{\frac{2}{3}}\pi\sqrt{n}}. \tag{1.4.13}$$