Honors 1: Undergraduate Math Lab*

Peter Sarnak†, Steven Miller‡, Alex Barnett§

September 11th, 2002

Courant Institute of Mathematical Sciences
New York University
New York, NY

Abstract

We review many basic number theory results. We give efficient algorithms for polynomial evaluation, calculating x^n, and finding the greatest common divisor. We briefly review probability theory. After an introduction to Algebraic and Transcendental Numbers, we review Dirichlet's Box Principle (aka the Pidgeonhole Principle), and give an application. We prove a weak version of Chebyshev's Theorem on the approximate number of primes. Lecture by Steven Miller. Notes by Steven Miller (and Florin Spinu, who helped write up the notes on Dirichlet's Box Principle and Chebyshev).

1 Notation

1. $\mathbb{W}$: the set of whole numbers: $\{1, 2, 3, 4, \dots\}$.
2. $\mathbb{N}$: the set of natural numbers: $\{0, 1, 2, 3, \dots\}$.
3. $\mathbb{Z}$: the set of integers: $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
4. $\mathbb{Q}$: the set of rational numbers: $\{x : x = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0\}$.

---

*Homepage: `http://www.math.nyu.edu/~millerj/`

†E-mail: `sarnak@math.princeton.edu`

‡E-mail: `millerj@cims.nyu.edu` or `sjmiller@math.princeton.edu`

§E-mail: `barnett@nmr.mgh.harvard.edu`

5. $\mathbb{R}$: the set of real numbers.

6. $\mathbb{C}$: the set of complex numbers: $\{z : z = x + iy,\ x, y \in \mathbb{R}\}$.

7. $\mathbb{Z}/n\mathbb{Z}$: the additive group of integers mod n.

8. $(\mathbb{Z}/n\mathbb{Z})^*$: the multiplicative group of invertible elements mod n.

9. $a|b$: a divides b, *i.e.* the remainder after integer division $\frac{b}{a}$ is 0.

10. (a, b) : greatest common divisor (gcd) of a and b, often written $\gcd(a, b)$.

11. $x \equiv y \pmod{n}$: there exists an integer a such that $x = y + an$.

12. wlog : without loss of generality.

13. s.t. : such that.

14. $\forall$: for all.

15. $\exists$: there exists.

16. big O notation : $A(x) = O(B(x))$, read "$A(x)$ is of order $B(x)$", means $\exists C > 0$ such that $\forall x, |A(x)| \leq C\, B(x)$.

17. $|S|$ or $\#S$: number of elements in the set S.

18. p : usually a prime number.

19. n : usually an integer.

2 Efficient Algorithms

For computational purposes, often having an algorithm to compute a quantity is not enough; we need an algorithm which will compute *quickly*. Below we study three standard problems, and show how to either rearrange the operations more efficiently, or give a more efficient algorithm than the obvious candidate.

2.1 Polynomial Evaluation

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The obvious way to evaluate is to calculate x^n and multiply by a_n (n multiplications), calculate x^{n-1} and multiply by a_{n-1} ($n-1$ multiplications) and add, et cetera. There are n additions and $\sum_{k=0}^{n} k$ multiplications, for a total of $n + \frac{n(n+1)}{2}$ operations. Thus, the standard method leads to $O(n^2)$ computations.

Instead, consider the following:

$$\Bigg(\bigg((a_n x + a_{n-1})x + a_{n-2}\bigg)x + \cdots + a_1\Bigg)x + a_0. \tag{1}$$

For example,

$$7x^4 + 4x^3 - 3x^2 - 11x + 2 = \Bigg(\bigg((7x+4)x - 3\bigg)x - 11\Bigg)x + 2. \tag{2}$$

Evaluating the long way takes 14 steps; cleverly rearranging takes 8 steps.

Exercise 1 *Prove that the second method takes at most* $2n$ *steps to evaluate* $a_n x^n + \cdots a_0$.

2.2 Exponentiation

Consider x^n. The obvious way to evaluate involves $n-1$ multiplications. By writing n in base two, we can evaluate x^n in at most $2\log_2 n$ steps.

Let k be the largest integer such that $2^k \leq n$. Then $\exists a_i \in \{0,1\}$ such that

$$n = a_k 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2 + a_0. \tag{3}$$

It costs k multiplications to evaluate x^{2^i}, $i \leq k$. How? Consider $y_0 = x^{2^0}$, $y_1 = y_0 \cdot y_0 = x^{2^0} \cdot x^{2^0} = x^{2^1}$, $y_2 = y_1 \cdot y_1 = x^{2^2}$, ..., $y_k = y^{k-1} \cdot y^{k-1} = x^{2^k}$.

Then

$$\begin{aligned} x^n &= x^{a_k 2^k + a_{k-1}2^{k-1} + \cdots + a_1 2 + a_0} \\ &= x^{a_k 2^k} \cdot x^{a_{k-1}2^{k-1}} \cdots x^{a_1 2} \cdot x^{a_0} \\ &= \left(x^{2^k}\right)^{a_k} \cdot \left(x^{2^{k-1}}\right)^{a_{k-1}} \cdots \left(x^2\right)^{a_1} \cdot \left(x^1\right)^{a_0} \\ &= y_k^{a_k} \cdot y_{k-1}^{a_{k-1}} \cdots y_1^{a_1} \cdot y_0^{a_0}. \end{aligned} \tag{4}$$

As each $a_i \in \{0, 1\}$, we have at most $k+1$ multiplications above (if $a_i = 1$ we have the term y_i in the product, if $a_i = 0$ we don't).

Thus, it costs k multiplications to evaluate the x^{2^i} $(i \leq k)$, and at most another k multiplications to finish calculating x^n. As $k \leq \log_2 n$, we see that x^n can be determined in at most $2 \log_2 n$ steps.

Note, however, that we do need more storage space for this method, as we need to store the values $y_i = x^{2^i}$, $i \leq \log_2 n$.

Exercise 2 *Instead of expanding n in base two, expand n in base three. How many calculations are needed to evaluate x^n this way? Why is it preferable to expand in base two rather than any other base?*

2.3 Euclidean Algorithm

The Euclidean Algorithm is an efficient way to determine the greatest common divisor of x and y, denoted $\gcd(x, y)$ or (x, y). Without loss of generality, assume $1 < x < y$.

The obvious way to determine $\gcd(x, y)$ is to divide x and y by all positive integers up to x. This takes at most $2x$ steps.

Let $[z]$ denote the greatest integer less than or equal to z. We write

$$y = \left[\frac{y}{x}\right] \cdot x + r_1, \ 0 \leq r_1 < x. \tag{5}$$

Exercise 3 *Prove that* $r_1 \in \{0, 1, \dots, x - 1\}$.

Exercise 4 *Prove* $\gcd(x, y) = \gcd(r_1, x)$. *Hint:* $r_1 = y - \left[\frac{y}{x}\right] \cdot x$.

We proceed in this manner until r_k equals zero or one. As each execution results in $r_i < r_{i-1}$, we proceed at most x times (although later we prove we need to apply these steps at most $2 \log_2 x$ times).

$$\begin{aligned}
x &= \left[\frac{x}{r_1}\right] \cdot r_1 + r_2, \ 0 \leq r_2 < r_1 \\
r_1 &= \left[\frac{r_1}{r_2}\right] \cdot r_2 + r_3, \ 0 \leq r_3 < r_2 \\
r_2 &= \left[\frac{r_2}{r_3}\right] \cdot r_3 + r_4, \ 0 \leq r_4 < r_3
\end{aligned}$$

$$\vdots$$

$$r_{k-2} = \left[\frac{r_{k-2}}{r_{k-1}}\right] \cdot r_{k-1} + r_k, \ 0 \leq r_k < r_{k-1}. \tag{6}$$

Exercise 5 *Prove that if* $r_k = 0$*, then* $\gcd(x, y) = r_{k-1}$*, while if* $r_k = 1$*, then* $\gcd(x, y) = 1$.

We now analyze how large k can be. The key observation is the following:

Lemma 2.1 *Consider three adjacent remainders in the expansion:* r_{i-1}*,* r_i *and* r_{i+1} *(where* $y = r_{-1}$ *and* $x = r_0$*). Then* $\gcd(r_i, r_{i-1}) = \gcd(r_{i+1}, r_i)$*, and* $r_{i+1} < \frac{r_{i-1}}{2}$.

Proof: We have the following relation:

$$r_{i-1} = \left[\frac{r_{i-1}}{r_i}\right] \cdot r_i + r_{i+1}, \ 0 \leq r_{i+1} < r_i. \tag{7}$$

If $r_i \leq \frac{r_{i-1}}{2}$, then as $r_{i+1} < r_i$, we immediately conclude that $r_{i+1} < r_i$. If $r_i > \frac{r_{i-1}}{2}$, then we note that

$$r_{i+1} = r_{i-1} - \left[\frac{r_{i-1}}{r_i}\right] \cdot r_i. \tag{8}$$

But $\left[\frac{r_{i-1}}{r_i}\right] = 1$ (easy exercise). Thus $r_{i-1} < \frac{r_{i-1}}{2}$. $\Box$

We count how often we apply Euclid's Algorithm. Going from $(x, y) = (r_0, r_{-1})$ to (r_1, r_0) costs one application. Every two applications leads to the first entry in the last pair being at most half of the second entry of the first pair.

Thus, if k is the largest integer such that $2^k \leq x$, we see we apply Euclid's Algorithm at most $1 + 2k \leq 1 + 2\log_2 x$ times. Each application requires one integer division, where the remainder is the input for the next step.

We have proven

Lemma 2.2 *Euclid's Algorithm requires at most* $1 + 2\log_2 x$ *divisions to find the greatest common denominator of* x *and* y.

Let us assume that $r_i = \gcd(x, y)$. Thus, the last equation before Euclid's Algorithm terminated was

$$r_{i-2} = \left[\frac{r_{i-2}}{r_{i-1}}\right] \cdot r_{i-1} + r_i, \ 0 \le r_i < r_{i-1}. \tag{9}$$

Therefore, we can find integers a_{i-1} and b_{i-2} such that

$$r_i = a_{i-1} r_{i-1} + b_{i-2} r_{i-2}. \tag{10}$$

Looking at the second to last application of Euclid's algorithm, we find that there are integers a'_{i-2} and b'_{i-3} such that

$$r_{i-1} = a'_{i-2} r_{i-2} + b'_{i-3} r_{i-3}. \tag{11}$$

Substituting for $r_{i-1} = r_{i-1}(r_{i-2}, r_{i-3})$ in the expansion of r_i yields that there are integers a_{i-2} and b_{i-3} such that

$$r_i = a_{i-2} r_{i-2} + b_{i-3} r_{i-3}. \tag{12}$$

Continuing by induction, and recalling $r_i = \gcd(x, y)$ yields

Lemma 2.3 *There exist integers a and b such that $\gcd(x, y) = ax + by$. Moreover, Euclid's Algorithm gives a constructive procedure to find a and b.*

Exercise 6 *Find a and b such that $a \cdot 244 + b \cdot 313 = \gcd(244, 313)$.*

Exercise 7 *Add details to complete an alternate proof of the existence of a and b with $ax + by = \gcd(x, y)$:*

1. *Let d be the smallest positive value attained by $ax + by$ as we vary $a, b \in \mathbb{Z}$. Such a d exists: consider $(a, b) = (1, 0)$ or $(0, 1)$. Thus, $d = ax + by$. We now show $d = \gcd(x, y)$.*

2. *$\gcd(x, y) | d$.*

3. *Let $e = Ax + By > 0$. Then $d | e$. Therefore, for any choice of $A, B \in \mathbb{Z}$, $d | (Ax + By)$.*

4. *$d | x$ and $d | y$ (consider clever choices of A and B; one choice gives $d | x$, one gives $d | y$). Therefore $d | \gcd(x, y)$. As we've shown $\gcd(x, y) | d$, this completes the proof.*

Note this is a non-constructive proof. By minimizing $ax + by$, we obtain $\gcd(x, y)$*, but we have no idea how many steps is required. Prove that a solution will be found either among pairs (a, b) with $a \in \{1, \ldots, y-1\}$ and $-b \in \{1, \ldots, x-1\}$, or $-a \in \{1, \ldots, y-1\}$ and $b \in \{1, \ldots, x-1\}$.*

3 Probabilities of Discrete Events

3.1 Introduction

Let $\Omega = \{\omega_1, \omega_2, \omega_3, \ldots\}$ be an at most countable set of events. We call Ω the **sample (or outcome) space**. We call the elements $\omega \in \Omega$ the **events**. Let $x : \Omega \to \mathbb{R}$. That is, for each event $\omega \in \Omega$, we attach a real number $x(\omega)$. We call x a **random variable**.

Example 3.1 *Flip a fair coin 3 times. The possible outcomes are $\Omega = \{HHH, HHT, HTH, THH, HTT, THT, TTH, TTT\}$. One possible random variable is $x(\omega)$ equals the number of heads in ω. Thus, $x(HHT) = 2$ and $x(TTT) = 0$.*

Example 3.2 *Let Ω be the space of all flips of a fair coin where all but the last flip are tails, and the last is a head. Thus, $\Omega = \{H, TH, TTH, TTTH, \ldots\}$. One possible random variable is $x(\omega)$ is the number of tails; another is $x(\omega)$ equals the number of the flip which is a head.*

We say $p(\omega)$ is a **probability function** on Ω if

1. $0 \leq p(\omega_i) \leq 1$ for all $\omega_i \in \Omega$.

2. $p(\omega) = 0$ if $\omega \notin \Omega$.

3. $\sum_i p(\omega_i) = 1$.

We call $p(\omega)$ the probability of event ω.

Often, we have a random variables where $x(\omega) = \omega$. In a convenient abuse of notation, we write X for Ω and x for $x(\omega)$ and ω. For example, consider two rolls of a fair die. Let X be the result of the first roll, and Y of the second. Then the sample space is $X = Y = \{1, 2, 3, 4, 5, 6\}$.

In general, consider X and Y with x_i occurring with probability $p(x_i)$ and y_j occurring with probability $q(y_j)$. We analyze the **joint probability** $r(x, y)$ of observing x and y.

X and Y are **independent** if $\forall x, y,\ r(x,y) = p(x)q(y)$. In the example of rolling a fair die twice, $r(x,y) = p(x)q(y) = \frac{1}{6} \cdot \frac{1}{6}$ if $x, y \in X = Y$, and 0 otherwise.

Exercise 8 *Consider again two rolls of a fair die. Now, let X represent the first roll, and Y the sum of the first two rolls. Prove X and Y are not independent.*

Events X_1 through X_N are **independent** if $p(x_1, \ldots, x_N) = p_1(x_1) \cdots p(x_N)$.

Exercise 9 *Construct three events such that any two are independent, but all three are not independent. Hint: roll a fair die twice.*

3.2 Means

If $x(\omega) = \omega$, the **mean (or expected value)** of an event x is defined by

$$\bar{x} \; = \; \sum_i x_i p(x_i). \tag{13}$$

More generally, for a sample space Ω with events ω and a random variable $x(\omega)$, we have

$$\bar{x}(\omega) \; = \; \sum_i x(\omega_i) p(\omega_i). \tag{14}$$

For example, the mean of one roll of a fair die is 3.5.

Exercise 10 *Let X be the number of tosses of a fair coin needed before getting the first head. Thus, $X = \{1, 2, \ldots\}$. Calculate $p(x_i)$ and $\bar{x}$. We could let Ω be the space of all tosses of a fair coin where all but the last toss are tails, and the last toss is a head. Then $x(\omega)$ is the number of tosses of ω.*

Instead of writing $\bar{x}$, we often write $E[x]$ or $E[X]$, read as **the expected value of x or X**. More generally, we would have $\bar{x}(\omega)$ and $E[x(\omega)]$.

The k^{th} moment of X is the expected value of x^k:

$$E[x^k] \; = \; \sum_i x_i^k p(x_i) \tag{15}$$

or

$$E[x^k(\omega)] \; = \; \sum_i x^k(\omega_i) p(\omega_i). \tag{16}$$

Lemma 3.3 (Additivity of the Means) *Let X and Y be two independent events with joint probability $r(x,y) = p(x)q(y)$. Let $z = x + y$. Then $E[z] = E[x+y] = E[x] + E[y]$.*

Proof:

$$\begin{aligned}
E[x+y] &= \sum_{(i,j)} (x_i + y_j) r(x_i, y_j) \\
&= \sum_i \sum_j (x_i + y_j) p(x_i) q(y_j) \\
&= \sum_i \sum_j x_i p(x_i) q(y_j) + \sum_i \sum_j y_j p(x_i) q(y_j) \\
&= \sum_i x_i p(x_i) \sum_j q(y_j) + \sum_i p(x_i) \sum_j y_j q(y_j) \\
&= E[x] \cdot 1 + 1 \cdot E[y] = E[x] + E[y]. \qquad (17)
\end{aligned}$$

The astute reader may notice that some care is needed to interchange the order of summations. If $\sum_i \sum_j |x_i y_j| r(x_i, y_j) < \infty$, then Fubini's Theorem is applicable, and we may interchange the summations at will.

We used the two events were independent to go from $\sum_{(i,j)} x_i r(x_i, y_j)$ to $\sum_i x_i p(x_i) \sum_j q(y_j) = E[x]$. Lemma 3.3 is true even if the two events are not independent.

If the events are not independent, we encounter sums like $\sum_i \sum_j x_i r(x_i, y_j)$; however, $\sum_j r(x_i, y_j) = p(x_i)$. Why? By summing over all possible y, we are asking what is the probability that $x = x_i$; we do not care what y is. Thus, $\sum_i \sum_j x_i r(x_i, y_j) = \sum_i x_i p(x_i) = E[x]$, and similarly for the other piece.

Exercise 11 *Write out the proof of the generalization of Lemma 3.3, where X and Y are not assumed independent.*

Given an outcome space $X = \{x_1, x_2, \dots\}$ with probabilities $p(x_i)$, let aX be shorthand for the event a times X with outcome space $\{ax_1, ax_2, \dots\}$ and probabilities $p_a(ax_i) = p(x_i)$.

Lemma 3.4 *Let X_1 through X_N be a finite collection of independent events. Let a_1 through a_N be real constants. Then*

$$E[a_1 x_1 + \cdots + a_N x_N] = a_1 E[x_1] + \cdots + a_N E[x_N]. \qquad (18)$$

Lemma 3.5 *Let X and Y be independent events. Then $E[xy] = E[x]E[y]$.*

Exercise 12 *Prove Lemmas 3.4 and 3.5.*

3.3 Variances

The **variance** σ_x^2 (and its square-root, the **standard deviation** σ_x) measure how spread out a probability distribution is. Assume $x(\omega) = \omega$. Given an event X with mean $\bar{x}$, we define the standard deviation σ_x^2 by

$$\sigma_x^2 \;=\; \sum_i (x_i - \bar{x})p(x_i). \tag{19}$$

More generally, given a sample space Ω, events ω, and a random variable $x : \Omega \to \mathbb{R}$,

$$\sigma^2_{x(\omega)} \;=\; \sum_i \Big(x(\omega_i) - \bar{x}(\omega)\Big)p(\omega_i). \tag{20}$$

Exercise 13 *Let* $X = \{0, 25, 50, 75, 100\}$ *with probabilities* $\{.2, .2, .2, .2, .2\}$. *Let* Y *be the same outcome space, but with probabilities* $\{.1, .25, .3, .25, .1\}$. *Calculate the means and the variances of* X *and* Y.

For computing variances, instead of equation 19 one often uses

Lemma 3.6 $\sigma_x^2 = E[x^2] - E[x]^2$.

Proof: Recall $\bar{x} = E[x]$. Then

$$\begin{aligned}
\sigma_x^2 &= \sum_i \Big(x_i - E[x]\Big)^2 p(x_i) \\
&= \sum_i (x_i^2 - 2x_iE[x] + E[x]^2)p(x_i) \\
&= \sum_i x_i^2 p(x_i) - 2E[x]\sum_i x_i p(x_i) + E[x]^2 \sum_i p(x_i) \\
&= E[x^2] - 2E[x]^2 + E[x]^2 = E[x^2] - E[x]^2. \qquad (21)
\end{aligned}$$

The main result on variances is

Lemma 3.7 (Variance of a Sum) *Let* X *and* Y *be two independent events. Then* $\sigma^2_{x+y} = \sigma_x^2 + \sigma_y^2$.

Proof: We constantly use the expected value of a sum of independent events is the sum of expected values (Lemma 3.3 and Lemma 3.4).

$$\begin{aligned}
\sigma_{x+y}^2 &= E[(x+y)^2] - E[(x+y)]^2 \\
&= E[x^2 + 2xy + y^2] - \Big(E[x] + E[y]\Big)^2 \\
&= \Big(E[x^2] + 2E[xy] + E[y^2]\Big) - \Big(E[x]^2 + 2E[x]E[y] + E[y]^2\Big) \\
&= \Big(E[x^2] - E[x]^2\Big) + \Big(E[y^2] - E[y]^2\Big) + 2\Big(E[xy] - E[x]E[y]\Big) \\
&= \sigma_x^2 + \sigma_y^2 + 2\Big(E[xy] - E[x]E[y]\Big). \qquad (22)
\end{aligned}$$

By Lemma 3.5, $E[xy] = E[x]E[y]$, completing the proof.

Lemma 3.8 *Consider n independent copies of the same event (for example, n flips of a coin or n rolls of a die). Then $\sigma_{nx} = \sqrt{n}\sigma_x$.*

Exercise 14 *Prove Lemma 3.8.*

Note that, if the event X has units of meters, then the variance σ_x^2 has units meters-squared, and the standard deviation σ_x and the mean $\bar{x}$ have units meters. Thus, it is the standard deviation that gives a good measure of the deviations of an event around the mean.

There are, of course, alternate measures one can use. For example, one could consider

$$\sum_i (x_i - \bar{x}) p(x_i). \qquad (23)$$

Unfortunately, this is a signed quantity, and large positive deviations can cancel with large negatives. This leads us to consider

$$\sum_i |x_i - \bar{x}| p(x_i). \qquad (24)$$

While this has the advantage of avoiding cancellation of errors (as well as having the same units as the events), the absolute value function is not a good function analytically. For example, it is not differentiable. This is primarily why we consider the standard deviation (the square-root of the variance).

Exercise 15 *Consider the following set of data: for $i \in \{1, \dots, n\}$, given x_i one observes y_i. Believing that X and Y are linearly related, find the best fit straight line. Namely, determine constants a and b that minimize the error (calculated via the variance)*

$$\sum_{i=1}^{n} \Big(y_i - (ax_i + b)\Big)^2 \;=\; \sum_{i=1}^{n} \Big(Observed_i - Predicted_i\Big)^2. \tag{25}$$

Hint: use Multi-variable Calculus to find linear equations for a and b, and then solve with Linear Algebra.

If instead of measuring total error by the squares of the individual error (for example, using the absolute value), closed form expressions for a and b become significantly harder.

If one requires that $a = 0$, show that the b leading to least error is $b = \bar{y} = \frac{1}{n}\sum_i y_i$.

3.4 Random Walks

Consider the classical problem of a drunk staggering home from a lamp post late at night. We flip a fair coin N times. With probability $\frac{1}{2}$ we get heads (tails). For each head (tail) the drunk staggers one unit to the right (left). How far do we expect the drunk to be?

It is very unlikely the drunk will be very far to the left or right.

Exercise 16 *Let x be $+1$ if we flip a head, -1 for a tail. For a fair coin, prove $E[x] = 0$, $\sigma_x^2 = 1$, $\sigma_x = 1$.*

Exercise 17 *Let $p_N(y)$ be the probability that after N flips of a fair coin, the drunk is y units to the right of the origin (lamp post).*

1. *Prove $p_N(y) = p_N(-y)$.*
2. *Consider $N = 2M$. Prove $p_{2M}(2k) = \binom{2M}{M+k}\frac{1}{2^{2M}}$, where $\binom{n}{r} = \frac{n!}{r!(n-r)!}$*
3. *Use Stirling's formula ($n! \approx n^n e^{-n}\sqrt{2\pi n} = \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n}$) to approximate $p_N(y)$.*

Label the coin tosses X_1 through X_N. Let X denote a generic toss of the coin, and Y_N be the distance of the drunkard after N tosses. By Lemma 3.4,

$E[y_N] = E[x_1 + \cdots + x_N] = E[x_1] + \cdots + E[x_N]$. As each $E[x_i] = E[x] = 0$, $E[y_N] = 0$.

Thus, we expect the drunkard to be at the lamp post. How spread out is his expected position? By Lemma 3.8,

$$\sigma_{y_N} = \sigma_{Nx} = \sqrt{N}\sigma_x = \sqrt{N}. \tag{26}$$

This means that a *typical* distance from the origin is $\sqrt{N}$. This is called a *diffusion process* and is very common in the real world.

3.5 Bernoulli Process

Recall $\binom{N}{r} = \frac{N!}{r!(N-r)!}$ is the number of ways to choose r objects from N objects when order does not matter. Consider n independent repetitions of an event with only two possible outcomes. We typically call one outcome **success** and the other **failure**, the event a **Bernoulli Trial**, and a collection of independent Bernoulli Trials a **Bernoulli Process**.

In each Bernoulli Trial, let there be probability p of success and $q = 1-p$ of failure. Often, we represent a success with 1 and a failure with 0.

Exercise 18 *For a Bernoulli Trial, show $\bar{x} = p$, $\sigma_x^2 = pq$, and $\sigma_x = \sqrt{pq}$.*

Let Y_N be the number of successes in N trials. Clearly, the possible values are $Y_N = \{0, 1, \cdots, N\}$. We analyze $p_N(k)$. Rigorously, the sample space Ω is all possible sequences of N trials, and the random variable $y_N : \Omega \to \mathbb{R}$ is given by $y_N(\omega)$ equals the number of successes in ω.

If $k \in Y_N$, we need k successes and $N-k$ failures. We don't care what order we have them (ie, if $k = 4$ and $N = 6$ then $SSFSSF$ and $FSSSSF$ both contribute). Each such string of k successes and $N-k$ failures has probability of $p^k \cdot (1-p)^{N-k}$. There are $\binom{N}{k}$ such strings.

Thus, $p_N(k) = \binom{N}{k} p^k \cdot (1-p)^{N-k}$ if $k \in \{0, 1, \cdots, N\}$ and 0 otherwise.

By clever algebraic manipulations, one can directly evaluate the mean $\overline{y_N}$ and the variance $\sigma_{y_N}^2$; however, Lemmas 3.4 and 3.8 allow one to calculate both quantities immediately, once one knows the mean and variance for one occurrence.

Lemma 3.9 *For a Bernouilli Process with N trials, each having probability p of success, the expected number of successes is $\overline{y_N} = Np$, and the variance is $\sigma_{y_N}^2 = Npq$.*

Exercise 19 *Prove Lemma 3.9.*

Consider the following problem: Let $Z = \{0, 1, 2, \ldots\}$ be the number of trials before the first success. What is $\bar{z}$ and σ_z^2?

First, we determine $p(k)$, the probability that the first success occurs after k trials. Clearly this probability is non-zero only for k a positive integer, in which case the string of results must be $k-1$ failures followed by 1 success. Therefore,

$$p(k) \;=\; p \cdot (1-p)^{k-1} \text{ if } k \in \{1, 2, \ldots\}, \text{ and 0 otherwise.} \tag{27}$$

To determine the mean $\bar{z}$ we must evaluate

$$\begin{aligned} \bar{z} &= \sum_{k=1}^{\infty} k \cdot p \cdot (1-p)^{k-1} \\ &= p \sum_{k=1}^{\infty} k q^{k-1}, \;\; 0 < q = 1-p < 1. \end{aligned} \tag{28}$$

Consider the geometric series

$$f(q) \;=\; \sum_{k=0}^{\infty} q^k \;=\; \frac{1}{1-q}. \tag{29}$$

A careful analysis shows we can differentiate term by term if $0 \le q < 1$. Then

$$f'(q) \;=\; \sum_{k=0}^{\infty} k q^{k-1} \;=\; \frac{1}{(1-q)^2}. \tag{30}$$

Recalling $q = 1-p$ and substituting yields

$$\begin{aligned} \bar{z} &= p \sum_{k=1}^{\infty} k q^{k-1} \\ &= \frac{p}{\big(1-(1-p)\big)^2} \;=\; \frac{1}{p}. \end{aligned} \tag{31}$$

Differentiating under the summation sign is a powerful tool in Probability Theory.

Exercise 20 *Calculate σ_z^2. Hint: differentiate $f(q)$ twice.*

3.6 Poisson Distribution

Divide the unit interval into N equal pieces. Consider N independent Bernoulli Trials, one for each sub-interval. If the probability of a success is $\frac{\lambda}{N}$, then by Lemma 3.9 the expected number of successes is $N \cdot \frac{\lambda}{N} = \lambda$.

We consider the limit as $N \to \infty$. Obviously, we still expect λ successes in each interval, but what is the probability of 3λ successes? How long do we expect to wait between successes?

We call this a **Poisson process with parameter** λ. For example, look at the midpoints of the N intervals. At each midpoint we have a Bernoulli Trial with probability of success $\frac{\lambda}{N}$ and failure $1 - \frac{\lambda}{N}$.

We determine the $N \to \infty$ limits. For fixed N, the probability of k successes in a unit interval is

$$\begin{aligned} p_N(k) &= \binom{N}{k} \Big(\frac{\lambda}{N}\Big)^k \Big(1 - \frac{\lambda}{N}\Big)^{N-k} \\ &= \frac{N!}{k!(N-k)!} \frac{\lambda^k}{N^k} \Big(1 - \frac{\lambda}{N}\Big)^{N-k} \\ &= \frac{N \cdot (N-1) \cdots (N-k+1)}{N \cdot N \cdots N} \frac{\lambda^k}{k!} \Big(1 - \frac{\lambda}{N}\Big)^N \Big(1 - \frac{\lambda}{N}\Big)^{-k} \\ &= 1 \cdot \Big(1 - \frac{1}{N}\Big) \cdots \Big(1 - \frac{k-1}{N}\Big) \frac{\lambda^k}{k!} \Big(1 - \frac{\lambda}{N}\Big)^N \Big(1 - \frac{\lambda}{N}\Big)^{-k}. \end{aligned} \tag{32}$$

For fixed, finite k, as $N \to \infty$, the first k factors in $p_N(k)$ tend to 1, $\left(1 - \frac{\lambda}{N}\right)^N \to e^{-\lambda}$, and $\left(1 - \frac{\lambda}{N}\right)^{-k} \to 1$.

Thus, we are led to the **Poisson Distribution**: Given a parameter λ (interpreted as the expected number of occurrences per unit interval), the probability of k occurrences in a unit interval is $p(k) = \frac{\lambda^k}{k!} e^{-\lambda}$ for $k \in \{0, 1, 2, \ldots\}$.

Exercise 21 *Check that $p(k)$ given above is a probability distribution. Namely, show $\sum_{k \geq 0} p(k) = 1$.*

Exercise 22 *Show, for the Poisson Distribution, that the mean $\bar{x} = \lambda$ and the variance $\sigma_x^2 = \lambda$. Hint: let*

$$f(\lambda) = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} = e^{\lambda}. \tag{33}$$

Differentiate once to determine the mean, twice to determine the variance.

3.7 Continuous Poisson Distribution

We calculate a very important quantity related to the Poisson Distribution (with parameter λ), namely, how long does one expect to wait between successes?

We've discussed that we expect λ successes per unit interval, and we've calculated the probability of k successes per unit interval.

Start counting at 0, and assume the first success is at x. What is $p_S(x)$? As before, we divide each unit interval into N equal pieces, and consider a Bernoulli Trial at the midpoint of each sub-interval, with probability $\frac{\lambda}{N}$ of success.

We have approximately $\frac{x-0}{1/N} = Nx$ midpoints from 0 to x (with N midpoints per unit interval). Let $\lceil y \rceil$ be the smallest integer greater than or equal to y. Then we have $\lceil Nx \rceil$ midpoints, where the results of the Bernoulli Trials of the first $\lceil Nx \rceil - 1$ midpoints are all failures and the last is a success.

Thus, the probability of the first success occuring in an interval of length $\frac{1}{N}$ containing x (with N divisions per unit interval) is

$$p_{N,S}(x) = \left(1 - \frac{\lambda}{N}\right)^{\lceil Nx \rceil - 1} \cdot \left(\frac{\lambda}{N}\right)^1. \tag{34}$$

For N large, the above converges to $e^{-\lambda x}\frac{\lambda}{N}$.

We say $p(x)$ is a **continuous probability distribution on** $\mathbb{R}$ if

1. $p(x) \geq 0$ for all $x \in \mathbb{R}$.
2. $\int_{\mathbb{R}} p(x)dx = 1$.
3. Probability$(a \leq x \leq b) = \int_a^b p(x)dx$.

We call $p(x)$ the **probability density function**.

Thus, as $N \to \infty$, we see the probability density function $p_S(x) = \lambda e^{-\lambda x}$. In the special case of $\lambda = 1$, we get the standard exponential decay, e^{-x}.

For instance, let $\pi(M)$ be the number of primes that are at most M. The Prime Number Theorem states $\pi(M) = \frac{M}{\log M}$ plus lower order terms.

Thus, the average spacing between primes around M is about $\log M$. We can model the distribution of primes as a Poisson Process, with parameter

$\lambda = \lambda_M = \frac{1}{\log M}$. While possible locations of primes (obviously) is discrete (it must be an integer, and in fact the location of primes aren't independent), a Poisson model often gives very good heuristics.

We can often renormalize so that $\lambda = 1$. This is denoted **unit mean spacing**. For example, one can show the M^{th} prime p_M is about $M \log M$, and spacings between primes around p_M is about $\log M$. Then the normalized primes, $q_M \approx \frac{p_M}{\log M}$ will have unit mean spacing and $\lambda = 1$.

3.8 Central Limit Theorem

$X_1, X_2, X_3, \dots$ are an infinite sequence of random variables such that the X_j are independent identically distributed random variables (abbreviated i.i.d.r.v.) with $E[X_j] = \bar{X}_j = 0$ (can always renormalize by shifting) and variance $E[X_j^2] = 1$. Let $S_N = \sum_{j=1}^{N} X_j$.

Theorem 3.10 *Fix $-\infty < a \le b < \infty$. Then as $N \to \infty$,*

$$Prob\Big(\frac{S_N}{\sqrt{N}} \in [a,b]\Big) \to \frac{1}{\sqrt{2\pi}} \int_a^b e^{-\frac{t^2}{2}} dt. \tag{35}$$

The probability function is called the Gaussian or the Normal distribution. This is the universal curve of probability. Note how robust the Central Limit Theorem is: it doesn't depend on fine properties of the X_j.

4 Algebraic and Transcendental Numbers

4.1 Definitions

A function $f : A \to B$ is **one-to-one** if $f(x) = f(y)$ implies $x = y$; f is **onto** if given any $b \in B$, $\exists a \in A$ with $f(a) = b$. f is a **bijection** if f is a one-to-one and onto function.

We say two sets A and B **have the same cardinality** (ie, are the same size) if there is a bijection $f : A \to B$. We denote this by $|A| = |B|$. If A has finitely many elements (say n elements), A is **finite** and $|A| = n < \infty$.

Exercise 23 *Show two finite sets have the same cardinality if and only if they have the same number of elements.*

Exercise 24 *If f is a bijection from A to B, prove there is a bijection $g = f^{-1}$ from B to A.*

A is **countable** if there is a bijection between A and the integers $\mathbb{Z}$. A is **at most countable** if A is either finite or countable.

Recall a binary relation R is an **equivalence relation** if

1. Reflexive: $R(x, x)$ is true (x is equivalent to x).
2. Symmetric: $R(x, y)$ true implies $R(y, x)$ is true (if x is equivalent to y then y is equivalent to x).
3. Transitive: $R(x, y)$ and $R(y, z)$ true imply $R(x, z)$ is true (if x is equivalent to y and y is equivalent to z, then x is equivalent to z).

We often denote equivalence by $\equiv$ or $=$.

Exercise 25 *Let $x, y, z \in \mathbb{Z}$, and let $n \in \mathbb{Z}$ be given. Define $R(x, y)$ to be true if $n|(x - y)$ and false otherwise. Prove R is an equivalence relation. We denote it by $x \equiv y$.*

Exercise 26 *Let x, y, z be subsets of X (for example, $X = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}^n$, et cetera). Define $R(x, y)$ to be true if $|x| = |y|$ (the two sets have the same cardinality), and false otherwise. Prove R is an equivalence relation.*

4.2 Countable Sets

We show several sets are countable. Consider the set of non-negative integers $\mathbb{N}$. Define $f : \mathbb{N} \to \mathbb{Z}$ by $f(2n) = n$, $f(2n + 1) = -n - 1$. By inspection, we see f gives the desired bijection.

Consider $\mathbb{W} = \{1, 2, 3, \ldots\}$ (the positive integers). Then $f : \mathbb{W} \to \mathbb{Z}$ defined by $f(2n) = n$, $f(2n + 1) = -n$ gives the desired bijection.

Thus, we have proved

Lemma 4.1 *To show a set S is countable, it is sufficient to find a bijection from S to either $\mathbb{Z}$, $\mathbb{N}$ or $\mathbb{W}$.*

We need the intuitively plausible

Lemma 4.2 *If $A \subset B$, then $|A| \leq |B|$.*

We can then prove

Lemma 4.3 *If $f : A \to C$ is a one-to-one function (not necessarily onto), then $|A| \leq |C|$. Further, if $C \subset A$, then $|A| = |C|$.*

Exercise 27 *Prove Lemmas 4.2 and 4.3.*

If A and B are sets, the **cartesian product** $A \times B$ is $\{(a, b) : a \in A, b \in B\}$.

Theorem 4.4 *If A and B are countable, so is $A \cup B$ and $A \times B$.*

Proof: we have bijections $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$. Thus, we can label the elements of A and B by

$$\begin{aligned} A &= \{a_0, a_1, a_2, a_3, \ldots\} \\ B &= \{b_0, b_1, b_2, b_3, \ldots\}. \end{aligned} \tag{36}$$

Assume $A \cap B$ is empty. Define $h : \mathbb{N} \to A \cup B$ by $h(2n) = a_n$ and $h(2n+1) = b_{n-1}$. We leave to the reader the case when $A \cap B$ is not empty.

To prove the second claim, consider the following function $h : W \to A \times B$:

$$\begin{aligned} & h(1) = (a_0, b_0) \\ & h(2) = (a_1, b_0), h(3) = (a_1, b_1), h(4) = (a_0, b_1) \\ & h(5) = (a_2, b_0), h(6) = (a_2, b_1), h(7) = (a_2, b_2), h(8) = (a_1, b_2), h(9) = (a_0, b_2) \\ & \qquad \vdots \\ & h(n^2+1) = (a_n, b_0), h(n^2+2) = (a_n, b_{n-1}), \ldots, \\ & \qquad\qquad h(n^2+n+1) = (a_n, b_n), h(n^2+n+2) = (a_{n-1}, b_n), \ldots, \\ & \qquad\qquad h((n+1)^2) = (a_0, b_n) \\ & \qquad \vdots \end{aligned} \tag{37}$$

Basically, look at all pairs of integers in the first quadrant (including those on the axes). Thus, we have pairs (a_x, b_y). The above function h starts at $(0, 0)$, and then moves through the first quadrant, hitting each pair once and only once, by going up and over. Draw the picture! $\Box$

Corollary 4.5 *Let A_i be countable $\forall i \in \mathbb{N}$. Then for any n, $A_1 \cup \cdots \cup A_n$ and $A_1 \times \cdots \times A_n$ are countable, where the last set is all n-tuples $(a_1, \ldots, a_n)$, $a_i \in A_i$. Further, $\cup_{i=0}^{\infty} A_i$ is countable. If each A_i is at most countable, then $\cup_{i=0}^{\infty} A_i$ is at most countable.*

Exercise 28 *Prove Corollary 4.5. Hint: for $\cup_{i=0}^{\infty} A_i$, mimic the proof used to show $A \times B$ is countable.*

As the natural numbers, integers and rationals are countable, by taking each $A_i = \mathbb{N}$, $\mathbb{Z}$ or $\mathbb{Q}$ we immediately obtain

Corollary 4.6 *$\mathbb{N}^n$, $\mathbb{Z}^n$ and $\mathbb{Q}^n$ are countable. Hint: proceed by induction. For example write $\mathbb{Q}^{n+1}$ as $\mathbb{Q}^n \times \mathbb{Q}$.*

Exercise 29 *Prove there are countably many rationals in the interval* $[0, 1]$.

4.3 Algebraic Numbers

Consider a polynomial $f(x) = 0$ with rational coefficients. By multiplying by the least common multiple of the denominators, we can clear the fractions. Thus, without loss of generality it is sufficient to consider polynomials with integer coefficients.

The **algebraic numbers**, $\mathcal{A}$, are the set of all $x \in \mathbb{C}$ such that there is a polynomial of finite degree and integer coefficients (depending on x, of course!) such that $f(x) = 0$. The remaining complex numbers are the **transcendentals**.

The **algebraic numbers of degree** n, $\mathcal{A}_n$, are the set of all $x \in \mathcal{A}$ such that

1. there exists a polynomial with integer coefficients of degree n such that $f(x) = 0$
2. there is no polynomial g with integer coefficients and degree less than n with $g(x) = 0$.

Thus, $\mathcal{A}_n$ is the subset of algebraic numbers x where for each $x \in \mathcal{A}_n$, the degree of the smallest polynomial f with integer coefficients and $f(x) = 0$ is n.

Exercise 30 *Show the following are algebraic: any rational, the square-root of any rational, the cube-root of any rational, $r^{\frac{p}{q}}$ where $r, p, q \in \mathbb{Q}$, $i = \sqrt{-1}$, $\sqrt{3\sqrt{2} - 5}$.*

Theorem 4.7 *The Algebraic Numbers are countable.*

Proof: If we show each $\mathcal{A}_n$ is at most countable, then as $\mathcal{A} = \cup_{n=1}^{\infty} \mathcal{A}_n$, by Corollary 4.5 $\mathcal{A}$ is at most countable.

Recall the **Fundamental Theorem of Algebra (FTA):** Let $f(x)$ be a polynomial of degree n with complex coefficients. Then $f(x)$ has n (not necessarily distinct) roots. Of course, we will only need a weaker version, namely that the Fundamental Theorem of Algebra holds for polynomials with integer coefficients.

Fix an $n \in \mathbb{N}$. We now show $\mathcal{A}_n$ is at most countable. We can represent every integral polynomial $f(x) = a_n x^n + \cdots + a_0$ by an $(n+1)$-tuple $(a_0, \ldots, a_n)$. By Corollary 4.6, the set of all $(n+1)$-tuples with integer coefficients ($\mathbb{Z}^{n+1}$) is countable. Thus, there is a bijection from $\mathbb{N}$ to $\mathbb{Z}^{n+1}$, and we can index each $(n+1)$-tuple $a \in \mathbb{Z}^{n+1}$:

$$\{a : a \in \mathbb{Z}^{n+1}\} \;=\; \bigcup_{i=1}^{\infty} \{\alpha_i\}, \tag{38}$$

where each $\alpha_i \in \mathbb{Z}^{n+1}$.

For each tuple α_i (or $a \in \mathbb{Z}^{n+1}$), there are n roots. Let R_{α_i} be the roots of the integer polynomial associated to α_i. The roots in R_{α_i} need not be distinct, and the roots may solve an integer polynomial of smaller degree. For example, $f(x) = (x^2 - 1)^4$ is a degree 8 polynomial. It has two roots, $x = 1$ with multiplicity 4 and $x = -1$ with multiplicity 4, and each root is a root of a degree 1 polynomial.

Let $R_n = \{x \in \mathbb{C} : x \text{ is a root of a degree } n \text{ polynomial}\}$. One can show that

$$R_n \;=\; \bigcup_{i=1}^{\infty} R_{\alpha_i} \;\supset\; \mathcal{A}_n. \tag{39}$$

By Lemma 4.5, R_n is countable. Thus, by Lemma 4.2, as R_n is at most countable, A_n is at most countable.

Therefore, each $\mathcal{A}_n$ is at most countable, so by Corollary 4.5 $\mathcal{A}$ is at most countable. As $\mathcal{A}_1 \supset \mathbb{Q}$ (given $\frac{p}{q} \in \mathbb{Q}$, consider $qx - p = 0$), $\mathcal{A}_1$ is at least countable. As we've shown $\mathcal{A}_1$ is at most countable, this implies $\mathcal{A}_1$ is countable. Thus, $\mathcal{A}$ is countable. $\Box$

4.4 Transcendental Numbers

A set is **uncountable** if there is no bijection between it and the rationals (or the integers, or any countable set).

Theorem 4.8 *The set of irrationals in* $[0,1]$ *is uncountable.*

Proof: Let $I = [0,1] - \mathbb{Q} = \{x : 0 \le x \le 1 \text{ and } x \notin \mathbb{Q}\}$. Assume that I is countable (the case where I is finite is even easier).

We can write every number in I in a base two expansion, say $y = .y_1y_2y_3y_4\cdots$, $y_i \in \{0,1\}$, $y = \sum_i y_i 2^{-1}$. Certain numbers can be written two different ways. For example, $0.010011111111111\cdots = .0101$. As we are assuming I is countable, including both representations of these numbers is equivalent to taking the union of two countable sets, which by Theorem 4.4 is countable.

Further, we can add back all the rationals in $[0,1]$, as there are countably many rationals in $[0,1]$. Call this set S (the union of the irrationals, the alternate representation of some of the irrationals, and the rationals). As X is contained in the union of three at most countable sets (and two are countable), X is countable by Theorem 4.4.

There is therefore a bijection between $\mathbb{N}$ and X. We can enumerate the elements by $\{x_1, x_2, x_3, \ldots\}$.

For each x_i, let $.x_{i1}x_{i2}x_{i3}\cdots x_{ii}\cdots$ be its binary expansion. We list the countable members of X:

$$\begin{aligned}
x_1 &= x_{11}x_{12}x_{13}x_{14}\cdots \\
x_2 &= x_{21}x_{22}x_{23}x_{24}\cdots \\
x_3 &= x_{31}x_{32}x_{33}x_{34}\cdots \\
&\vdots \\
x_n &= x_{n1}x_{n2}x_{n3}x_{n4}\cdots x_{nn}\cdots \\
&\vdots
\end{aligned} \tag{40}$$

We construct a real number $x \in [0,1]$ not in X. As this was supposed to be (more than a) complete list of all reals in $[0,1]$, this will contradict the assumption that I is countable.

Consider the number $z = .z_1 z_2 z_3 \cdots z_n \cdots$ defined by $z_n = 1 - x_{nn}$. Can z be one of the numbers in our list? For example, could $z = x_m$?

No, as they differ in the m^{th} digit. Thus, z is not on our list, violating the assumption that we had a complete enumeration. Note we had to be careful and make sure we included all equivalent ways of writing the same number. Thus, while z disagrees with the base two expansion of x_m, it cannot be an equivalent way of representing x_m, as all equivalent ways of representing x_m are in our list. This is merely an annoying technical detail.

Thus, the set of irrationals in $[0, 1]$ is not countable. $\Box$.

The above proof is due to Cantor $(1873 - 1874)$, and is known as **Cantor's Diagonalization Argument**. Note Cantor's proof shows that *most* numbers are transcendental, though it doesn't tell us *which* numbers are transcendental. We can easily show many numbers (such as $\sqrt{3 + 2^{\frac{3}{5}}\sqrt{7}}$) are algebraic. What of other numbers, such as π and e?

Lambert (1761), Legendre (1794), Hermite (1873) and others proved π irrational; Legendre (1794) also proved π irrational. In 1882 Lindemann proved π transcental.

What about e? Euler (1737) proved that e and e^2 are irrational, Liouville (1844) proved e is not an algebraic number of degree 2, and Hermite (1873) proved e is transcendental.

Liouville (1851) showed transcendental numbers exist; we will discuss his construction later.

5 Introduction to Number Theory

5.1 Dirichlet's Box Principle

Definition 5.1 (Dirichlet's Box Principle / Pidgeon Hole Principle) *Consider n boxes, and place $n+1$ objects in the n boxes. Then some box contains at least two objects.*

We will use Dirichlet's Box Principle to find good rational approximations to irrational numbers.

5.1.1 Approximation by Rationals

Let $\alpha \in \mathbb{R} - \mathbb{Q}$ be an irrational number. We are looking for a rational number $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right|$ is small, so that $\frac{p}{q}$ is a good rational approximation to α.

Lemma 5.2 *Let $\alpha \in \mathbb{R} - \mathbb{Q}$. Then there exist $p, q \in \mathbb{Z}, q \neq 0$ such that:*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q} \tag{1}$$

Proof. It is enough to prove this for $\alpha \in (0,1)$. Let $q \geq 1$ and divide the interval $[0,1)$ into q intervals $[\frac{p}{q}, \frac{p+1}{q})$ of length $\frac{1}{q}$. Then α belongs to one of these intervals. For some $0 < p < q$ we then have:

$$\alpha \in \left[\frac{p}{q}, \frac{p+1}{q}\right) \Rightarrow \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q}. \tag{2}$$

To obtain a better approximation, we start with an irrational number $\alpha \in (0,1)$ and an integer parameter $Q > 1$. As before, divide the interval $(0,1)$ into Q equal pieces $(\frac{a}{Q}, \frac{a+1}{Q})$. Consider the $Q+1$ numbers inside the interval $(0,1)$:

$$\{\alpha\}, \{2\alpha\}, ..., \{(Q+1)\alpha\}, \tag{3}$$

where $\{x\}$ denotes the fractional part of x. Letting $[x]$ denote the greatest integer less than or equal to x, we have $x = [x] + \{x\}$.

By Dirichlet's Box Principle, at least two of these numbers, say $\{q_1\alpha\}$ and $\{q_2\alpha\}$, belong to a common interval of length $\frac{1}{Q}$. Without loss of generality, we may take $1 \leq q_1 < q_2 \leq Q+1$.

Hence

$$\left|\{q_2\alpha\} - \{q_1\alpha\}\right| \leq \frac{1}{Q} \tag{4}$$

and

$$|(q_2\alpha - n_2) - (q_1\alpha - n_1)| \leq \frac{1}{Q}, \quad n_i = [q_i\alpha]. \tag{5}$$

Now let $q = q_1 - q_2$, $1 \leq q \leq Q$ and $p = n_1 - n_2 \in \mathbb{Z}$. Then

$$\left|q\alpha - p\right| \leq \frac{1}{Q} \tag{6}$$

and hence

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}. \quad (7)$$

We have proven

Theorem 5.3 *Given $\alpha \in \mathbb{R}$, there exist $p, q \in \mathbb{Z}, q \neq 0$, such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \quad (8)$$

5.2 Counting the Number of Primes

5.2.1 Euclid

Lemma 5.4 (Euclid) *There are infinitely many primes.*

Proof by contradiction: Assume there are only finitely many primes, say $p_1, p_2, \dots, p_n$. Consider

$$x = p_1 p_2 .. p_n + 1. \quad (9)$$

x cannot be prime, as we are assuming p_1 through p_n is a complete list of primes. Thus, x is composite, and divisible by a prime. However, p_i cannot divide x, as it gives a remainder of 1. Thus, x would have to be divisible by some prime not in our list, again contradicting the assumption that p_1 through p_n is a complete enumeration of the primes. □

Exercise 31 *Try, using Euclid's argument, to find an explicit lower bound (as weak as you like) to the function:*

$$\pi(X) = \#\{p : p \textit{ is prime and } p \leq X\}. \quad (10)$$

5.2.2 Dirichlet's Theorem

Theorem 5.5 (Primes in Arithmetic Progressions) *Let a and b be relatively prime integers. Then there are infinitely many primes in the progression $an + b$. Further, for a fixed a, to first order all relatively prime b give progressions having the same number of primes.*

Notice that the condition $(a, b) = 1$ is necessary. If $\gcd(a, b) > 1$, $an + b$ can never be prime. Dirichlet's remarkable result is that this condition is also sufficient.

Exercise 32 *Dirichlet's theorem is not easy to prove, but try to prove it in the particular case $a = 4, b = -1$, i.e. for the arithmetic progression $4n - 1$, using an argument similar to Euclid's. Proving there are infinitely many primes of the form $4n + 1$ is a lot harder.*

5.2.3 Prime Number Theorem

Theorem 5.6 *(Prime Number Theorem or PNT) As $X \to \infty$,*

$$\pi(X) \sim \frac{X}{\log X} \tag{11}$$

The Prime Number Theorem was proved in 1896 by Jacques Hadamard and Charles Jean Gustave Nicolas Baron de la Vallee Poussin. Of course, we need to quantify what $\pi(X) \sim \frac{X}{\log X}$ means. Basically, there is an error function $E(X)$ such that $|\pi(X) - \frac{X}{\log X}| \leq E(X)$, and $E(X)$ grows slower than $\frac{X}{\log X}$.

A weaker version was proved by Pafnuty Chebyshev (around 1850).

Theorem 5.7 (Chebyshev) *There exist explicit positive constants A and B such that, for $n > 30$:*

$$\frac{AX}{\log X} \leq \frac{\pi(X)}{X} \leq \frac{BX}{\log X}. \tag{12}$$

Chebyshev showed one can take $A = \log\left(\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}4^{\frac{1}{4}}}{30^{\frac{1}{30}}}\right) \approx .921$ and $B = \frac{6A}{5} \approx 1.105$, which are indeed very close to 1. To highlight the method, we will use cruder arguments and prove the theorem for a smaller A and a larger B.

Chebyshev's argument uses an identity using von Mangoldt's Lambda function $\Lambda(n)$, where $\Lambda(n) = \log p$ if $m = p^k$ for some prime p, and 0 otherwise.

Define the function

$$T(X) = \sum_{1 \leq n \leq X} \Lambda(n) \left[\frac{X}{n}\right] = \sum_{n \geq 1} \Lambda(n) \left[\frac{X}{n}\right]. \tag{13}$$

Exercise 33 *Show that* $T(X) = \sum_{n \le X} \log n$.

Now, it is easy to see (compare upper and lower sums) that

$$\sum_{n \le X} \log n = \int_1^X \log \mathrm{t}\ \mathrm{dt} + O(\log X) = X \log X - X + O(\log X), \tag{14}$$

giving a good approximation to the function $T(X)$. The trick is to look at

$$T(X) - 2T\Big(\frac{X}{2}\Big) = \sum_n \Lambda(n)\bigg(\bigg[\frac{X}{n}\bigg] - 2\bigg[\frac{X}{2n}\bigg]\bigg) \tag{15}$$

By the previous remarks, the LHS $= X \log 2 + O(\log X)$. Also,

$$\text{RHS} \le \sum_{p \le X} (\log p) \frac{\log X}{\log p} = \pi(X) \log X. \tag{16}$$

Hence we immediately obtain the lower bound:

$$\pi(X) \ge \frac{X \log 2}{\log X} + O(\log X) \tag{17}$$

Exercise 34 *Prove the bound in Equation 16.*

To obtain an upper bound for $\pi(X)$, we notice that, since $[2\alpha] \ge 2[\alpha]$, the sum in equation (15) has only positive terms. By dropping terms we get a lower bound.

$$\begin{aligned} T(X) - 2T\Big(\frac{X}{2}\Big) &\ge \sum_{X/2 < n \le X} \Lambda(n)\bigg(\bigg[\frac{X}{n}\bigg] - 2\bigg[\frac{X}{2n}\bigg]\bigg) \\ &\ge \sum_{X/2 < p \le X} \log p \\ &\ge \log\Big(\frac{X}{2}\Big) \sum_{X/2 < p \le X} 1 \\ &= \log\Big(\frac{X}{2}\Big)\bigg(\pi(X) - \pi\Big(\frac{X}{2}\Big)\bigg) \end{aligned} \tag{18}$$

Hence we obtain an upper bound for the number of primes between $\frac{X}{2}$ and X:

$$\pi(X) - \pi(X/2) \leq \frac{X \log 2}{\log(\frac{X}{2})} + O(1) \tag{19}$$

Now, if we write inequality (19) for $X, \frac{X}{2}, \frac{X}{2^2}, \ldots$ we get

$$\begin{aligned}
\pi(X) - \pi(X/2) &\leq 2\frac{X/2}{\log(X/2)} \\
\pi(X/2) - \pi(X/2^2) &\leq 2\frac{X/2^2}{\log(X/2^2)} \\
&\vdots \\
\pi(X/2^{k-1}) - \pi(X/2^k) &\leq 2\frac{X/2^k}{\log(X/2^k)}
\end{aligned} \tag{20}$$

as long as $\frac{X}{2^k} \geq 1$, i.e. $k \leq [\log_2 X] = k_0$. Summing the above inequalities we get on the left hand side a telescoping sum. All the terms cancel, except for the leading term $\pi(X)$ and $\pi(X/2^{k_0}) = 0$.

Thus

$$\pi(X) \leq 2\sum_{k=1}^{k_0} \frac{X/2^k}{\log(X/2^k)} \tag{21}$$

To evaluate the sum in the above inequality we split it into two parts, k "small" and k "large". More precisely, let $n_0 = \log_2(X^{1/10})$ so that $2^{n_0} = X^{1/10}$ and note that:

$$2\sum_{k>n_0} \frac{X/2^k}{\log(X/2^k)} \leq 2\sum_{k>n_0} \frac{X}{2^k} \leq \frac{2X}{2^{n_0}} = \frac{2X}{X^{1/10}} = 2X^{9/10}. \tag{22}$$

Hence the contribution from k "large" is very small compared to what we expect (i.e. order of magnitude $\frac{X}{\log X}$), or we can say that the main term comes from the sum over k small.

We now evaluate the contribution from small k.

$$2\sum_{k=1}^{n_0} \frac{X}{2^k} \frac{1}{\log(X/2^k)} \leq \frac{2X}{\log(X/2^{n_0})} \sum_{k=1}^{n_0} \frac{1}{2^{n_0}} \leq \frac{2X}{\log(X^{9/10})} = \frac{20}{9}\frac{X}{\log X} \tag{23}$$

Hence the right hand side of the equation (21) is made up of two parts, a main term of size $\frac{BX}{\log X}$ coming from equation (23), and a lower order term coming from equation (22).

For X sufficiently large,

$$\pi(X) \leq \frac{BX}{\log X} \tag{24}$$

where B can be any constant strictly bigger than $\frac{20}{9}$.

To obtain Chebyshev's better constant we would have to work a little harder along these lines, but it is the same method.

Gathering equations (17) and (24) we see we have proven

$$\frac{AX}{\log X} \leq \pi(X) \leq \frac{BX}{\log X}. \tag{25}$$

While this is not an asymptotic for $\pi(X)$, it does give the right order of magnitude for $\pi(X)$, namely $\frac{X}{\log X}$.

Exercise 35 *Using Chebyshev's Theorem, Prove Bertrand's Postulate: for any integer $n \geq 1$, there is always a prime number between n and $2n$.*