Course Notes

Conjecture and Proof

Alex Rutar

BSM Fall 2018

Contents

Chapter 1

An Introduction

1.1 Sidon Sets

We define a Sidon set $S \subseteq N$ as a subset such that pairwise sums are unique. Write $1 \le a_1 < a_1 < \cdots < a_k \le n$ with $a_i + a_j \ne a_l + a_r$ (possibly $i = j$, $l = r$). what is the maximum value of k? For example, the powers of two provide a lower bound of $\max k \ge \lfloor \log_2 n \rfloor + 1$ by binary representations and uniqueness of multiplication by 2.

We can also bound above: $2 \le a_i + a_j \le 2n$ and the number of sums is $\binom{k}{2} + k$. We must have

$$\binom{k}{2} + k \le 2n - 1$$

which can be rearranged to (losing a small amount of precision)

$$k < 2\sqrt{n}$$

We can get a better upper bound: note that if we have equal sums, we also have equal differences: $a_i + a_j = a_l + a_r$ implies $a_i - a_l = a_r - a_j$. We now have $\binom{k}{2}$ differences and $n-1$ places, and by the same argument as above we get

$$k < \sqrt{2n} + 1$$

This trick works because subtraction is not commutative!

Let's now try to get a better lower bound. Always pick the smallest number available that does not violate the rule. We can take

$$1, 2, 4, 8, \ldots$$

Assume that we already picked $a_1 < a_2 < a_3 < \cdots < a_l$. Then can we take a_{l+1}: x is bad if $x + a_i = a_j + a_k$, $x + x = a_j + a_k$, $x = a_j + a_k - a_i$ so there are at most l^3 bad numbers. The second is impossible otherwise we would have $x < \max\{a_j, a_k\}$. Thus there are at most l^3 bad numbers, including $a_i = a_i + a_j - a_k$. Thus if $l^3 < n$, we can certainly pick an a_{l+1}. We therefore have

$$\sqrt[3]{n} \le \max k < \sqrt{2n} + 1$$

1.2 Irrational Numbers

1.2.1 A few proofs of irrationality

Proof We provide five different proofs that $\sqrt{5}$ is irrational:

1. By contradiction, suppose $\sqrt{5} = \frac{a}{b}$ with $(a,b) = 1$ and $b > 0$. Then $5b^2 = a^2$, so $5|a^2$. But since 5 is prime (or generally, a product of distinct primes), $5|a$ and write $a = 5c$ so that $5b^2 = (5c)^2 = 25c^2$. But then $b^2 = 5c^2$ so $5|b$, a contradiction.

2. As above, get $5b^2 = a^2$. Using unique factorization in $\mathbb{Z}$, note that n is a square iff $n = p_1^{k_1} \cdots p_l^{k_l}$ and $2|k_i$ for all i (proof is constructive). But then b^2, a^2 both have an even exponent in the 5 position, so that $5b^2$ has an odd exponent, a contradiction.

   More generally, if there exists an odd exponent in the standard form of m, then $\sqrt{m}$ is irritional.

3. Suppose $\sqrt{5} = \frac{a}{b}$. We must have $\lim_{n\to\infty}(\sqrt{5}-2)^n \to 0$. If we multiply $(c+d\sqrt{5})(h+j\sqrt{5})$, we have another number of the same form. Then $(\sqrt{5}-2)^n = A_n - B_n\sqrt{5} = A_n + B_n\frac{a}{b} = \frac{C_n}{b} \geq \frac{1}{b}$ with $C_n \neq 0$, contradicting the limit.

4. In geometry, we say a and b are commesurable (have a common measure) if there exists c so that $kc = a$ and $lc = b$ where $k, l \in \mathbb{Z}$. Then a/b is rational if and only if a, b have a common measure. To see the forward direction, we have $\frac{a}{b} = \frac{m}{n}$ so that $\frac{a}{m} = \frac{b}{n}$ and a common measure is $\frac{a}{m}$. Conversely, if $kc = a$ and $lc = b$ then $\frac{a}{b} = \frac{k}{l}$.

   Thus we will show that $\sqrt{5}$ and 1 have no common measure. Suppose c is a common measure of 1 and $\sqrt{5}$. Consider a rectangle with sides $1, 2$ and diagonal of length $\sqrt{5}$. Let $AB = 1$, $BC = 2$ and choose E so that $EC = BC$. Drop a perpindicular from E onto AB. Then $AEF \sim ABC$ since they share two angles. But then $FE = 2AE$. Then c is also a common measure of FE. Similarly, $FB = FE$ since $FBC \cong FEC$. Then c is also a common measure of FB and thus of AF.

   Repeat this construction, so we must have c arbitrarily small because the ratios of the hypotenuses are a constant ratio less than 1. Thus we have our contradiction.

5. $\sqrt{5}$ is a root of the polynomial $x^2 - 5$. We have the rational root test, which states that possible rational roots must Write $f = a_0 + a_1 x + \cdots + a_n x^n$. Consider a root of the form $r/2$, so $f(r/s) = 0$. Then

   $$0 = a_0 s^n + a_1 r s^{n-1} + a_2 r^2 s^{n-2} + \cdots + a_n r^n$$

   so $s|a_n r^n$ so $s|a_n$ (since $(s,r) = 1$). Similarly, $r|a_0$.

   If $\sqrt{5} = 1/b$, then $a|-5$ and $b|1$ so $a/b = \pm 1, \pm 5$. Check, and none of these work, so there are no rational roots. □

Prop. 1.2.1 *e is irrational.*

Proof Assume $e = \frac{a}{b}$, $b > 0$, $(a,b) = 1$ and write

$$\frac{a}{b} = e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

and muliply by $b!$ to get

$$\text{integer} = \text{integer} + \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \cdots$$

but the infinite sum is positive less than $\frac{1}{2} + \frac{1}{4} + \cdots = 1$, a contradiction. $\square$

Prop. 1.2.2 $\sin 1^\circ$ *is irrational.*

Proof We show that if $\sin 1^\circ$ is rational, then $\sin 45^\circ$ is rational. Write $z = \cos 1^\circ + i \sin 1^\circ$ so that $z^{45} = (\cos 1^\circ + i \sin 1^\circ)^{45} = \cos 45^\circ + i \sin 45^\circ$. Expand the binomial coefficient to get

$$\begin{aligned} \sum_{n=0}^{45} \binom{45}{n} (\cos 1^\circ)^n (i \sin 1^\circ)^{45-n} &= \text{real} + \sum_{\substack{n=0 \\ 2|n}}^{45} \binom{45}{n} (\cos 1^\circ)^n (i \sin 1^\circ)^{45-n} \\ &= \text{real} + i \sum_{\substack{n=0 \\ 2|n}}^{45} (\pm 1) \binom{45}{n} (\cos 1^\circ)^n (\sin 1^\circ)^{45-n} \end{aligned}$$

but since $(\cos 1^\circ)^2 = 1 - (\sin 1^\circ)^2$ is rational, the entire imaginary part is rational. Thus equating with $\sin 45^\circ$ means that $\sin 45^\circ = \sqrt{2}/2$ is rational, our contradiction. $\square$

1.2.2 Algebraic Numbers

It is interesting to consider numbers which are roots of polynomials with rational (equiv. integer) coefficients of degree at least 1. The rational numbers $\frac{a}{b}$ are roots of the degree one polynomials $x - \frac{a}{b}$.

Def'n. 1.2.3 *We say that* $\alpha \in \mathbb{C}$ *is algebraic if there exists* $p \in \mathbb{Z}[x]$, $p \neq 0$, *so that* $p(\alpha) = 0$. *If* α *is not algebraic, then it is transcendental.*

Def'n. 1.2.4 *We say that* f *is the minimal polynomial of* α *if* $f(\alpha) = 0$ *and* f *has minimal degree.*

Def'n. 1.2.5 *With this in mind, we define the* ***degree*** *of an algebraic number* $\deg \alpha = \deg m_\alpha$.

We have the following properties of the minimal polynomial:

Thm. 1.2.6 *The following hold:*

(a) The minimal polynomial is unique up to a constant factor.

(b) $g(\alpha) = 0 \Leftrightarrow m_\alpha | g$

(c) $g = m_\alpha \Leftrightarrow g(\alpha) = 0$ *and* g *is irreducible over* $\mathbb{Q}$, *i.e.* g *cannot be factored into polynomials of smaller degree with rational coefficients.*

(d) The algebraic numbers form a subfield of the complex numbers.

Proof We first show (b). If $m_\alpha | g$, then $g(\alpha) = m_\alpha(\alpha) f(\alpha) = 0$. For the reverse direction, write $g = m_\alpha \cdot q + r$ where $\deg r < \deg m_\alpha$. Then $0 = g(\alpha) = m_\alpha(\alpha) \cdot q + r(\alpha)$ so $r(\alpha) = 0$. But since m_α is the minimal polynomial, we must have $r = 0$ and $m_\alpha | g$.

Now we see (a) from (b). Suppose p, q are both minimal polynomials. Then $p|q$ so $q = hp$, where $\deg q = \deg p$. Thus $\deg h = 0$ is a constant polynomial.

Now we see (c). We certainly have $g(\alpha) = 0$. Now suppose for contradiction that g is reducible, and write $g = f \cdot h$. But then $f(\alpha)h(\alpha) = 0$, so w.l.o.g. $f(\alpha) = 0$ with $\deg f < \deg g$, so g is not minimal. Conversely, $m_\alpha | g$ so $m_\alpha = cg$. □

Ex. 1.2.7 Show that $\deg \sqrt[3]{2} = 3$. By (c), it suffices to show that $x^3 - 2$ is irreducible, which follows by the rational root test.

Now consider $f = x^4 - 2$, and suppose $f = g \cdot h$. g and h cannot be degree 1 by the rational root theorem, but we could have $\deg g = \deg h = 2$. To prove this, we use the Eisenstein criterion with $p = 2$. multiplication by i

Thm. 1.2.8 (Gelfond-Schneider) *Suppose $0, 1 \neq \alpha$ is algebraic, and β is algebraic, and not rational. Then α^β is transcendental.*

Cor. 1.2.9 $\beta = \log_{10} 3$ *is transcendental.*

Proof Write $10^\beta = 3$. Suppose β is algebraic. β is certainly irrational, but then 10^β is transcendental, a contradiction. □

1.3 Constructing the irrationals

Let $\alpha \in \mathbb{R}$, $\frac{r}{s} \in \mathbb{Q}$. We want to find

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{f(s)}$$

We always assume $(r, s) = 1$, $s > 0$.

1.3.1 Linear Diophantine Equations

First suppose $\alpha = a/b$. Then

$$\left|\frac{a}{b} - \frac{r}{s}\right| = \frac{|sa - rb|}{bs} \geq \frac{1}{bs}$$

where equality holds when $sa - rb = \pm 1$. This is an example of a linear diophantine equation: we wish to solve $Ax + By = C$ for integers A, B, C, x, y.

Prop. 1.3.1 *$Ax + By = C$ is solvable if and only if $(A, B)|C$. If it is solvable, there are infinitely many solutions.*

Proof If it is solvable, we have x_0, y_0 so $Ax_0 + By_0 = C$. Then (A, B) divides A and B so it must divide a linear combination of A and B, so it must also divide C.

The reverse direction is a consequence of the Euclidean algorithm.

Now suppose we have a solution $Ax_0 + By_0 = C$, then $A(x_0 + tB) + B(y_0 - tA) = C$ is also a solution. □

Thm. 1.3.2 *If α is irrational, then there exists infinitely many $\frac{r}{s}$ so that*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^2}$$

Lemma 1.3.3 *Let $\alpha \in \mathbb{R}$, $u > 0$ an integer. Then there exists r/s so that $|\alpha - r/s| < 1/(su)$ for $s \leq u$.*

Proof Define $\{\beta\} = \beta - \lfloor \beta \rfloor$. Clearly $0 \leq \{\beta\} < 1$. Thus $0 \leq 0, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\} < 1$. Partition $[0,1)$ into intervals $[a/n, (a+1)/n)$ for $a \leq n-1$. Then by the pidgeonhole principle, there exists i, j so that $|\{j\alpha\} - \{i\alpha\}| < 1/n$. Thus

$$|(j-i)\alpha - (\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor)| < \frac{1}{n}$$

and take $s = j - i$ and $r = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor$ so that

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{ns}$$

showing the lemma. □

Proof Now, let's prove the theorem. First, choose n_1 and get

$$\left||\alpha - \frac{r_1}{s_1}\right| < \frac{1}{u_1 s_1} < \frac{1}{s_1^2}$$

Now repeat with some new choice of n_2, to get some r_2/s_2. Fix $d = |\alpha - r_1/s_1|$. In order to guarantee $|\alpha - r_2/s_2| < d$, choose n_2 so that $\frac{1}{n_2} < d$, and since $d > 0$ (α is irrational), this is always possible. Then

$$\left|\alpha - \frac{r_2}{s_2}\right| < \frac{1}{s_2 n_2} < \frac{1}{n_2} < d$$

As a side note, if we find r, s not relatively prime, write $m = (r, s)$ and $r = mr'$, $s = ms'$. Then

$$\left|\alpha - \frac{r'}{s'}\right| < \frac{1}{m^2 s'^2} < \frac{1}{s'^2}$$

□

Now, suppose we fix a given s. Then at most how many r can occur? Note that $\frac{k}{s} < \alpha < \frac{k+1}{s}$. Then we cannot have $r = k$ and $r = k+1$: if so,

$$\left|\alpha - \frac{k}{s}\right| < \frac{1}{s^2}$$
$$\left|\alpha - \frac{k+1}{s}\right| < \frac{1}{s^2}$$

so we must have $\frac{2}{s^2} < s$. Thus if $s > 1$, then r is unique, and if $s = 1$, then there are two values of r. Thus

$$\lim_{k\to\infty} \left|\alpha - \frac{r_k}{s_k}\right| = 0$$

for

$$\left|\alpha - \frac{r_k}{s_k}\right| < \frac{1}{s_k^2}$$

Cor. 1.3.4 *If α is irrational, and consider the sequence $\{0\}, \{\alpha\}, \{2\alpha\}, \dots, \{n\alpha\}, \dots$. This is dense in* $[0,1]$.

Proof From the lemma, we have $|s\alpha - r| < 1/s$, so as $s \to \infty$, $|s\alpha - r| \to 0$. Thus $s\alpha$ is close to an integer, so $\{s\alpha\}$ is close to 0 or 1. Now $\{2s\alpha\} = 2s\alpha + 2\lfloor s\alpha \rfloor + 2\{s_\alpha\} = 2\lfloor s_\alpha \rfloor + \{2s\alpha\}$ as long as $2\{s\alpha\} < 1$. But then the collection $\{ns\alpha\}$ is within ϵ of any point on $[0,1]$. □

Thm. 1.3.5 *If $\deg \alpha = n$, then there exists $c = c(\alpha) > 0$ so that, for any $r/s \in \mathbb{Q}$,*

$$\left|\alpha - \frac{r}{s}\right| > \frac{c}{s^n}$$

Proof Let $m_\alpha = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$, $a_i \in \mathbb{Z}$. Then over $\mathbb{C}$,

$$\begin{aligned} m_\alpha &= a_0 + a_1 x + \cdots + a_n x^n \\ &= a_n (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_n) \end{aligned}$$

Thus

$$\begin{aligned} \left| m_\alpha \left(\frac{r}{s} \right) \right| &= \left| a_0 + a_1 \frac{r}{s} + \cdots + a_n \left(\frac{r}{s} \right)^n \right| \\ &= \left| a_n \left(\frac{r}{s} - \alpha \right) \left(\frac{r}{s} - \alpha_2 \right) \cdots \left(\frac{r}{s} - \alpha_n \right) \right| \end{aligned}$$

Now suppose for all $c > 0$, there exists r/s so that $|\alpha - r/s| < c/s^n$. Then for each $1/2^k$, we have r_k/s_k so that

$$\left| \alpha - \frac{r_k}{s_k} \right| < \frac{1}{2^k s_k^n} \Leftrightarrow \left| s_k^n \left(\alpha - \frac{r_k}{s_k} \right) \right| < \frac{1}{2^k}$$

But also recall that

$$\left| a_0 + \frac{r}{s} + \cdots + a_n \left(\frac{r}{s} \right)^n \right| = \frac{\text{integer}}{s^n}$$

so

$$\begin{aligned} \frac{1}{s_k^n} \leq \left| m_\alpha \left(\frac{r_k}{s_k} \right) \right| &= \left| a_n \left(\frac{r_k}{s_k} - \alpha \right) \left(\frac{r_k}{s_k} - \alpha_2 \right) \cdots \left(\frac{r_k}{s_k} - \alpha_n \right) \right| \\ &= \left| \left(\frac{r_k}{s_k} - \alpha \right) g \left(\frac{r_k}{s_k} \right) \right| \end{aligned}$$

and

$$1 \leq {}_k^n \left(\frac{r_k}{s_k} - \alpha \right) \left| \left| g \left(\frac{r_k}{s_k} \right) \right| \right.$$

a contradiction, since the right hand side goes to 0. □

To construct a transcendental number, consider

$$\alpha = \sum_{j=1}^{\infty} \frac{1}{v_j}$$

and define

$$\frac{r_k}{s_k} = \sum_{j=1}^{k} \frac{1}{v_j}$$

Assume $v_1, \ldots, v_k$ satisfy $|\alpha - r_j/s_j| < 1/s_j^r$. Choose v_{k+1} so that

$$\left|\alpha - \frac{r_k}{s_k}\right| < \frac{1}{s_k^k}$$

or equivalently, $v_{j+1} > 2v_j$. Choose as well $2s^k < v_{k+1}$. Then

$$\left|\alpha - \frac{r_k}{s_k}\right| = \frac{1}{v_{k+1}} + \frac{1}{v_{k+2}} + \cdots < \frac{2}{v_{k+1}} < \frac{1}{s_k^k}$$

Thm. 1.3.6 *For any $\delta > 0$, the set of α that satisfy "$\exists$ infinitely many $\frac{r}{s}$ so that $|\alpha - r/s| < 1/s^{2+\delta}$" has measure 0. If α is algebraic, there is only finitely many r/s satisfying the property.*

Chapter 2

Cardinality

2.1 Principles

Cardinality is a way of thinking about the size of a set.

Def'n. 2.1.1 *Two sets A and B have the same* ***cardinality*** *if there is a bijection between the sets. If this is the case, we say that $|A| = |B|$. If there exists an injection, then we say $|A| \leq |B|$.*

In particular, cardinality is an equivalence relation.

1. Reflexive: $|A| \sim |A|$ by the identity map.
2. Symmetric: If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is also a bijection.
3. Transitive: If $f : A \to B$ and $g : B \to C$ are bijections, then $\phi = g \circ f : A \to C$ is a bijection.

If $A \subseteq B$, then $|A| \leq |B|$ since the embedding maps are injective (the identity function restricted to A). For example, we have $|\mathbb{N}| \leq |\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{R}|$. We also have $|\mathbb{N}| = |\mathbb{Z}|$ from the bijection given, say, by $f : \mathbb{Z} \to \mathbb{N}$ defined by

$$f(n) = \begin{cases} 2n & n > 0 \\ -2n+1 & n \leq 0 \end{cases}$$

which is also listed below.

$\mathbb{Z}$	0	1	-1	2	-2	3	$\cdots$
$\mathbb{N}$	1	2	3	4	5	6	$\cdots$

Def'n. 2.1.2 *A set A is countable if A is finite or countably infinite. A is countably infinite if $|A| = |\mathbb{N}|$.*

Countable sets can be "listed". If A is finite, we can write $A = \{a_1, \ldots, a_n\}$ for some $n \in \mathbb{N}$. If A is countably infinite, then there exists a bijection $U : \mathbb{N} \to A$ that lets us write

$$A = \{U(i) : i \in \mathbb{N}\}$$

and write $a_i = U(i)$. On the other hand, if $A = \{a_i : i \in \mathbb{N}\}$, we have our bijection $f : A \to \mathbb{N}$ given by $a_i \mapsto i$.

2.2 Cardinality Examples

1. $\mathbb{N}\times\mathbb{N} = \{(a,b) : a,b \in \mathbb{N}\}$. We have $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$.
2. $|\mathbb{Q}| = |\mathbb{N}|$.

Prop. 2.2.1 *The following hold:*

(1) Every infinite subset of $\mathbb{N}$ *is countably infinite.*

(2) If A *is infinite and* $|A| \leq |\mathbb{N}|$*, then* $|\mathbb{N}| = |A|$.

Proof Prove (1), (2) separately:

(1) We use the well-ordering property of $\mathbb{N}$: every non-empty subset of $\mathbb{N}$ has a least element. Let B be an infinite subset of $\mathbb{N}$, so it is non-empty. Thus B has some least element b_1. But then, $B \setminus \{b_1\}$ is also non-empty, so we can repeat this process to create an increasing sequence
$$b_1 < b_2 < b_3 < \cdots <$$
I claim that every element of B is in this set. Let $b \in B$ and consider $\{n \in B : n \leq b\}$. This set is finite with, say, k elements, so $b = b_k$. We then get our bijection by the standard map $b_i \mapsto i$.

(2) Assume $j : A \to \mathbb{N}$ is an injection. Let $B = j(A) \subseteq \mathbb{N}$. Notice $j : A \to B$ is a bijection, so $|A| = |B|$ and B is infinite. By (1), B is countably infinite, so $|B| = |\mathbb{N}|$, and the result follows by transitivity. □

2.3 Uncountable Sets

Thm. 2.3.1 *The set of real numbers* $\{x : 0 \leq x < 1\} = [0,1)$ *is uncountable.*

Proof (Cantor) Suppose it's countable, say $[0,1) = \{r_i : i \in \mathbb{N}\}$. Let $r_i = .r_{i1}r_{i2}\ldots$, with $r_{ij} \in \{0,\ldots,9\}$. Define a by $a = .a_1a_2a_3\ldots$ were
$$a_k = \begin{cases} 1 & : r_{kk} \in \{5,6,7,8,9\} \\ 8 & : r_{kk} \in \{0,1,2,3,4\} \end{cases}$$
and note that a has a unique decimal representation. Since $a_k \neq r_{kk}$ for any k, $a \neq r_k$ for any k. □

Rmk. 2.3.2 (Author's Remark) If you work with some topological properties, you can work with sets called *perfect sets*. Perfect sets are closed sets that contain no isolated points: any element $a \in S$ can be written as a limit $\lim\{a_i\}$ where $a_i \in S \setminus \{a\}$. In particular, the interval $[0,1]$ is a perfect set. We then have the following theorem:

Thm. 2.3.3 *Non-empty perfect sets are uncountable.*

Proof If S is perfect, then S is certainly not finite: given any $x \in S$, we can use increasingly small open neighbourhoods about x, all of which intersect $S \setminus \{x\}$ and avoid any previous elements of the sequence, thus constructing a countably infinite subset. Thus S is either countable or uncountable. Suppose it were countable and write

$$S = \{x_1, x_2, x_3, \ldots\}$$

and consider the interval $U_1 = \{x_1 - 1, x_1 + 1\}$. Now we construct inductively a sequence of nested intervals. Let $U_1 \subset \ldots \subset U_k$ be previous intervals and $x_1, \ldots, x_k$ be previous points. Now choose $x_{k+1} \in U_k$ and some neighbourhood U_{k+1} so that $x_1, \ldots, x_k \notin U_{k+1}$ (this can be done since we only need to avoid finitely many points), and $\overline{U_{k+1}} \subset U_k$. But now we have a sequence $\{U_n\}$ of sets and $\{x_n\}$ of points so that

1. $x_k \in U_k$.
2. $\overline{U_{k+1}} \subset U_k$
3. $x_j \notin U_k$ for all $0 < j < n$

But now consider the set

$$V = \bigcap_{n=1}^{\infty} \left(\overline{U_n} \cap S \right)$$

Each set $\overline{U_N} \cap S$ is closed and bounded, hence compact, and $\overline{U_{n+1}} \cap S \subset \overline{U_n} \cap S$. Then by the nested compact set lemma, V is non-empty and contains some element v. But $v \neq x_i$ for all i, since $v \in U_{i+1}$ but $x_i \notin U_{i+1}$. Thus our enumeration is incomplete, and S is not countable. □

Note that the proof is essentially the diagonalization argument described above!

Cor. 2.3.4 $\mathbb{R}$ *is uncountable.*

Proof Suppose $\mathbb{R}$ is countable, say $g : \mathbb{R} \to \mathbb{N}$ is a bjection. Then

$$g : [0,1) \subseteq \mathbb{R} \to \mathbb{N}$$

so

$$g \circ j : [0,1) \to \mathbb{N}$$

is a bijection, so $[0,1)$ is countable - a contradiction. □

Ex. 2.3.5 There exist transcendental numbers.

Proof The set of algebraic numbers is countable: there are a countable number of minimal polynomials, each of which has finitely many roots which are the algebraic numbers. □

2.4 Cardinal Numbers

We use the following notation: $|\mathbb{N}| = \aleph_0$, $|\mathbb{R}| = \aleph_1$. But does this notation make sense? This is the subject of the Continuum Hypothesis: is there a set A with $|\mathbb{N}| < |A| < |\mathbb{R}|$? This is undecidable; it is independent of the standard axioms (ZFC axioms).

Def'n. 2.4.1 *Given a set A, the power set of A denoted* (A) *is defined as* $(A) = \{x : x \subseteq A\}$.

Thm. 2.4.2 (Cantor) *For any set A,* $|A| < |(A)|$, *where* $|A| < |B|$ *if* $|A| \leq |B|$ *and* $|A| \neq |B|$.

Proof We certainly have an injection given by the map $a \mapsto \{a\}$, so $|A| \leq |(A)|$. Thus suppose we have some bijection $g : A \to (A)$. Define the set

$$B = \{a \in A : a \notin g(a)\} \subseteq A$$

Since $B \subseteq A$, we have $B \in (A)$. Hence there exists $x \in A$ such that $g(x) = B$. But now we have our contradiction in two cases! If $x \in B$, then $x \notin g(x) = B$. If $x \notin B = g(A)$, then $x \in B$. Thus no such g exists. □

Using this we can construct an infinite list of cardinalities, since $|A| < |(A)| < |((A))| < \cdots$.

Def'n. 2.4.3 *We define* $2^A = \{f : A \to \{0,1\}\}$.

For example, if $|A| = n$, then $|2^A| = 2^n = |(A)|$.

Thm. 2.4.4 $|2^A| = |(A)|$.

Proof Define $g : (A) \to 2^A$ by $B \mapsto \mathbb{1}_B$ where $\mathbb{1}_B$ is the indicator function defined as

$$\mathbb{1}_B = \begin{cases} 0 & : x \notin B \\ 1 & : x \in B \end{cases}$$

and $\mathbb{1}_B \in 2^A$ certainly. g is injective: if $B, C \subseteq A$ and $B \neq C$, then there exists some $x \in B$ but $x \notin C$ without loss of generality so $\mathbb{1}_B(x) = 1$ and $\mathbb{1}_C(x) = 0$. g is surjective: take $f \in 2^A$ and set $B = \{x \in A : f(x) = 1\}$. Then $f = \mathbb{1}_B$ so $g(B) = f$. □

Cor. 2.4.5 $|A| < |2^A|$.

Thm. 2.4.6 (Schroeder-Bernstein) *If* $|A| \leq |B|$ *and* $|B| \leq |A|$ *then* $|A| = |B|$.

Proof General idea: partition A into two sections, D and D^c so that $D^c = g(f(D)^c$. If this holds, then we can define the bijection as

$$\phi(x) = \begin{cases} f(x) & : x \in D \\ g^{-1}(x) & : x \in D^c \end{cases}$$

Define $Q : \mathcal{P}(A) \to \mathcal{P}(A)$ by the map

$$E \mapsto [g(f(E)^c)]^c \subseteq A$$

We wish to show that Q has a fixed point, that is some $D \subseteq A$ such that $Q(D) = D$.

We first show that if $E \subseteq F \subseteq A$, then $Q(E) \subseteq Q(F)$. This is simply a matter of following definitions.

$$\begin{aligned} f(E) \subseteq f(F) &\Rightarrow f(E)^c \supseteq f(F)^c \\ &\Rightarrow g(f(E)^c) \subseteq g(f(F)^c) \\ &\Rightarrow (g(f(E)^c))^c \subseteq (g(f(F)^c))^c \\ &\Rightarrow Q(E) \subseteq Q(F) \end{aligned}$$

Now let $\mathcal{D} = \{E \subseteq A : E \subseteq Q(E)\}$. Set $D = \bigcup_{E \in \mathcal{D}} E \subseteq A$. If $E \in \mathcal{D}$, then $E \subseteq D$. By the claim, $Q(E) \subseteq Q(D)$. If $E \in \mathcal{D}$ then $E \subseteq Q(E) \subseteq Q(D)$, since $E \subseteq D$. So

$$\begin{aligned} \bigcup_{E \in \mathcal{D}} E \subseteq Q(D) &\Rightarrow Q(D) \subseteq Q(Q(D)) \\ &\Rightarrow Q(D) \in \mathcal{D} \\ &\Rightarrow Q(D) \subseteq D \end{aligned} \qquad \square$$

Hence $D = Q(D)$.

As discussed at the beginning, cardinality is an equivalence relation. The notation $|A| \leq |B|$ also makes sense as an ordering by Schroeder-Bernstein. Finally by Cantor's argument, we have an infinite set of cardinalities.

Cor. 2.4.7

1. *If* $A_1 \subseteq A_2 \subseteq A_3$, *and* $|A_1| = |A_3|$, *then* $|A_1| = |A_2| = |A_3|$.
2. $|(0,1)| = |[0,1)| = |\mathbb{R}|$
3. $|\mathbb{R}| = |2^{\mathbb{N}}|$.

Proof

1. We have injections i, j

$$A_1 \overset{i}{\hookrightarrow} A_2 \overset{j}{\hookrightarrow} A_3$$

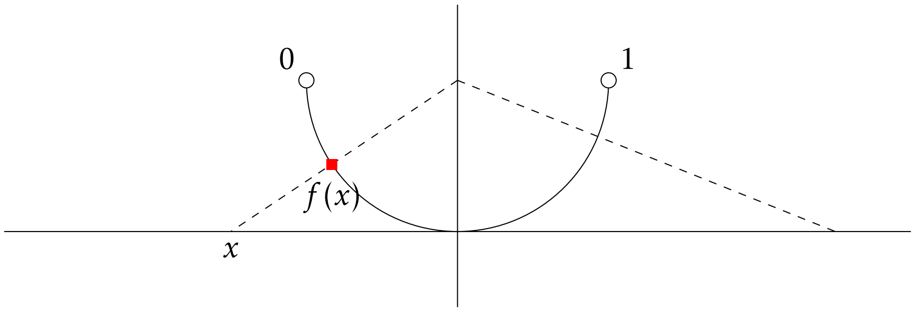
given by the embedding maps, and a bijection $k : A_3 \to A_1$. Then $k \circ j : A_2 \to A_1$ is an injection, so by Schroeder-Bernstein, $|A_1| = |A_2|$ and $|A_2| = |A_3|$ by transitivity.

2. It suffices to show $|(0,1)| = |\mathbb{R}|$. Consider $f(x) = \arctan x$ which is a bijection $f : \mathbb{R} \to \left(\frac{-\pi}{2}, \frac{\pi}{2}\right)$. Thus

$$\frac{1}{\pi} \arctan x + \frac{1}{2} : \mathbb{R} \to (0,1)$$

is a bijection. There are many other examples of such functions! A good exercise is to find a rational function.

Alternative Proof:



3. $|\mathbb{R}| = |2^{\mathbb{N}}|$. Recall $2^{\mathbb{N}} = \{f : \mathbb{N} \to \{0,1\}\}$. Show $|[0,1)| = |2^{\mathbb{N}}|$. Take $r \in [0,1)$ and write as $r = .r_1 r_2 r_3 \ldots$ where $r_j \in \{0,1\}$ (binary representation of r. Define $f_r(n) = r_n, n \in \mathbb{N}$ so $f_r : \mathbb{N} \to \{0,1\}$ so $f_r \in 2^{\mathbb{N}}$. Define $i : [0,1) \to 2^{\mathbb{N}}$ by the map $r \mapsto f_r$. This is injective since if $r \neq r'$, then the k^{th} digits are different for some k and that means $f_r \neq f_{r+1}$ and $|[0,1)| \leq |2^{\mathbb{N}}|$.

   Similarly, we have an injection $2^{\mathbb{N}} \to [0,1)$ given

   $$f \mapsto 0.0f(1)0f(2)0f(3)\ldots \in [0,1)$$

   This is an injection because non-unique binary representation have to end with a tail of 1's (in one case) and a tail of 0's (in the other case). (A good exercise is to think about how to formalize this properly). Thus by Schroeder-Bernstein, the result follows. □

Thm. 2.4.8 *For any prime p, $c^p \equiv c \pmod{p}$.*

Proof This follows by induction. For $c = 0, 1$ this is obvious, and if it holds for c, then by the binomial theorem $(c+1)^p = c^p + 1 = c + 1 \pmod{p}$. □

This generalizes to the Euler-Fermat Theorem:

Thm. 2.4.9 *If $(c,m) = 1$ then $c^{\phi(m)} \equiv 1 \pmod{m}$*

Proof Note that $\phi(p^l) = p^l - p^{l-1} = p^l\left(1 - \frac{1}{p}\right)$, and it can be shown that ϕ is multiplicative for coprime values, so

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

where $p_1, \ldots, p_k$ are the prime divisors of n. □

Recall that $G(k) = \min t$ such that for all $n \geq n_0$, $n = x_1^k + \cdots + x_t^k$ for $x_i \geq 0$.

Thm. 2.4.10 *If $k > 1$, then $g(k) \geq k + 1$.*

Proof We first show that $G(k) \geq k$. Suppose not, and get n_0 so that for all$n \geq n_0$, $n = x_1^k + \cdots + x_{k-1}^k$. Fix N, and we get the number of integers with such a representation with $N \geq n_0$. Then $x_i^k \leq t \leq N$, so $0 \leq x_i \leq \lfloor \sqrt[k]{N} \rfloor$. Thus the number of formal sums $x_1^k + \cdots + x_{k-1}^k$ denoted by B must satisfy $B \geq N - n_0$. Furthermore, $B \sim N^{k/(k-1)}$ while $N - n_0 \sim N$, a contradiction.

We now show that $G(k) \geq k+1$. Assume not, so $\exists n_0$ so $\forall n > n_0$, $n = x_1^k + \cdots + x_k^l$ and let A' denote the number of representable integers up to N, and $A' - n_0$. Now let B' denote the number of formal sums quotiented by permutation. Thus $B' \geq A'$, where $A' \sim N$ but $B' \sim \frac{(\sqrt[k]{N})^k}{k!} = \frac{N}{k!}$, a contradiction.

Let's compute B' more precisely. We choose k pieces from $0, 1, \ldots, \lfloor \sqrt[k]{N} \rfloor$, where repetition is allowed. The number of ways to choose such k pieces is given by the number of $(\lfloor \sqrt[k]{N} \rfloor + 1)$–part compositions of k, so that

$$B' = \binom{k + \lfloor \sqrt[k]{N} \rfloor}{k} = \frac{(\left\lfloor \sqrt[k]{N} \right\rfloor + k) \cdots + (\left\lfloor \sqrt[k]{N} \right\rfloor + 1)}{k!}$$

□

Since

B'≥ A', we have

$$\frac{1}{k!}\left(1 + \frac{k}{\sqrt[k]{N}}\right)\left(1 + \frac{k-1}{\sqrt[k]{N}}\right) \cdots \left(1 + \frac{1}{\sqrt[k]{N}}\right) \geq 1 = \frac{k_0}{N}$$

and as $N \to \infty$, everything goes to 1 except the first term. □