Course Notes

Conjecture and Proof

Alex Rutar

BSM Fall 2018

Contents

1 An Introduction **3**
1.1 Sidon Sets . . . 3
1.2 Irrational Numbers . . . 4
1.2.1 A few proofs of irrationality . . . 4
1.2.2 Algebraic Numbers . . . 5
1.3 Constructing the irrationals . . . 6
1.3.1 Linear Diophantine Equations . . . 6

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 $1 \leq a_1 < a_1 < \cdots < a_k \leq n$ with $a_i + a_j \neq a_l + a_r$ (possibly $i = j$, $l = r$). what is the maximum value of k? For example, the powers of two provide a lower bound of $\max k \geq \lfloor \log_2 n \rfloor + 1$ by binary representations and uniqueness of multiplication by 2.

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

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

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

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

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. □

Prop. 1.2.2 $\sin 1°$ *is irrational.*

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

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

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

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 $\{0\}, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}, \ldots$. 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 $[0,1]$. $\square$