Applications of the course to Number Theory

Rational Approximations

Theorem 1 (Dirichlet)

If ξ is real and irrational then there are infinitely many distinct rational numbers p/q such that

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1}$$

Proof Let $Q \geq 1$ be given. For a real number α let $[\alpha]$ be the largest integer no greater than α, called the *integer part* of α and set $\{\alpha\} = \alpha - [\alpha]$, the *fractional part* of α. Consider the fractional parts $\{0\xi\}$, $\{\xi\}$, $\{2\xi\}$, $\{3\xi\}, ..., \{Q\xi\}$ and the intervals $[i/Q, (i+1)/Q], 0 \leq i \leq Q-1$. There are $Q+1$ fractional parts distributed amongst the Q intervals. So there must exist some interval containing at least two of the fractional parts, i.e. $\{a\xi\}$ and $\{b\xi\}$, $0 \leq a < b \leq Q$, say, lying in $[j/Q, (j+1)/Q]$. Being in the same interval means that $|\{b\xi\} - \{a\xi\}| \leq 1/Q$. Write $a\xi = m + \{a\xi\}$ and $b\xi = n + \{b\xi\}$ for appropriate integers m and n. Then

$$\{b\xi\} - \{a\xi\} = (b\xi - n) - (a\xi - m) = (b-a)\xi - (n-m).$$

Writing $q = b - a$ so $0 \leq q \leq Q$ and $p = n - m$ we find that we can solve

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{qQ}$$

for some $0 \leq q \leq Q$. Since this is true for all Q this gives the infinity of solutions for (4) (noting that $1/qQ \leq 1/q^2$ when $q \leq Q$). ■

This can be improved

Theorem 2 (Hurwitz)

If ξ is real and irrational then there are infinitely many distinct rational numbers p/q such that

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Proof Not given (The easiest way is to used continued fractions.) ■

The constant $\sqrt{5}$ is best possible, in that the result does not hold if it is replaced by a larger value. So if $c > \sqrt{5}$ then there exist irrational ξ for which there are only finitely many distinct p/q satisfying $|\xi - p/q| < 1/cq^2$. In particular $\xi = (1+\sqrt{5})/2$ would be such an exception. Yet it can be shown that the number of exceptions are relatively rare.

Theorem 3

If $f(q)/q$ increases with q and

$$\sum_{q=1}^{\infty} \frac{1}{f(q)}$$

is divergent then, for almost all ξ we can find an infinite sequence of distinct rationals $p/q, q > 0$ satisfying

$$\left| \xi - \frac{p}{q} \right| < \frac{1}{q f(q)}.$$

Proof Not given ■

This result shows that orders of approximation such as

$$< \frac{1}{q^2 \log q} \quad \text{and} \quad < \frac{1}{q^2 \log q \log \log q}$$

are usually possible, for almost all ξ.

I leave it as an exercise to the student to prove that

$$\sum_{q=1}^{\infty} \frac{1}{q \log q} \quad \text{and} \quad \sum_{q=1}^{\infty} \frac{1}{q \log q \log \log q}$$

diverge. (The easiest method is to bound above by integrals.)

Though we don't give the proof of Theorem 3 we do prove a (partial) converse below.

Borel Cantelli Lemma

Observation Let $A_i, i \geq 1$ be an infinite collection of sets. An element x will lie in finitely many of these A_i, if and only if

$$\exists N \geq 1 : \forall n \geq N, x \notin A_n.$$

So the element x will belong to infinitely many of these A_i if and only if

$$\begin{aligned}
& \neg \left(\exists N \geq 1 : \forall n \geq N, x \notin A_n \right) \\
\equiv \quad & \forall N \geq 1, \exists n \geq N : \neg(x \notin A_n) \\
\equiv \quad & \forall N \geq 1, \exists n \geq N : x \in A_n \\
\equiv \quad & x \in \bigcap_{N \geq 1} \bigcup_{k \geq N} A_k.
\end{aligned}$$

Theorem 4 (Borel Cantelli Lemma) *If* $A_1, A_2, ... \in \mathcal{F}$ *and* $\sum_{i=1}^{\infty} \mu(A_i) < \infty$ *then*

$$\mu\{x : x \textit{belongs to infinitely many } A_i\} = 0.$$

Proof

By the observation it suffices to prove that

$$\mu\left(\bigcap_{N\geq 1}\bigcup_{k\geq N} A_k\right) = 0.$$

Let $\varepsilon > 0$ be given. By the definition of convergence of the series in the assumptions we have that there exists $M \geq 1$ such that

$$\sum_{i=M}^{\infty} \mu(A_i) < \varepsilon.$$

For this M we also have

$$\bigcap_{N\geq 1}\bigcup_{k\geq N} A_k \subseteq \bigcup_{k\geq M} A_k.$$

Hence

$$\begin{aligned} \mu\left(\bigcap\nolimits_{N\geq 1}\bigcup\nolimits_{k\geq N} A_k\right) &\leq \mu\left(\bigcup\nolimits_{k\geq M} A_k\right) && \text{since } \mu \text{ is monotone,} \\ &\leq \sum\nolimits_{i=M}^{\infty} \mu(A_i) && \text{since } \mu \text{ is sub-additive,} \\ &< \varepsilon. \end{aligned}$$

True for all $\varepsilon > 0$ implies the required result. ∎

Theorem 4 has many applications in Probability Theory but here we give one in Number Theory, concerning rational approximations.

Theorem 5 *Let* $f : \mathbb{N} \to \mathbb{R}$ *be given. Define* $D \subseteq [0,1]$ *by* $\alpha \in D$ *if, and only if, there exist infinitely many* p/q, $p, q \in \mathbb{Z}$, $p > 0$ *such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qf(q)}.$$

Then if

$$\sum_{q=1}^{\infty} \frac{1}{f(q)} < \infty \tag{2}$$

we have that the Lebesgue measure of D is zero.

Proof Define

$$A_q = \bigcup_{0 \le p \le q} \left(\frac{p}{q} - \frac{1}{qf(q)}, \frac{p}{q} + \frac{1}{qf(q)} \right).$$

Then $\alpha \in D$ if, and only if, $\alpha \in A_q \cap [0,1]$ for infinitely many q, so it suffices to show, subject to (2), that $\mu\left(\bigcap_{N\ge1}\bigcup_{k\ge N}(A_k \cap [0,1])\right) = 0$. Yet

$$\mu\left(A_q \cap [0,1]\right) \le \mu\left(A_q\right) \le 2\sum_{0\le p\le q} \frac{1}{qf(q)} \le \frac{2(q+1)}{qf(q)} \le \frac{4}{f(q)}.$$

Hence

$$\sum_{q=1}^{\infty} \mu\left(A_q \cap [0,1]\right) \le \sum_{q=1}^{\infty} \frac{4}{f(q)} < \infty.$$

So the sets $A_q \cap [0,1]$ satisfy the conditions of Theorem 4 and hence
$\mu\left(\bigcap_{N\ge1}\bigcup_{k\ge N}(A_k \cap [0,1])\right) = 0$, that is, $\mu(D) = 0$. ■

Note This theorem shows that Dirichlet's result cannot be extended to

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^2 \log^2 q},$$

for instance, for many ξ. (I'll leave it to the student to check that

$$\sum_{q=1}^{\infty} \frac{1}{q^2 \log^2 q}$$

converges but agin the easiest way is to bound the sum from above by an integral.)

It is obvious that this result is a partial converse of Theorem 3, where we also needed that $f(q)/q$ increases with q. For such f we see that there are two cases for the sum in (2), it either diverges as in Theorem 3, when a property holds for almost all numbers, or the sum converges as in Theorem 5, when the property holds for almost no number. We say that the property satisfies a zero-one law (There is never a case "in the middle".)

As remarked above this shows that Dirichlet's result on approximations cannot be substantially improved for all ξ. Yet there are numbers ξ that have exceptionally good approximations.

6 Liouville numbers

Theorem 6 *For any algebraic number α of degree $n > 1$ there exists $M = M(\alpha) > 1$ such that*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Mq^n}$$

for all integers $p, q, p > 0$.

Proof If p/q is chosen such that

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

then the result is trivial so assume that p/q satisfies $|q\alpha - p| \leq q$.

Assume α is a root of

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n,$$

where $a_i \in \mathbb{Z}$. Given any p/q we must have $f(p/q) \neq 0$ for if not we would be able to write $f(x) = (qx - p)g(x)$ for some polynomial g with integer coefficients but with $\deg g = n - 1$. Also, since α is algebraic of degree strictly greater than 1, we have that $g(\alpha) = 0$ in which case α is algebraic of degree $\leq n - 1$. This would be a contradiction.

So

$$0 \neq f\left(\frac{p}{q}\right) = \frac{a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-1} + ... + a_np^n}{q^n}.$$

Thus $a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-1} + ... + a_np^n$ is an integer since all $p, q, a_i \in \mathbb{Z}$ not equal to zero. Hence (and this is the "trick") we must have $|a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-1} + ... + a_np^n| \geq 1$ and

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}. \tag{3}$$

For a real number x close to α we can use the Mean Value Theorem to get

$$|f(x)| = |f(x) - f(\alpha)| = |f'(\zeta)||x - \alpha|$$

for some $\zeta : |\zeta - \alpha| \leq |\alpha - x|$. Choose $x = p/q$ which by assumption above satisfies $|p/q - \alpha| \leq 1$ and so ζ satisfies $|\zeta - \alpha| \leq |p/q - \alpha| \leq 1$. Define

$$M = \sup(1, |f'(\zeta)| : |\zeta - \alpha| \leq 1).$$

Then, combining with (3) gives

$$\begin{aligned}\frac{1}{q^n} &\leq \left|f\left(\frac{p}{q}\right)\right| = |f'(\zeta)|\left|\frac{p}{q}-\alpha\right| \\ &\leq M\left|\frac{p}{q}-\alpha\right|,\end{aligned}$$

which is the required result. ∎

Example We can follow the method of proof of the above theorem when $\alpha = (1+\sqrt{5})/2$. Then $f(x) = x^2 - x - 1$ and $f'(x) = 2x - 1$. As we take better approximations p/q to α then ζ, which lies between α and p/q must get closer to α, that is, $|f'(\zeta)|$ must get closer to $|f'(\alpha)| = \sqrt{5}$. So we can take M no smaller than $\sqrt{5}$, confirming the optimal nature of the Theorem of Hurwitz above.

Liouville's Theorem has been improved such that given any algebraic number (whatever its degree) and any $\kappa > 2$ then there exists a constant $c = c(\alpha, \kappa)$ with

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^\kappa}$$

for all rationals p/q. From Dirichlet's Theorem this is seen to be best possible in that we cannot take $\kappa \leq 2$. Strangely, there is no known formulae or method for calculating $c(\alpha, \kappa)$ in general. Only for some particular α and κ is it known. For instance, $c(\sqrt[3]{2}, 2.955) \geq 10^{-6}$, that is,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{10^{-6}}{q^{2.955}}$$

for all rationals p/q.

Definition A real number α is a *Liouville number* if α is irrational and for all $n \geq 1$ there exists integers $p, q > 0$ such that

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{q^n}.$$

Example

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$$

is a Liouville number.

Verification Let α_N be the sum of the first N terms so

$$\begin{aligned}
\alpha_N &= \frac{1}{10}+\frac{1}{10^2}+\frac{1}{10^6}+...+\frac{1}{10^{N!}} \\
&= \frac{10^{N!-1}+10^{N!-2}+...+10^N+1}{10^{N!}} \\
&= \frac{10n+1}{10^{N!}} = \frac{p}{10^{N!}},
\end{aligned}$$

for some integer p, of the form $10n+1$ and so coprime to $10^{N!}$. Then

$$\begin{aligned}
\left|\frac{p}{10^{N!}}-\alpha\right| &= \frac{1}{10^{(N+1)!}}+\frac{1}{10^{(N+2)!}}+\frac{1}{10^{(N+3)!}}+... \\
&< \frac{2}{10^{(N+1)!}} < \frac{1}{(10^{N!})^N}.
\end{aligned}$$

So for every N we can find a very good rational approximation to α, so α is a Liouville number.

Theorem 7

Every Liouville number is transcendental.

Proof

Assume not, so there exists a Liouville number α that is algebraic for some degree n. Note that $n > 1$ since α is irrational. Then Theorem 6 implies that there exists $M \geq 1$ such that

$$\left|\alpha-\frac{p}{q}\right| > \frac{1}{Mq^n}$$

for all integers $p, q > 0$. Choose an integer $k \geq n$ such that $2^k > 2^n M$. Then since α is Liuoville we can find integers $p, q > 0$ such that

$$\left|\frac{p}{q}-\alpha\right| < \frac{1}{q^k} < \frac{1}{Mq^n}$$

by the choice of k. This is a contradiction so the assumption is false and every Liouville number is transcendental. ■

Let E be the set of all Liouville numbers.

Theorem 8

The set E has zero Lebesgue measure in $[0,1]$.

Proof By definition $\alpha \in E$ if, and only if, $\alpha \in \mathbb{Q}^c$ and for all $k \geq 1$ there exist integers $p > 0$ and q such that

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{q^k}.$$

So

$$\begin{aligned} E &= \mathbb{Q}^c \cap \bigcap_{k=1}^{\infty} \bigcup_{p=-\infty}^{+\infty} \bigcup_{q\geq 2} \left(\frac{p}{q} - \frac{1}{q^k}, \frac{p}{q} + \frac{1}{q^k}\right) \\ &= \mathbb{Q}^c \cap \bigcap_{k=1}^{\infty} G_k, \end{aligned}$$

say. Note that

$$G_k \cap [0,1] \subseteq \bigcup_{q\geq 2} \bigcup_{p=0}^{q} \left(\frac{p}{q} - \frac{1}{q^k}, \frac{p}{q} + \frac{1}{q^k}\right).$$

Let μ be the Lebesgue measure on $\mathbb{R}$. Then

$$\begin{aligned} \mu\left(G_k \cap [0,1]\right) &\leq \sum_{q\geq 2} \sum_{p=0}^{q} \mu\left(\frac{p}{q} - \frac{1}{q^k}, \frac{p}{q} + \frac{1}{q^k}\right) \\ &= \sum_{q\geq 2} \sum_{p=0}^{q} \frac{2}{q^k} \\ &= \sum_{q\geq 2} \frac{2(q+1)}{q^k} \\ &\leq 4 \sum_{q\geq 2} \frac{1}{q^{k-1}}. \end{aligned}$$

To bound this sum observe that

$$\frac{1}{q^{k-1}} < \int_{q-1}^{q} \frac{dt}{t^{k-1}}$$

since $t^{k-1} \leq q^{k-1}$ in the range of the integral. Adding gives

$$\sum_{q\geq 2} \frac{1}{q^{k-1}} < \int_1^{\infty} \frac{dt}{t^{k-1}} = \frac{1}{k-2}.$$

Hence $\mu\left(G_k \cap [0,1]\right) \leq 4/(k-2)$. But $E \cap [0,1] \subseteq G_k \cap [0,1]$ for all k so $\mu\left(E \cap [0,1]\right) \leq 4/(k-2)$ for all $k \geq 2$. Hence $\mu\left(E \cap [0,1]\right) = 0$. ■