Introduction to Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Dirichlet's Theorem

Dirichlet's Theorem

Theorem (Dirichlet's Theorem)

For any real θ and any integer $Q > 1$, there exist integers p, q with $0 < q < Q$, such that

$$|q\theta - p| \leq \frac{1}{Q}.$$

- Recall that $\{x\}$ denotes the fractional part of x and consider:
  - the $Q+1$ numbers $0, 1, \{\theta\}, \{2\theta\}, \ldots, \{(Q-1)\theta\}$ in $[0,1]$;
  - the Q subintervals $[0, \frac{1}{Q}), [\frac{1}{Q}, \frac{2}{Q}), \ldots, [\frac{Q-1}{Q}, 1]$.

  Then two of the $Q+1$ numbers must lie in one of the Q sub-intervals.

  The difference between the two numbers has the form

  $$\{m\theta\} - \{n\theta\} = m\theta - [m\theta] - (n\theta - [n\theta]) = (m-n)\theta - ([m\theta] - [n\theta]) = q\theta - p,$$

  where p, q are integers with $0 < q < Q$. Moreover, $|q\theta - p| \leq \frac{1}{Q}$.

Dirichlet's Theorem (Real Q)

Corollary

For any real θ and any real $Q > 1$, there exist integers p, q with $0 < q < Q$, such that $|q\theta - p| \le \frac{1}{Q}$.

- Suppose $Q > 1$ is not an integer.

  We apply Dirichlet's Theorem with $[Q] + 1$.

  There exist integers p, q with $0 < q < [Q] + 1$, such that $|q\theta - p| \le \frac{1}{[Q]+1}$.

  However, since q is an integer,

$$0 < q \le [Q] < Q$$

  and, moreover,

$$|q\theta - p| \le \frac{1}{[Q]+1} < \frac{1}{Q}.$$

Dirichlet's Theorem (Relatively Prime p, q)

Corollary

For any real θ and any real $Q > 1$, there exist relatively prime integers p, q with $0 < q < Q$, such that $|q\theta - p| \leq \frac{1}{Q}$.

- Suppose that the p, q obtained a priori by Dirichlet's Theorem are not relatively prime.

  Then $k = (p, q) > 1$ and $p = kp'$ and $q = kq'$, with $(p', q') = 1$.

  Then, we have

$$|q'\theta - p'| = \frac{1}{k}|kq'\theta - kp'| = \frac{1}{k}|q\theta - p| = \leq \frac{1}{k}\frac{1}{Q} < \frac{1}{Q}.$$

  So we could choose p', q' in place of p, q.

Corollary of Dirichlet's Theorem (Irrational θ)

Corollary

For any irrational θ, there exist infinitely many rationals $\frac{p}{q}$, $q > 0$, such that $|\theta - \frac{p}{q}| < \frac{1}{q^2}$.

- For the existence, taking $Q > 1$, we apply Dirichlet's Theorem to get p, q,

$$|q\theta - p| \le \frac{1}{Q}, \quad 0 < q < Q.$$

Then, $|\theta - \frac{p}{q}| = \frac{1}{q}|q\theta - p| \le \frac{1}{q}\frac{1}{Q} < \frac{1}{q^2}$.
For the cardinality, consider a $Q' > \frac{1}{|q\theta - p|}$. Then $\frac{1}{Q'} < |q\theta - p|$.
It follows that the p', q' associated with Q',

$$|q'\theta - p'| \le \frac{1}{Q'}, \quad 0 < q' < Q',$$

are different.

The Case of Rational θ

- The preceding corollary does not remain valid for rational θ.
- Suppose $\theta = \frac{a}{b}$ with a, b integers and $b > 0$.

  Then, when $\theta \neq \frac{p}{q}$, we have

$$\left|\theta - \frac{p}{q}\right| \geq \frac{1}{qb}.$$

  So, there are only finitely many rationals $\frac{p}{q}$, such that $|\theta - \frac{p}{q}| < \frac{1}{q^2}$.

Subsection 2

Continued Fractions

The Continued Fraction Representation

- The continued-fraction algorithm sets up one-one correspondences:
- Between all irrational θ and all infinite sets of integers $a_0, a_1, a_2, \ldots$, with $a_1, a_2, \ldots$ positive.

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}.$$

- Between all rational θ and all finite sets of integers $a_0, a_1, \ldots, a_n$, with $a_1, a_2, \ldots, a_{n-1}$ positive and $a_n \geq 2$.

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \frac{1}{a_n}}}}.$$

The Continued Fraction Algorithm

- Let θ be any real number.
  - We put $a_0 = [\theta]$.
  - If $a_0 \neq \theta$, we write $\theta = a_0 + \frac{1}{\theta_1}$, so that $\theta_1 > 1$, and we put $a_1 = [\theta_1]$.
  - If $a_1 \neq \theta_1$, we write $\theta_1 = a_1 + \frac{1}{\theta_2}$, so that $\theta_2 > 1$, and we put $a_2 = [\theta_2]$.
  - The process continues indefinitely unless $a_n = \theta_n$, for some n.

  If the latter occurs, then θ is rational.
- In the "end", we have

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \frac{1}{a_n}}}}.$$

The Continued Fraction Algorithm: Terminology

- If θ is rational then the process terminates.

  The expression above is called the **continued fraction** for θ.

  We write $\theta = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n}$ or, more briefly, as $\theta = [a_0, a_1, a_2, \ldots, a_n]$.
- If $a_n \neq \theta_n$, for all n, so that the process does not terminate, then θ is irrational.

  We show that $\theta = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots$, or, briefly, $\theta = [a_0, a_1, a_2, \ldots]$.
  - The integers $a_0, a_1, a_2, \ldots$ are the **partial quotients** of θ.
  - The numbers $\theta_1, \theta_2, \ldots$ are the **complete quotients** of θ.

  We prove that the rationals $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$, where p_n, q_n denote relatively prime integers, tend to θ as $n \to \infty$.

  They are the **convergents** to θ.

The Continued Fraction Algorithm (Recurrences)

Claim: The p_n, q_n are generated recursively by the equations

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2},$$

where $p_0 = a_0, q_0 = 1$ and $p_1 = a_0 a_1 + 1$, $q_1 = a_1$.

The recurrences can be checked easily for $n = 2$.

Assume they hold for $n = m-1 \geq 2$. We verify them for $n = m$.

Define relatively prime p'_j, q'_j $(j = 0, 1, \ldots)$ by $\frac{p'_j}{q'_j} = [a_1, a_2, \ldots, a_{j+1}]$.

Then $\frac{p_j}{q_j} = a_0 + \frac{q'_{j-1}}{p'_{j-1}}$. So $p_j = a_0 p'_{j-1} + q'_{j-1}$ and $q_j = p'_{j-1}$.

Now we compute:

$$\begin{aligned} p_m &= a_0 p'_{m-1} + q'_{m-1} = a_0(a_m p'_{m-2} + p'_{m-3}) + a_m q'_{m-2} + q'_{m-3} \\ &= a_m(a_0 p'_{m-2} + q'_{m-2}) + a_0 p'_{m-3} + q'_{m-3} = a_m p_{m-1} + p_{m-2}; \\ q_m &= p'_{m-1} = a_0 p'_{m-2} + p'_{m-3} = a_0 q_{m-1} + q_{m-2}. \end{aligned}$$

The Continued Fraction Algorithm (Converse)

- By the definition of $\theta_1, \theta_2, \ldots$, we have $\theta = [a_0, a_1, \ldots, a_n, \theta_{n+1}]$, where $0 < \frac{1}{\theta_{n+1}} \le \frac{1}{a_{n+1}}$. Hence, θ lies between $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$. It is readily seen by induction that the above recurrences give

$$p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1},$$

and, thus, we have $|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}| = \frac{1}{q_n q_{n+1}}$. It follows that the convergents $\frac{p_n}{q_n}$ to θ, satisfy

$$\left|\theta - \frac{p_n}{q_n}\right| \le \frac{1}{q_n q_{n+1}},$$

and so certainly $\frac{p_n}{q_n} \overset{n\to\infty}{\longrightarrow} \theta$.

In view of the latter inequality and preceding results, it is clear that, when θ is rational the continued-fraction process terminates.

The Continued Fraction Algorithm and Euclid's Algrithm

- For rational θ, the process is closely related to Euclid's algorithm. Take $\theta = \frac{a}{b}$.

$$\begin{array}{rclcrcl} a & = & bq_1 + r_1 & & \frac{a}{b} & = & q_1 + \frac{r_1}{b} \\ q_1 & = & r_1 q_2 + r_2 & & \frac{q_1}{r_1} & = & q_2 + \frac{r_2}{r_1} \\ & \vdots & & & & \vdots & \\ q_{k-1} & = & r_{k-1} q_k + r_k & & \frac{q_{k-1}}{r_{k-1}} & = & q_k + \frac{r_k}{r_{k-1}} \\ q_k & = & r_k q_{k+1} & & \frac{q_k}{r_k} & = & q_{k+1} \end{array}$$

  - The partial quotients $a_0, a_1, a_2, \ldots$ of θ are just $q_1, q_2, q_3, \ldots, q_{k+1}$;
  - The complete quotients $\theta_1, \theta_2, \ldots$ are given by $\dfrac{b}{r_1}, \dfrac{r_1}{r_2}, \ldots, \dfrac{r_{k-1}}{r_k}$.

In other words, on defining $a_j = q_{j+1}$, $0 \le j \le k$, we have

$$\theta = [a_0, a_1, \ldots, a_k].$$

Example

- For $\theta = \frac{187}{35}$, we have

$$\begin{array}{rcl} 187 & = & 35 \cdot 5 + 12 \\ 35 & = & 12 \cdot 2 + 11 \\ 12 & = & 11 \cdot 1 + 1 \\ 11 & = & 1 \cdot 11 + 0 \end{array}$$

So, we have $\frac{187}{35} = [5, 2, 1, 11]$,

i.e.,

$$\frac{187}{35} = 5 + \frac{1}{2 + \frac{1}{1 + \frac{1}{11}}}.$$

Subsection 3

Rational Approximations

An Inequality Involving Two Convergents

Theorem

For any real θ, of any two consecutive convergents, say $\frac{p_n}{q_n}$ and $\frac{p_{n+1}}{q_{n+1}}$, at least one satisfies $|\theta - \frac{p}{q}| < \frac{1}{2q^2}$.

- The differences $\theta - \frac{p_n}{q_n}$ and $\theta - \frac{p_{n+1}}{q_{n+1}}$ have opposite signs.

  So we get

$$\left|\theta - \frac{p_n}{q_n}\right| + \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}.$$

  But, for any real α, β, with $\alpha \neq \beta$, we have $\alpha\beta < \frac{1}{2}(\alpha^2 + \beta^2)$.

  It follows that

$$\frac{1}{q_n q_{n+1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}.$$

  This gives the result.

An Inequality Involving Three Convergents

Theorem

For any real θ, of any three consecutive convergents, say $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ and $\frac{p_{n+2}}{q_{n+2}}$, one at least satisfies $|\theta - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$.

- Suppose the result fails. Then the equations above would give
$$\frac{1}{\sqrt{5}q_n^2} + \frac{1}{\sqrt{5}q_{n+1}^2} \le \frac{1}{q_n q_{n+1}}.$$
Setting $\lambda = \frac{q_{n+1}}{q_n}$, we get $\lambda + \frac{1}{\lambda} \le \sqrt{5}$. Thus, $\lambda^2 - \sqrt{5}\lambda + 1 \le 0$ or $(\lambda - \frac{1}{2}(1+\sqrt{5}))(\lambda + \frac{1}{2}(1-\sqrt{5})) < 0$. So $\lambda < \frac{1}{2}(1+\sqrt{5})$.
Similarly, setting $\mu = \frac{q_{n+2}}{q_{n+1}}$, we get $\mu < \frac{1}{2}(1+\sqrt{5})$.
By the preceding section, we have $q_{n+2} = a_{n+2}q_{n+1} + q_n$.
So $\mu = \frac{q_{n+2}}{q_{n+1}} = a_{n+2} + \frac{q_n}{q_{n+1}} \ge 1 + \frac{1}{\lambda}$.
This contradicts $\lambda < \frac{1}{2}(1+\sqrt{5})$ implies $\frac{1}{\lambda} > \frac{1}{2}(-1+\sqrt{5})$.

Hurwitz's Theorem

Theorem (Hurwitz's Theorem)

For any irrational θ, there exist infinitely many rational $\frac{p}{q}$, such that

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

- Follows by the preceding result.
- The constant $\frac{1}{\sqrt{5}}$ is best possible.

  (We will prove this later in this set.)

Closedness of Approximations

Theorem

The convergents give successively closer approximations to θ. In fact $|q_n\theta - p_n|$ decreases as n increases.

- Recall the recurrences

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2},$$

with $p_0 = a_0$, $q_0 = 1$ and $p_1 = a_0 a_1 + 1$, $q_1 = a_1$.
Consider the fractions $r_n = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_{n+1} + q_{n-1}}$, $n \geq 1$.
  - $r_1 = \theta$;
  - $r_{n+1} = r_n$, for every $n \geq 1$.

We conclude that, for all $n \geq 1$,

$$\theta = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_{n+1} + q_{n-1}}.$$

Closedness of Approximations (Cont'd)

- We got $\theta = \frac{p_n\theta_{n+1}+p_{n-1}}{q_n\theta_{n+1}+q_{n-1}}$.

  Now we compute

$$\begin{array}{rcl}
|q_n\theta - p_n| & = & \left|q_n\frac{p_n\theta_{n+1}p_{n-1}}{q_n\theta_{n+1}+q_{n-1}} - p_n\right| \\
& = & \left|\frac{p_nq_n\theta_{n+1}+p_{n-1}q_n-p_nq_n\theta_{n+1}-p_nq_{n-1}}{q_n\theta_{n+1}+q_{n-1}}\right| \\
& = & \left|\frac{p_{n-1}q_n-p_nq_{n-1}}{q_n\theta_{n+1}+q_{n-1}}\right| = \frac{1}{q_n\theta_{n+1}+q_{n-1}} \\
& < & \frac{1}{q_n+q_{n-1}} = \begin{cases} \frac{1}{a_1+1} < \frac{1}{\theta_1}, & \text{if } n=1 \\ \frac{1}{(a_n+1)q_{n-1}+q_{n-2}} < \frac{1}{q_{n-1}\theta_n+q_{n-2}}, & \text{if } n>1 \end{cases}
\end{array}$$

Best Approximability of Convergents

Theorem

The convergents are indeed the best approximations to θ in the sense that, if p, q are integers with $0 < q < q_{n+1}$, then $|q\theta - p| \geq |q_n\theta - p_n|$.

- We may find integers u, v satisfying

$$p = up_n + vp_{n+1}, \quad q = uq_n + vq_{n+1}.$$

It follows from $0 < q < q_{n+1}$, that
  - $u \neq 0$;
  - If $v \neq 0$, then u, v have opposite signs.

Recalling that $q_n\theta - p_n$ and $q_{n+1}\theta - p_{n+1}$ have opposite signs, we obtain:

$$\begin{array}{rcl} |q\theta - p| & = & |(uq_n + vq_{n+1})\theta - (up_n + vp_{n+1})| \\ & = & |u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})| \\ & \geq & |q_n\theta - p_n|. \end{array}$$

Sufficient Condition for a Convergent to θ

Theorem

If a rational $\frac{p}{q}$ satisfies $|\theta - \frac{p}{q}| < \frac{1}{2q^2}$, then it is a convergent to θ.

- We compute, for $q_n \leq q \leq q_{n+1}$,

$$\begin{array}{rcl} |\frac{p}{q} - \frac{p_n}{q_n}| & \leq & |\theta - \frac{p}{q}| + |\theta - \frac{p_n}{q_n}| \\ & = & \frac{1}{q}|q\theta - p| + \frac{1}{q_n}|q_n\theta - p_n| \\ & \overset{\text{previous}}{\leq} & (\frac{1}{q} + \frac{1}{q_n})|q\theta - p| \\ & \leq & (\frac{1}{q_n} + \frac{1}{q_n})\frac{1}{2q} = \frac{1}{qq_n}. \end{array}$$

It follows that $|pq_n - p_n q| < 1$.

Therefore, $\frac{p}{q} = \frac{p_n}{q_n}$.

Subsection 4

Quadratic Irrationals

Quadratic Irrationals

- By a **quadratic irrational** we mean a zero of a polynomial

$$ax^2 + bx + c,$$

  where
  - a, b, c are integers;
  - the discriminant $d = b^2 - 4ac$ is positive and not a perfect square.

Examples of Quadratic Irrationals

- $\sqrt{2}$ is a zero of $x^2 - 2 = 0$;
- $\frac{1}{3}(3 + \sqrt{3})$ is a zero of $3x^2 - 6x + 2 = 0$;
- $\frac{1}{2}(3 + \sqrt{2})$ is a root of the equation $4x^2 - 12x + 7 = 0$;
- $\sqrt{20}$ is a zero of $x^2 - 20 = 0$;
- $\sqrt{22}$ is a root of $x^2 - 22 = 0$.

Ultimately Periodic Continued Fractions

- A continued fraction $[a_0, a_1, a_2, \ldots]$ is **ultimately periodic** if there exist k and m, such that the partial quotients $a_0, a_1, \ldots$ satisfy

$$a_{m+n} = a_n, \text{ for all } n \geq k.$$

- I.e., a continued fraction θ is ultimately periodic if and only if it has the form

$$\theta = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+m-1}}],$$

where the bar indicates that the block of partial quotients is repeated indefinitely.

Examples of Quadratic Irrationals

- $\sqrt{2} = [1, \overline{2}]$;
- $\frac{1}{3}(3 + \sqrt{3}) = [1, 1, \overline{1, 2}]$;
- $\frac{1}{2}(3 + \sqrt{2}) = [2, 4, \overline{1, 4}]$;
- $\sqrt{20} = [4, \overline{2, 8}]$;
- $\sqrt{22} = [4, \overline{1, 2, 4, 2, 1, 8}]$.

Characterization of Quadratic Irrationals

Theorem

A continued fraction represents a quadratic irrational if and only if it is ultimately periodic.

- Suppose, first, that $\theta = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+m-1}}]$.

  Set $\phi = \theta_k = [\overline{a_k, \ldots, a_{k+m-1}}]$.

  By preceding work,
  - if $\frac{p_n}{q_n}$ are convergents to θ, $\theta = \frac{p_{k-1}\theta_k + p_{k-2}}{q_{k-1}\theta_k + q_{k-2}} = \frac{p_{k-1}\phi + p_{k-2}}{q_{k-1}\phi + q_{k-2}}$.
  - if $\frac{p'_m}{q'_m}$ are convergents to ϕ, $\phi = \frac{p'_{m-1}\phi + p'_{m-2}}{q'_{m-1}\phi + q'_{m-2}}$.

  The latter shows that ϕ is quadratic.

  The former, then, shows that θ is quadratic.

  Finally, the non-termination shows that θ is irrational.

Necessity (Transformation)

- Suppose θ is a quadratic irrational, i.e., θ satisfies $ax^2+bx+c=0$, where a,b,c are integers with $d=b^2-4ac>0$.

  Let $\frac{p_n}{q_n}$, $n=1,2,\ldots$, denote the convergents to θ.

  Consider the binary form

  $$f(x,y)=ax^2+bxy+cy^2.$$

  Define the substitution

  $$x=p_nx'+p_{n-1}y', \quad y=q_nx'+q_{n-1}y'.$$

  - It has determinant $p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}$.
  - It takes f into $f_n(x,y)=a_nx^2+b_nxy+c_ny^2$, with discriminant d.
  - We have $a_n=f(p_n,q_n)$ and $c_n=f(p_{n-1},q_{n-1})=a_{n-1}$.

  Note that $f(\theta,1)=0$.

  This will be used twice below.

Necessity (Boundedness of Parameters)

- We noted that $f(\theta,1)=0$.

  We now compute:

$$\begin{array}{rcl}\frac{a_n}{q_n^2} & = & f(\frac{p_n}{q_n},1)-f(\theta,1)=a((\frac{p_n}{q_n})^2-\theta^2)+b((\frac{p_n}{q_n})-\theta) \\ & \leq & |a|\left|\frac{p_n}{q_n}-\theta\right|\left|\frac{p_n}{q_n}+\theta\right|+|b|\left|\frac{p_n}{q_n}-\theta\right| \\ & \leq & |a|\frac{1}{q_n^2}\left|\frac{p_n}{q_n}+\theta\right|+|b|\frac{1}{q_n^2}<|a|\frac{2|\theta|+1}{q_n^2}+|b|\frac{1}{q_n^2} \\ & = & \frac{(2|\theta|+1)|a|+|b|}{q_n^2}.\end{array}$$

  Thus, $|a_n|<(2|\theta|+1)|a|+|b|$, a bound independent of n.

  But $c_n=a_{n-1}$ and $b_n^2-4a_nc_n=d$.

  So b_n and c_n are likewise bounded.

Necessity (Ultimate Periodicity)

- For $n \geq 1$, if $\theta_1, \theta_2, \ldots$ denote the complete quotients of θ,

$$\theta = \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}.$$

Using the transformations, we get

$$\begin{array}{rcl} f_n(\theta_{n+1}, 1) & = & f(p_n \theta_{n+1} + p_{n-1}, q_n \theta_{n+1} + q_{n-1}) \\ & = & (q_n \theta_{n+1} + q_{n-1})^2 f\left(\frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n+1}}, 1\right) \\ & = & (q_n \theta_{n+1} + q_{n-1})^2 f(\theta, 1) = 0 \end{array}$$

Hence, there are only finitely many possibilities for $\theta_1, \theta_2, \ldots$.

This shows that $\theta_{\ell+m} = \theta_\ell$, for some positive ℓ, m.

So, the continued fraction for θ is ultimately periodic.

Purely Periodic Continued Fractions

- The continued fraction of a quadratic irrational θ is said to be **purely periodic** if
$$\theta = [\overline{a_0, \ldots, a_{m-1}}].$$
- If θ is a quadratic irrational, the **conjugate** θ' of θ is the quadratic irrational that is a root of the same quadratic equation as θ

Characterization of Pure Periodicity

Theorem

Pure periodicity occurs if and only if $\theta > 1$ and the conjugate θ' of θ satisfies $-1 < \theta' < 0$.

- Suppose $\theta > 1$ and $-1 < \theta' < 0$.
  By induction the conjugates θ'_n of the complete quotients θ_n, $n = 1, 2, \ldots$, of θ also satisfy $-1 < \theta'_n < 0$. The proof is based on
  - $\theta'_n = a_n + \frac{1}{\theta'_{n+1}}$, where $\theta = [a_0, a_1, \ldots]$;
  - $a_n \geq 1$, for all n including $n = 0$.

  The inequality $-1 < \theta'_n < 0$ shows that $a_n = [\frac{-1}{\theta'_{n+1}}]$.

  Since θ is a quadratic irrational, we have $\theta_m = \theta_n$, for some $n > m$.

  This gives $\frac{1}{\theta'_m} = \frac{1}{\theta'_n}$ whence $a_{m-1} = a_{n-1}$ and, hence, that $\theta_{m-1} = \theta_{n-1}$.

  Repetition of this conclusion yields $\theta = \theta_{n-m}$.

  Hence, θ is purely periodic.

Purely Periodic Continued Fractions (Converse)

- If $\theta = [\overline{a_0, \ldots, a_{m-1}}]$ is purely periodic, then $\theta > a_0 \geq 1$. Further, for some $n \geq 1$, we have
$$\theta = \frac{p_n \theta + p_{n-1}}{q_n \theta + q_{n-1}},$$
where $\frac{p_n}{q_n}$, $n = 1, 2, \ldots$, denote the convergents to θ.
So, θ satisfies the equation
$$q_n x^2 + (q_{n-1} - p_n) x - p_{n-1} = 0.$$
Note that the quadratic on the left
  - has the value $-p_{n-1} < 0$ for $x = 0$;
  - has the value $p_n + q_n - (p_{n-1} + q_{n-1}) > 0$ for $x = -1$.

  Hence, the conjugate θ' of θ satisfies $-1 < \theta' < 0$.

A Consequence

Corollary

The continued fractions of $\sqrt{d}+[\sqrt{d}]$ and $\frac{1}{\sqrt{d}-[\sqrt{d}]}$ are purely periodic, where d is any positive integer, not a perfect square.

- Note that:

$$\begin{array}{rcccl} & & \sqrt{d}+[\sqrt{d}] & > & 1; \\ -1 & < & -\sqrt{d}+[\sqrt{d}] & < & 0. \end{array}$$

Similarly,

$$\begin{array}{rcccl} & & \frac{1}{\sqrt{d}-[\sqrt{d}]} & > & 1; \\ -1 & < & \frac{1}{-\sqrt{d}-[\sqrt{d}]} & < & 0. \end{array}$$

By the criterion, the continued fractions of $\sqrt{d}+[\sqrt{d}]$ and $\frac{1}{\sqrt{d}-[\sqrt{d}]}$ are purely periodic.

Almost Purely Periodic Continuous Fractions

- A continued fraction
$$[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+m-1}}]$$
is **almost purely periodic** if $k = 1$.
I.e., only the initial partial quotient a_0 precedes the repeated block.
Example: We saw that $\sqrt{d} + [\sqrt{d}]$ and $\frac{1}{\sqrt{d}-[\sqrt{d}]}$ are purely periodic.
But
$$\sqrt{d} = [\sqrt{d}] + (\sqrt{d} - [\sqrt{d}]) = [\sqrt{d}] + \frac{1}{\frac{1}{\sqrt{d}-[\sqrt{d}]}}.$$
So $\sqrt{d}$ is almost purely periodic.

Subsection 5

Liouville's Theorem

Algebraic Numbers and Minimal Polynomials

- A real or complex number is said to be **algebraic** if it is a zero of a polynomial
$$P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$
where $a_0, a_1, \ldots, a_n$ denote integers, not all 0.
- For each algebraic number θ, there is a polynomial P as above, with least degree, such that $P(\theta) = 0$.
  - P is unique if one assumes that $a_0 > 0$ and that $a_0, a_1, \ldots, a_n$ are relatively prime.
  - P is irreducible over the rationals.
- P is called the **minimal polynomial** for θ.
- The **degree** of θ is defined as the degree of P.

Liouville's Theorem

Theorem (Liouville's Theorem)

For any algebraic number α with degree $n > 1$, there exists a number $c = c(\alpha) > 0$, such that $|\alpha - \frac{p}{q}| > \frac{c}{q^2}$, for all rationals $\frac{p}{q}, q > 0$.

- Let P be the minimal polynomial for α.
  By the Mean Value Theorem, for any rational $\frac{p}{q}, q > 0$, there exists ξ between α and $\frac{p}{q}$, such that $P(\alpha) - P(\frac{p}{q}) = (\alpha - \frac{p}{q})P'(\xi)$.
  By definition, $P(\alpha) = 0$, and, by irreducibility, $P(\frac{p}{q}) \neq 0$.
  But $q^n P(\frac{p}{q})$ is an integer and so $|P(\frac{p}{q})| \geq \frac{1}{q^n}$.
  Assume $|\alpha - \frac{p}{q}| < 1$ (otherwise the conclusion is trivial).
  Then $|\xi| = |\alpha + (\xi - \alpha)| \leq |\alpha| + |\alpha - \xi| \leq |\alpha| + |\alpha - \frac{p}{q}| < |\alpha| + 1$.
  So $|P'(\xi)| < C$, for some $C = C(\alpha)$.
  This gives $|\alpha - \frac{p}{q}| = \frac{|P(\alpha) - P(\frac{p}{q})|}{|P'(\xi)|} > \frac{1}{Cq^2} = \frac{1/C}{q^2}$.

Hurwitz's Theorem Revisited

Theorem (Hurwitz's Theorem)

For any irrational θ, there exist infinitely many rational $\frac{p}{q}$, such that $|\theta - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$ and, by taking $\theta = \alpha = \frac{1}{2}(1+\sqrt{5}) = [1, 1, \ldots]$, we see that $\frac{1}{\sqrt{5}}$ is best possible.

- If $\alpha = \frac{1}{2}(1+\sqrt{5})$, then $P(x) = x^2 - x - 1$ and $P'(x) = 2x - 1$.
  Let $\frac{p}{q}, q > 0$, be any rational and let $\delta = |\alpha - \frac{p}{q}|$.
  $|P(\frac{p}{q})| \leq \delta |P'(\xi)|$, for some ξ between α and $\frac{p}{q}$.
  So $|\xi| \leq \alpha + \delta$ and $|P'(\xi)| \leq 2(\alpha + \delta) - 1 = 2\delta + \sqrt{5}$.
  But $|P(\frac{p}{q})| \geq \frac{1}{q^2}$, whence $\delta(2\delta + \sqrt{5}) \geq \frac{1}{q^2}$.
  So, for any $c' < \frac{1}{\sqrt{5}}$ and for all sufficiently large q, we have $\delta > \frac{c'}{q^2}$.
  Hence, Hurwitz's theorem is best possible.

Transcendental Numbers

- A real or complex number that is not algebraic is said to be **transcendental**.

  Claim: The series
  $$\theta = \frac{1}{2^{1!}} + \frac{1}{2^{2!}} + \frac{1}{2^{3!}} + \cdots$$
  represents a transcendental number.

  Set
  $$p_j = 2^{j!}\left(\frac{1}{2^{1!}} + \frac{1}{2^{2!}} + \cdots + \frac{1}{2^{j!}}\right), \quad q_j = 2^{j!}, \quad j = 1, 2, \ldots.$$
  Then p_j, q_j are integers, satisfying $|\theta - \frac{p_j}{q_j}| = \frac{1}{2^{(j+1)!}} + \frac{1}{2^{(j+2)!}} + \cdots$.

  The sum on the right is at most
  $$\frac{1}{2^{(j+1)!}}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) = \frac{1}{2^{(j+1)!-1}} < \frac{1}{q_j^j}.$$
  It follows from Liouville's theorem that θ is transcendental.

Remarks on Transcendental Numbers

- Any real number θ for which there exists an infinite sequence of distinct rationals $\frac{p_j}{q_j}$ satisfying $|\theta - \frac{p_j}{q_j}| < \frac{1}{q_j^{\omega_j}}$, where $\omega_j \stackrel{j\to\infty}{\longrightarrow} \infty$, will be transcendental.

  Example: This condition will hold for:
  - any infinite decimal in which there occur sufficiently long blocks of zeros;
  - any continued fraction in which the partial quotients increase sufficiently rapidly.

Subsection 6

Transcendental Numbers

The Integral $I(t)$

- Consider the integral

$$I(t) = \int_0^t e^{t-x} f(x) dx, \quad t \geq 0,$$

where f is a real polynomial with degree m.

- More generally, let, for all $i \geq 0$,

$$I_i(t) = \int_0^t e^{t-x} f^{(i)}(x) dx, \quad t \geq 0,$$

where $f^{(i)}(x)$ denotes the i-th derivative of $f(x)$.

- With this notation, $I(t) = I_0(t)$.

Computing $I(t)$

- If $I_i(t) = \int_0^t e^{t-x} f^{(i)}(x)dx,\ t \geq 0$, then

$$I_i(t) = e^t f^{(i)}(0) - f(t) + I_{i+1}(t).$$

This needs an integration by-parts:

$$\begin{aligned} I_i(t) &= \int_0^t e^{t-x} f^{(i)}(x)dx = \int_0^t (-e^{t-x})' f^{(i)}(x)dx \\ &= (-e^{t-x} f^{(i)}(x))\Big|_0^t - \int_0^t (-e^{t-x}) f^{(i+1)}(x)dx \\ &= e^t f^{(i)}(0) - f^{(i)}(t) + I_{i+1}(t). \end{aligned}$$

- If $I(t) = \int_0^t e^{t-x} f(x)dx,\ t \geq 0$, then

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t).$$

This follows by repeated application of the recursive formula above.

Bounding $I(t)$

- If $\overline{f}$ denotes the polynomial obtained from f by replacing each coefficient with its absolute value, then

$$|I(t)| \le \int_0^t |e^{t-x} f(x)| dx \le te^t \overline{f}(t).$$

Note that $|f(x)| \le \overline{f}(x)$.

So we have

$$\begin{array}{rcl} |I(t)| & = & |\int_0^t e^{t-x} f(x) dx| \le \int_0^t e^{t-x} |f(x)| dx \\ & \le & \int_0^t e^{t-x} \overline{f}(x) dx \le e^t \overline{f}(t) \int_0^t dx \\ & = & te^t \overline{f}(t). \end{array}$$

Transcendence of e

- Suppose that e is algebraic, so that

$$a_0 + a_1 e + \cdots + a_n e^n = 0,$$

for some integers $a_0, a_1, \ldots, a_n$, with $a_0 \neq 0$.
Set

$$f(x) = x^{p-1}(x-1)^p \cdots (x-n)^p, \quad p \text{ is a large prime.}$$

The degree m of f is $(n+1)p-1$.
Define

$$J = a_0 I(0) + a_1 I(1) + \cdots + a_n I(n).$$

By the preceding equations,

$$\begin{aligned} J &= \sum_{k=0}^n a_k I(k) = \sum_{k=0}^n a_k (e^k \sum_{j=0}^m f^{(i)}(0) - \sum_{j=0}^m f^{(j)}(k)) \\ &= \sum_{k=0}^n a_k (-\sum_{j=0}^m f^{(j)}(k)) = \sum_{j=0}^m \sum_{k=0}^n a_k f^{(j)}(k). \end{aligned}$$

Transcendence of e (Cont'd)

- For $1 \le k \le n$, define

$$g_k(x) = \frac{f(x)}{(x-k)^p}.$$

Then

$$f^{(j)}(k) = \begin{cases} 0, & \text{if } j < p \\ \binom{j}{p} p! g_k^{(j-p)}(k), & \text{if } j \ge p \end{cases}.$$

So, for all j, $f^{(j)}(k)$ is an integer divisible by $p!$.

Transcendence of e (Cont'd)

- Define
$$h(x) = \frac{f(x)}{x^{p-1}}.$$
Then
$$f^{(j)}(0) = \begin{cases} 0, & \text{if } j < p-1 \\ \binom{j}{p-1}(p-1)!h^{(j-p+1)}(0), & \text{if } j \geq p-1 \end{cases}.$$
Note that:
  - $h(0) = (-1)^{np}(n!)^p$;
  - $h^{(j)}(0)$ is an integer divisible by p, for $j > 0$.

  We conclude that:
  - For $j \neq p-1$, $f^{(j)}(0)$ is an integer divisible by $p!$;
  - $f^{(p-1)}(0)$ is an integer divisible by $(p-1)!$, but not by p for $p > n$.

Transcendence of e (Conclusion)

- Recall that $J = \sum_{j=0}^{m} \sum_{k=0}^{n} a_k f^{(j)}(k)$.
  It follows that J is a non-zero integer divisible by $(p-1)!$.
  So $|J| \geq (p-1)!$.
  But, now, note that:
  - If $k \leq n$, $\overline{f}(k) = k^{p-1}(k+1)^p \cdots (k+n)^p \leq (2n)^m$.
  - $m = (n+1)p - 1 \leq 2np$.

  Hence,

$$\begin{aligned} |J| &= |a_0 I(0) + \cdots + a_n I(n)| \leq |a_0||I(0)| + \cdots + |a_n||I(n)| \\ &\leq |a_1| 1 e^1 \overline{f}(1) + \cdots + |a_n| n e^n \overline{f}(n) \\ &\leq |a_1| e (2n)^{2np} + \cdots + |a_n| n e^n (2n)^{2np} \\ &= (|a_1| e + \cdots + |a_n| n e^n)((2n)^{2n})^p \leq c^p, \end{aligned}$$

  for some c independent of p.
  The inequalities are inconsistent for p sufficiently large.

Subsection 7

Minkowski's Theorem

Blichfeldt's Theorem

Theorem (Blichfeldt's Theorem)

Any bounded region $\mathscr{R}$ with volume V exceeding 1 contains distinct points $\mathbf{x},\mathbf{y}$, such that $\mathbf{x}-\mathbf{y}$ is an integer point, i.e., a point all of whose coordinates are integers.

- Let $\mathbf{u}=(u_1,\ldots,u_n)$ be an integer point.
  Set $\mathscr{R}_{\mathbf{u}}=\{(x_1,\ldots,x_n)\in\mathscr{R}: u_j\le x_j<u_j+1, 1\le j\le n\}$.
  Denote by $V_{\mathbf{u}}$ the volume of $\mathscr{R}_{\mathbf{u}}$.
  $\mathscr{R}$ may be expressed as the disjoint union of $\mathscr{R}_{\mathbf{u}}$.
  Consequently, $V=\sum V_{\mathbf{u}}>1$.
  This gives $\sum(\mathscr{R}_{\mathbf{u}}-\mathbf{u})>1$.
  But, for all $\mathbf{u}$, $\mathscr{R}_{\mathbf{u}}-\mathbf{u}$ lies in the unit square.
  Thus, there exist $\mathbf{u},\mathbf{v}$, such that $(\mathscr{R}_{\mathbf{u}}-\mathbf{u})\cap(\mathscr{R}_{\mathbf{v}}-\mathbf{v})\neq\emptyset$.
  So, there exist points $\mathbf{x}$ in $\mathscr{R}_{\mathbf{u}}$ and $\mathbf{y}$ in $\mathscr{R}_{\mathbf{v}}$, such that $\mathbf{x}-\mathbf{u}=\mathbf{y}-\mathbf{v}$, and so $\mathbf{x}-\mathbf{y}$ is an integer point.

Convex Bodies and Symmetry

- By a **convex body** $\mathscr{S}$ we mean a bounded, open set of points in Euclidean *n*-space, such that

$$\mathbf{x},\mathbf{y} \in \mathscr{S} \quad \text{implies} \quad \lambda\mathbf{x} + (1-\lambda)\mathbf{y} \in \mathscr{S}, \text{ for all } 0 < \lambda < 1.$$

- A set of points $\mathscr{S}$ is said to be **symmetric about the origin** if, for every point $\mathbf{x}$,

$$\mathbf{x} \in \mathscr{S} \quad \text{implies} \quad -\mathbf{x} \in \mathscr{S}.$$

Minkowski's Theorem

Theorem (Minkowski's Theorem)

If a convex body $\mathscr{S}$, symmetric about the origin, has volume exceeding 2^n, then it contains an integer point other than the origin.

- Define $\mathscr{R} = \frac{1}{2}\mathscr{S} := \{\frac{1}{2}\mathbf{x} : \mathbf{x} \in \mathscr{S}\}$.

  Then $V(\mathscr{R}) = \frac{1}{2^n} V(\mathscr{S}) > 1$.

  By Blichfeldt's Theorem, there exist $\mathbf{x}, \mathbf{y} \in \mathscr{R}$, with $\mathbf{x} \neq \mathbf{y}$, such that $\mathbf{x} - \mathbf{y}$ is an integer point.

  By definition, $2\mathbf{x}, 2\mathbf{y} \in \mathscr{S}$.

  By symmetry, $-2\mathbf{y} \in \mathscr{S}$.

  By convexity, $\mathbf{x} - \mathbf{y} = \frac{1}{2}(2\mathbf{x}) + \frac{1}{2}(-2\mathbf{y}) \in \mathscr{S}$.

Linear Independence

- Points $\mathbf{a}_1, \ldots, \mathbf{a}_n$ in Euclidean n-space are said to be **linearly independent** if, for all real numbers $t_1, \ldots, t_n$,

$$t_1\mathbf{a}_1 + \cdots + t_n\mathbf{a}_n = \mathbf{0} \quad \text{implies} \quad t_1 = \cdots = t_n = 0.$$

- If

$$\mathbf{a}_j = (a_{1j}, \ldots, a_{nj}), \quad 1 \le j \le n,$$

  then $\mathbf{a}_1, \ldots, \mathbf{a}_n$ are linearly independent if and only if

$$d = \det(a_{ij}) \neq 0.$$

Lattices and Determinants

- By a **lattice** Λ we mean a set of points of the form

$$\mathbf{x} = u_1\mathbf{a}_1 + \cdots + u_n\mathbf{a}_n,$$

where $\mathbf{a}_1, \ldots, \mathbf{a}_n$ are fixed linearly independent points and $u_1, \ldots, u_n$ run through all the integers.
- The points $\mathbf{a}_1, \ldots, \mathbf{a}_n$ are referred to as the **generators** or as a **basis** for the lattice.
- The **determinant** of Λ is defined as

$$d(\Lambda) = |d| = \det(a_{ij}),$$

where, as before,

$$\mathbf{a}_j = (a_{1j}, \ldots, a_{nj}), \quad 1 \leq j \leq n.$$

General Minkowski's Theorem

Theorem (General Minkowski's Theorem)

If, for any lattice Λ, a convex body $\mathscr{S}$, symmetric about the origin, has volume exceeding $2^n d(\Lambda)$, then it contains a point of Λ other than the origin.

- Let A be the invertible linear transformation $\mathbf{e}_i \mapsto \mathbf{a}_i$, $i = 1, \ldots, n$.
  Define $\mathscr{R} = \frac{1}{2} A^{-1}(\mathscr{S})$.
  Then $V(\mathscr{R}) = \frac{1}{2^n d(\Lambda)} V(\mathscr{S}) > 1$.
  By Blichfeldt's Theorem, there exist $\mathbf{x}, \mathbf{y} \in \mathscr{R}$, with $\mathbf{x} \neq \mathbf{y}$, such that $\mathbf{x} - \mathbf{y}$ is an integer point.
  As before, $A(\mathbf{x} - \mathbf{y}) = 2A(\frac{1}{2}\mathbf{x} + \frac{1}{2}(-\mathbf{y})) \in \mathscr{S}$.
  Moreover, it is in Λ, since $\mathbf{x} - \mathbf{y}$ is an integer point.

Minkowski's Linear Forms Theorem

Corollary

Let $\lambda_1,\ldots,\lambda_n > 0$ and Λ be the lattice generated by $\mathbf{a}_1,\ldots,\mathbf{a}_n$.
If $\lambda_1\cdots\lambda_n > d(\Lambda)$, then there exist integers $u_1,\ldots,u_n$, not all 0, such that

$$|u_1 a_{j1} + \cdots + u_n a_{jn}| < \lambda_j, \quad 1 \le j \le n.$$

- Consider $\mathscr{S} = \{\mathbf{x} : |x_j| < \lambda_j, 1 \le j \le n\}$.
  Note that $\mathscr{S}$ is convex and symmetric and, moreover,

  $$V(\mathscr{S}) = 2^n \lambda_1 \cdots \lambda_n > 2^n d(\Lambda).$$

  Thus, by the General Minkowski's Theorem, $\mathscr{S}$ contains a point in Λ other than the origin.
  This means that, there exist integers $u_1,\ldots,u_n$, not all 0, such that

  $$|u_1 a_{j1} + \cdots + u_n a_{jn}| < \lambda_j, \quad 1 \le j \le n.$$

Generalizations of Dirichlet's Theorem I

Corollary

If $\theta_1,\ldots,\theta_n$ are any real numbers and if $Q>0$, then there exist integers $p,q_1,\ldots,q_n$, not all 0, such that $|q_j|<Q$, $1\le j\le n$, and

$$|q_1\theta_1+\cdots+q_n\theta_n-p|\le\frac{1}{Q^n}.$$

- In Minkowski's Linear Forms Theorem, take:

$$\lambda_j=Q,\ 1\le j\le n,\quad \lambda_{n+1}=\frac{1}{Q^n}$$

and

$$\mathbf{a}_j=\mathbf{e}_j,\ j=1,\ldots,n,\quad \mathbf{a}_{n+1}=(\theta_1,\ldots,\theta_n,-1).$$

Generalizations of Dirichlet's Theorem II

Corollary

There exist integers $p_1,\ldots,p_n,q$, not all 0, such that $|q| \le Q^n$ and $|q\theta_j - p_j| < \frac{1}{Q}$, $1 \le j \le n$.

- In Minkowski's Linear Forms Theorem, take:

$$\lambda_j = \frac{1}{Q},\ 1 \le j \le n, \quad \lambda_{n+1} = Q^n$$

and

$$\begin{array}{lcl} \mathbf{a}_1 & = & (-1,0,\ldots,0,\theta_1) \\ \mathbf{a}_2 & = & (0,-1,\ldots,0,\theta_2) \\ & \vdots & \\ \mathbf{a}_n & = & (0,0,\ldots,-1,\theta_n) \\ \mathbf{a}_{n+1} & = & (0,0,\ldots,0,(-1)^{n+1}). \end{array}$$