MAU23101 Introduction to number theory
6 - Continued fractions

Nicolas Mascot

mascotn@tcd.ie

Module web page

Michaelmas 2020–2021

Version: April 17, 2021

Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

Concept & Notations

Continued fractions

Given $x \in \mathbb{R}$, recall that $\lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leqslant x\}$. Thus

$$\lfloor 3 \rfloor = \lfloor \pi \rfloor = \lfloor 3.99 \rfloor = 3.$$

To a sequence of integers $a_0, a_1, a_2, \cdots \in \mathbb{N}$, we attach the continued fractions

$$[a_0, a_1, a_2, \cdots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \in \mathbb{Q}.$$

Continued fractions

To a sequence of integers $a_0, a_1, a_2, \cdots \in \mathbb{N}$, we attach the continued fractions

$$[a_0, a_1, a_2, \cdots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \in \mathbb{Q}.$$

Example

$$[2, 3, 5, 7] = 2 + \cfrac{1}{3 + \cfrac{1}{5 + \cfrac{1}{7}}} = \frac{266}{115}.$$

Continued fractions

To a sequence of integers $a_0, a_1, a_2, \dots \in \mathbb{N}$, we attach the continued fractions

$$[a_0, a_1, a_2, \cdots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \in \mathbb{Q}.$$

Remark

$$[a_0, a_1, \cdots, a_{n-1}, a_n] = [a_0, a_1, \cdots, a_{n-1} + \frac{1}{a_n}].$$

Continued fractions

To a sequence of integers $a_0, a_1, a_2, \dots \in \mathbb{N}$, we attach the continued fractions

$$[a_0, a_1, a_2, \cdots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \in \mathbb{Q}.$$

We will see that $\lim_{n \to +\infty} [a_0, a_1, a_2, \cdots, a_n]$ exists; we will then denote it by

$$[a_0, a_1, a_2, \cdots] \in \mathbb{R}.$$

Continued fraction expansion of a real number

The continued fraction attached to a real number

Let $x \in \mathbb{R}$ be fixed. We construct two sequences

$$x_0, x_1, x_2, \dots \in \mathbb{R} \text{ and } a_0, a_1, a_2, \dots \in \mathbb{Z}$$

by setting $x_0 = x$ and inductively $a_n = \lfloor x_n \rfloor$ and $x_{n+1} = \frac{1}{x_n - a_n}$. If $x_n = a_n$ for some n, we stop.

Note that $x_n > 1$ and $a_n \geq 1$ for all $n \geq 1$.

Example

For $x = \pi$, we find

- $x_0 = x = \pi = 3.14159\dots,$
- $a_0 = \lfloor x_0 \rfloor = 3,\qquad x_1 = \frac{1}{x_0 - a_0} = \frac{1}{0.14159...} = 7.06251\dots,$
- $a_1 = \lfloor x_1 \rfloor = 7,\qquad x_2 = \frac{1}{x_1 - a_1} = \frac{1}{0.06251...} = 15.99659\dots,$
- $a_2 = \lfloor x_2 \rfloor = 15,\qquad x_3 = \frac{1}{x_2 - a_2} = \frac{1}{0.99659...} = 1.00341\dots,$
- $a_3 = \lfloor x_3 \rfloor = 1,\qquad x_4 = \frac{1}{x_3 - a_3} = \frac{1}{0.00341...} = 292.63459\dots,$
- $a_4 = \lfloor x_4 \rfloor = 292,\qquad$ and so on.

The continued fraction attached to a real number

Theorem

This process stops if $x \in \mathbb{Q}$, and goes on for all $n \in \mathbb{N}$ if $x \in \mathbb{R} \setminus \mathbb{Q}$.

Proof.

Suppose $x = \frac{A}{B} \in \mathbb{Q}$. Then $x_0 = \frac{A}{B}$, $a_0 = \left\lfloor \frac{A}{B} \right\rfloor = Q$, $x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\frac{A}{B} - Q} = \frac{B}{A - BQ} = \frac{B}{R}$, where $A = BQ + R$ is the Euclidean division of A by B. So the continued fraction expansion follows the steps of the Euclidean algorithm for $\gcd(A, B)$. After finitely many steps, we get remainder 0, so $x_n \in \mathbb{N}$, so $a_n = x_n$, so we stop.

Conversely,

$$x_n = a_n \Longrightarrow x_n \in \mathbb{Q} \Longrightarrow x_{n-1} = \frac{1}{x_n} + a_{n-1} \in \mathbb{Q} \Longrightarrow \cdots \Longrightarrow x_0 \in \mathbb{Q},$$

so this cannot happen if $x \in \mathbb{R} \setminus \mathbb{Q}$. □

The continued fraction attached to a real number

Theorem

This process stops if $x \in \mathbb{Q}$, and goes on for all $n \in \mathbb{N}$ if $x \in \mathbb{R} \setminus \mathbb{Q}$.

Example

For $x = \frac{23}{9} \in \mathbb{Q}$, we find

- $x_0 = x = \frac{23}{9}$,
- $a_0 = \lfloor x_0 \rfloor = 2, \qquad x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\frac{23}{9} - 2} = \frac{9}{5}$,
- $a_1 = \lfloor x_1 \rfloor = 1, \qquad x_2 = \frac{1}{x_1 - a_1} = \frac{1}{\frac{9}{5} - 1} = \frac{5}{4}$,
- $a_2 = \lfloor x_2 \rfloor = 1, \qquad x_3 = \frac{1}{x_2 - a_2} = \frac{1}{\frac{5}{4} - 1} = 4$,
- $a_3 = \lfloor x_3 \rfloor = x_3 \rightsquigarrow$ STOP.

Rationals as continued fractions

Theorem

For all $n \geqslant 0$, we have

$$[a_0, a_1, \cdots, a_{n-1}, x_n] = x.$$

Proof.

Induction on n.

- For $n = 0$, $[x_0] = x_0 = x$, OK.
- If true for n, then

$$\begin{aligned}[a_0, a_1, \cdots, a_n, x_{n+1}] &= [a_0, a_1, \cdots, a_{n-1}, a_n + 1/x_{n+1}] \\ &= [a_0, a_1, \cdots, a_{n-1}, x_n] = x. \end{aligned}$$

□

Rationals as continued fractions

Theorem

For all $n \geqslant 0$, we have

$$[a_0, a_1, \cdots, a_{n-1}, x_n] = x.$$

Corollary

Every $x \in \mathbb{Q}$ can be expressed as a finite continued fraction.

Example

$$\frac{23}{9} = [2,1,1,4] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}.$$

Convergents

Two more sequences

Definition

To a sequence of integers $a_0, a_1, a_2, \dots \in \mathbb{N}$, *we attach two sequences* $p_{-2}, p_{-1}, p_0, p_1, \dots \in \mathbb{N}$ *and* $q_{-2}, q_{-1}, q_0, q_1, \dots \in \mathbb{N}$ *by*

$$p_{-2} = 0, \quad p_{-1} = 1, \qquad p_n = a_n p_{n-1} + p_{n-2} \text{ for } n \geq 0;$$
$$q_{-2} = 1, \quad q_{-1} = 0, \qquad q_n = a_n q_{n-1} + q_{n-2} \text{ for } n \geq 0.$$

Thus for example $p_0 = a_0$, $q_0 = 1$; and $p_1 = a_1 a_0 + 1$, $q_1 = a_1$.

Remark

If $x > 1$, then $a_n \geq 1$ for all n, so $p_n, q_n \geqslant F_n$ for all $n \geq 0$, where F_n is the Fibonacci sequence defined by

$$F_0 = F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}.$$

In particular $p_n, q_n \to +\infty$; more specifically

$$p_n, q_n \geq F_n \sim \left(\frac{1 + \sqrt{5}}{2} \right)^{n-1}.$$

The convergents

Definition

The quantities $[a_0, a_1, \cdots, a_n]$ $(n \geq 0)$ *are called the* *convergents of the continued fraction.*

Theorem

For all $n \geq 0$, *we have* $[a_0, a_1, \cdots, a_n] = \dfrac{p_n}{q_n}$.

The convergents

Theorem

For all $n \geq 0$, we have $[a_0, a_1, \cdots, a_n] = \frac{p_n}{q_n}$.

Proof.

Induction on n.

- For $n = 0$, $p_0/q_0 = a_0/1 = [a_0] \rightsquigarrow$ OK.
- Suppose it is true for n. Define a new sequence a'_m for $m \leq n$ by $a'_0 = a_0, \cdots, a'_{n-1} = a_{n-1}, a'_n = a_n + \frac{1}{a_{n+1}}$, and the corresponding p'_m, q'_m; then $p'_m = p_m$ for $m < n$ whereas $p'_n = a'_n p'_{n-1} + p'_{n-2} = (a_n + \frac{1}{a_{n+1}})p_{n-1} + p_{n-2} = p_n + \frac{p_{n-1}}{a_{n+1}}$, and similarly for the q_m. Thus

$$[a_0, a_1, \cdots, a_n, a_{n+1}] = [a_0, a_1, \cdots, a_n + \frac{1}{a_{n+1}}] = [a'_0, a'_1, \cdots, a'_n]$$

$$\overset{\text{Ind.}}{=} \frac{p'_n}{q'_n} = \frac{p_n + \frac{p_{n-1}}{a_{n+1}}}{q_n + \frac{q_{n-1}}{a_{n+1}}} = \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}p_n + p_{n-1}} = \frac{p_{n+1}}{q_{n+1}}.$$

□

The convergents

Theorem

For all $n \geq 0$*, we have* $[a_0, a_1, \cdots, a_n] = \dfrac{p_n}{q_n}$.

Corollary

For all $y > 0$ *and for all* n*,*

$$[a_0, a_1, \cdots, a_n, y] = \frac{yp_n + p_{n-1}}{yq_n + q_{n-1}}.$$

Identities between successive convergents

Theorem

For all $n \geq 0$, we have

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n \quad \text{and} \quad q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n.$$

Proof.

Let $M_n = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$ and $X_n = \begin{pmatrix} q_n & p_n \\ q_{n-1} & p_{n-1} \end{pmatrix}$. As $X_n = M_n X_{n-1}$,

$$\begin{aligned} q_n p_{n-1} - p_n q_{n-1} &= \det(X_n) = \det(M_n M_{n-1} \cdots M_0 X_{-1}) \\ &= \det(M_n) \det(M_{n-1}) \cdots \det(M_0) \det(X_{-1}) \\ &= (-1)^{n+1} \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = (-1)^n. \end{aligned}$$

In particular,

$$\begin{aligned} q_n p_{n-2} - p_n q_{n-2} &= (a_n q_{n-1} + q_{n-2}) p_{n-2} - (a_n p_{n-1} + p_{n-2}) q_{n-2} \\ &= a_n (q_{n-1} p_{n-2} - p_{n-1} q_{n-2}) = (-1)^{n-1} a_n. \end{aligned}$$

□

Identities between successive convergents

Theorem

For all $n \geq 0$, we have

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n \quad \text{and} \quad q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n.$$

Corollary

The fraction p_n/q_n is always in lowest terms.

Convergence of continued fractions

Cheat sheet

Fix $x \in \mathbb{R} \setminus \mathbb{Q}$ (so the continued fraction is infinite). We define a_n, x_n for $n \geq 0$ by

$$x_0 = x; \quad \text{and for } n \geq 0,\ a_n = \lfloor x_n \rfloor,\ x_{n+1} = \frac{1}{x_n - a_n};$$

and then p_n, q_n for $n \geq -2$ by

$$p_{-2} = 0, \quad p_{-1} = 1, \qquad p_n = a_n p_{n-1} + p_{n-2} \text{ for } n \geq 0,$$

$$q_{-2} = 1, \quad q_{-1} = 0, \qquad q_n = a_n q_{n-1} + q_{n-2} \text{ for } n \geq 0.$$

Comparison of successive convergents

Lemma

For all $n \geq 0$, we have $\frac{p_n}{q_n} < x$ if n is even, and $\frac{p_n}{q_n} > x$ if n is odd.

Proof.

The function $y \mapsto [a_0, \cdots, a_{n-1}, y]$ is a composition of n reciprocals, so it is increasing if n is even, and decreasing if n is odd.

Besides, $\frac{p_n}{q_n} = [a_0, \cdots, a_{n-1}, a_n]$ whereas $x = [a_0, \cdots, a_{n-1}, x_n]$, and $a_n = \lfloor x_n \rfloor < x_n$. □

Comparison of successive convergents

Lemma

For all $n \geq 0$, we have $\frac{p_n}{q_n} < x$ if n is even, and $\frac{p_n}{q_n} > x$ if n is odd.

Lemma

The subsequence $\dfrac{p_{2n}}{q_{2n}}$ is increasing.

The subsequence $\dfrac{p_{2n+1}}{q_{2n+1}}$ is decreasing.

Proof.

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - q_n p_{n-2}}{q_n q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}.$$

□

Convergence of continued fractions

Theorem

$$\lim_{n\to+\infty}[a_0, a_1, \cdots, a_n] = x.$$

Proof.

We have proved that

$$\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+2}}{q_{2n+2}} < x < \frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}.$$

This shows that $\dfrac{p_{2n}}{q_{2n}} \to \ell_0 \leq x$, and $\dfrac{p_{2n+1}}{q_{2n+1}} \to \ell_1 \geq x$.

But

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_n q_{n-1} - p_{n-1} q_n}{q_n q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \to 0 \rightsquigarrow \ell_0 = \ell_1 = x. \quad \square$$

Convergence of continued fractions

Theorem

$$\lim_{n \to +\infty} [a_0, a_1, \cdots, a_n] = x.$$

Corollary

Every $x \in \mathbb{R}$ can be expressed as a continued fraction.

Remark

If $x \notin \mathbb{Q}$, this expression is unique: If $x = [b_0, b_1, \cdots]$ where $b_n \in \mathbb{N}$, then $0 \leq x - b_0 = \cfrac{1}{b_1 + \cfrac{1}{\ddots}} < \frac{1}{b_1} \leq 1$,

so necessarily $b_0 = \lfloor x \rfloor$, etc.

Diophantine approximation

The quality of a rational approximation

Fix $x \in \mathbb{R} \setminus \mathbb{Q}$, and define as usual a_n, p_n, q_n.
Since $x \notin \mathbb{Q}$, we have $x \neq p/q$ for all $p, q \in \mathbb{Z}$. But as $\mathbb{Q}$ is dense in $\mathbb{R}$, we can choose p, q so that $\left| x - \frac{p}{q} \right|$ is as small as we want.

Example

For $\pi = 3.1415926535\dots$, we have $\left|\pi - \frac{314}{100}\right| < 10^{-2}$, $\left|\pi - \frac{314159}{100000}\right| < 10^{-5}$, etc.

But can we achieve $\left| x - \frac{p}{q} \right|$ small with p, q not too large?

The quality of a rational approximation

Fix $x \in \mathbb{R} \setminus \mathbb{Q}$, and define as usual a_n, p_n, q_n.
Since $x \notin \mathbb{Q}$, we have $x \neq p/q$ for all $p, q \in \mathbb{Z}$. But as $\mathbb{Q}$ is dense in $\mathbb{R}$, we can choose p, q so that $\left|x - \frac{p}{q}\right|$ is as small as we want.
But can we achieve $\left|x - \frac{p}{q}\right|$ small with p, q not too large?

Definition (Unofficial)

The quality of the approximation p/q of x is

$$\mathrm{Qual}_x(p/q) = q\left|x - \frac{p}{q}\right| = |qx - p|$$

The smaller $\mathrm{Qual}_x(p/q)$, the better the approximation. So how small can $\mathrm{Qual}_x(p/q)$ be?

Convergents are excellent approximations

Proposition

For all $n \geq 0$, we have $\dfrac{1}{q_n(q_n + q_{n+1})} < \left| x - \dfrac{p_n}{q_n} \right| < \dfrac{1}{q_n q_{n+1}}$.

Proof.

We know that $\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+2}}{q_{2n+2}} < x < \frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}}$, so for all n,

$$\left| x - \frac{p_n}{q_n} \right| < \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \frac{|p_{n+1}q_n - p_n q_{n+1}|}{q_n q_{n+1}} = \frac{|\pm 1|}{q_n q_{n+1}},$$

but also $\left| x - \dfrac{p_n}{q_n} \right| > \left| \dfrac{p_{n+2}}{q_{n+2}} - \dfrac{p_n}{q_n} \right| = \dfrac{|p_{n+2}q_n - p_n q_{n+2}|}{q_n q_{n+1}} = \dfrac{|\pm a_{n+2}|}{q_n q_{n+2}}$

$$= \frac{a_{n+2}}{q_n(a_{n+2}q_{n+1} + q_n)} = \frac{1}{q_n(q_{n+1} + \frac{q_n}{a_{n+2}})} > \frac{1}{q_n(q_n + q_{n+1})}.$$

□

Convergents are excellent approximations

Proposition

For all $n \geq 0$*, we have* $\dfrac{1}{q_n(q_n+q_{n+1})} < \left| x - \dfrac{p_n}{q_n} \right| < \dfrac{1}{q_n q_{n+1}}$.

Corollary

$\mathrm{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Convergents are excellent approximations

Proposition

For all $n \geq 0$*, we have* $\dfrac{1}{q_n(q_n+q_{n+1})} < \left| x - \dfrac{p_n}{q_n} \right| < \dfrac{1}{q_n q_{n+1}}$.

Corollary

$\operatorname{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

n	-2	-1	0	1	2	3	4
a_n			3	7	15	1	292
p_n	0	1					
q_n	1	0					

Convergents are excellent approximations

Proposition

For all $n \geq 0$, we have $$\frac{1}{q_n(q_n+q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Corollary

$\operatorname{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

n	-2	-1	0	1	2	3	4
a_n			3	7	15	1	292
p_n	0	1	3				
q_n	1	0	1				

Convergents are excellent approximations

Proposition

For all $n \geq 0$, *we have* $\dfrac{1}{q_n(q_n + q_{n+1})} < \left| x - \dfrac{p_n}{q_n} \right| < \dfrac{1}{q_n q_{n+1}}$.

Corollary

$\mathrm{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

n	-2	-1	0	1	2	3	4
a_n			3	7	15	1	292
p_n	0	1	3	22			
q_n	1	0	1	7			

Convergents are excellent approximations

Proposition

For all $n \geq 0$, we have $$\frac{1}{q_n(q_n+q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Corollary

$\operatorname{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

n	-2	-1	0	1	2	3	4
a_n			3	7	15	1	292
p_n	0	1	3	22	333		
q_n	1	0	1	7	106		

Convergents are excellent approximations

Proposition

For all $n \geq 0$*, we have* $\dfrac{1}{q_n(q_n+q_{n+1})} < \left| x - \dfrac{p_n}{q_n} \right| < \dfrac{1}{q_n q_{n+1}}$.

Corollary

$\operatorname{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

n	-2	-1	0	1	2	3	4
a_n			3	7	15	1	292
p_n	0	1	3	22	333	355	
q_n	1	0	1	7	106	113	

Convergents are excellent approximations

Proposition

For all $n \geq 0$, we have $$\frac{1}{q_n(q_n+q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Corollary

$\mathrm{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

$$[3] = 3$$

$$\pi = 3.14159265358979\cdots$$

Convergents are excellent approximations

Proposition

For all $n \geq 0$, *we have* $\dfrac{1}{q_n(q_n+q_{n+1})} < \left| x - \dfrac{p_n}{q_n} \right| < \dfrac{1}{q_n q_{n+1}}$.

Corollary

$\operatorname{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

$$[3,7] = \frac{22}{7} = 3.14285714285714$$

$$\pi = 3.14159265358979\cdots$$

Convergents are excellent approximations

Proposition

For all $n \geq 0$*, we have* $\frac{1}{q_n(q_n+q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}$.

Corollary

$\mathrm{Qual}_x(p_n/q_n) < \frac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

$$[3,7,15] = \frac{333}{106} = 3.14150943396226\cdots$$

$$\pi = 3.14159265358979\cdots$$

Convergents are excellent approximations

Proposition

For all $n \geq 0$, we have $$\frac{1}{q_n(q_n + q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Corollary

$\operatorname{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ *tends to* 0.

Example

With $x = \pi$, we get

$$\begin{aligned} [3,7,15,1] &= \frac{355}{113} = 3.14159292035398\cdots \\ \pi &= 3.14159265358979\cdots \end{aligned}$$

Convergents are excellent approximations

Corollary

$\mathrm{Qual}_x(p_n/q_n) < \dfrac{1}{q_{n+1}}$ tends to 0.

Corollary

For any $x \in \mathbb{R} \setminus \mathbb{Q}$, we can find $p, q \in \mathbb{Z}$ such that $\mathrm{Qual}_x(p/q)$ is arbitrarily small.

Counter-example

Not true if $x \in \mathbb{Q}$! Indeed, if $x = a/b$, then unless $p/q = x$,

$$\mathrm{Qual}_x(p/q) = q\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|qa - pb|}{b} \geq \frac{1}{b}.$$

Convergents are the best!

Theorem

Let $x \in \mathbb{R} \setminus \mathbb{Q}$*, and let* $p, q \in \mathbb{Z}$*.*
For all $n \geq 0$*, if* $q \leq q_n$*, then* $\operatorname{Qual}_x(p/q) > \operatorname{Qual}_x(p_n/q_n)$ *unless* $p/q = p_n/q_n$*.*
Conversely, if $\operatorname{Qual}_x(p/q) < \frac{1}{2q}$*, then* $p/q = p_n/q_n$ *for some* n*.*

Convergents are the best!

Theorem

For all $n \geq 0$*, if* $q \leq q_n$*, then* $\operatorname{Qual}_x(p/q) > \operatorname{Qual}_x(p_n/q_n)$ *unless* $p/q = p_n/q_n$*.*

Proof.

Fix n, let $q \leq q_n$, and suppose $p/q \neq p_n/q_n$. The linear system

$$\begin{cases} p_n y + p_{n-1} z = p \\ q_n y + q_{n-1} z = q \end{cases}$$

in y, z can be written $AX = B$, where $X = \left(\begin{smallmatrix} y \\ z \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} p \\ q \end{smallmatrix}\right) \in \mathbb{Z}^2$, and $A = \left(\begin{smallmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$, so its only solution $X = A^{-1}B$ lies in $\mathbb{Z}^2$. We can assume y, z both nonzero: if $y = 0$ then $p/q = p_{n-1}/q_{n-1}$ is less good, and if $z = 0$ then $p/q = p_n/q_n$. Finally, y and z have opposite signs since $q = q_n y + q_{n-1} z$, so $y(q_n x - p_n)$ and $z(q_{n-1}x - p_{n-1})$ have the same sign. Thus

$$|qx - p| = |y(q_n x - p_n)| + |z(q_{n-1}x - p_{n-1})|.$$

□

Convergents are the best!

Theorem

Conversely, if $\mathrm{Qual}_x(p/q) < \frac{1}{2q}$, *then* $p/q = p_n/q_n$ *for some* n.

Proof.

Write $qx - p = \epsilon\theta/q$ with $\epsilon = \pm 1$ and $\theta \in (0, \frac{1}{2})$, so $x = \frac{p+\epsilon\theta/q}{q}$.
Expand $p/q = [a'_0, \cdots, a'_n]$, and let p'_m/q'_m be its convergents.
WLOG $\gcd(p,q) = 1$, so $p'_n = p$ and $q'_n = q$.
If $a'_n > 1$, then also $p/q = [a'_0, \cdots, a'_n - 1, 1]$, so we may choose the parity of n so that $q'_n p'_{n-1} - p'_n q'_{n-1} = (-1)^n = \epsilon$.
Define $y = \frac{1}{\theta} - \frac{q'_{n-1}}{q'_n} = [b_0, b_1, \cdots]$; then $b_0 = \lfloor y \rfloor \geq 1$, and

$$[a'_0, \cdots, a'_n, b_0, b_1, \cdots] = [a'_0, \cdots, a'_n, y] = \frac{yp'_n + p'_{n-1}}{yq'_n + q'_{n-1}}$$

$$= \frac{\frac{p'_n}{\theta} - p'_n \frac{q'_{n-1}}{q'_n} + p'_{n-1}}{q'_n/\theta - q'_{n-1} + q'_{n-1}} = \frac{\frac{p'_n}{\theta} + \frac{-p'_n q'_{n-1} + q'_n p'_{n-1}}{q'_n}}{q'_n/\theta} = \frac{p + \epsilon\theta/q}{q} = x. \quad \square$$

Continued fractions attached to quadratic irrationals

Quadratic irrationals

Definition

Fix $d \in \mathbb{Z}$ *not a square, so* $\sqrt{d} \notin \mathbb{Q}$*, and introduce*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}, \quad \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

Given $\alpha = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$*, we define*

$$\overline{\alpha} = a - b\sqrt{d} \in \mathbb{Q}[\sqrt{d}], \qquad N(\alpha) = \alpha\overline{\alpha} = a^2 - db^2 \in \mathbb{Q}.$$

Proposition

$\mathbb{Z}[\sqrt{d}]$ *is a* <u>*ring*</u>*: if* $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$*, then* $\alpha + \beta, \alpha - \beta, \alpha\beta \in \mathbb{Z}[\sqrt{d}]$.

$\mathbb{Q}[\sqrt{d}]$ *is a* <u>*field*</u>*: if* $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$*, then* $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in \mathbb{Q}[\sqrt{d}]$.

Proof.

$$(a + b\sqrt{d}) \pm (a' + b'\sqrt{d}) = (a \pm a') + (b \pm b')\sqrt{d}.$$

$$(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + bb'd) + (ab' + ba')\sqrt{d}.$$

$$\alpha/\beta = (\alpha\overline{\beta})/(\beta\overline{\beta}) = (\alpha\overline{\beta})/N(\beta).$$

□

Properties of the norm

Lemma

Fix $d \in \mathbb{Z}$ not a square, and let $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$.

1. $N(\alpha\beta) = N(\alpha)N(\beta)$.
2. $\overline{\alpha+\beta} = \overline{\alpha} + \overline{\beta}, \quad \overline{\alpha-\beta} = \overline{\alpha} - \overline{\beta}, \quad \overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}, \quad \overline{\alpha/\beta} = \overline{\alpha}/\overline{\beta}$.

Proof.

1. If $\alpha = a + b\sqrt{d}$, then
$$N(\alpha) = \begin{vmatrix} a & bd \\ b & a \end{vmatrix} = \det\left(\mu_\alpha : \begin{array}{ccc} \mathbb{Q}[\sqrt{d}] & \longrightarrow & \mathbb{Q}[\sqrt{d}] \\ x & \longmapsto & \alpha x \end{array}\right);$$
and $\det(\mu_{\alpha\beta}) = \det(\mu_\alpha \circ \mu_\beta) = \det(\mu_\alpha)\det(\mu_\beta)$.
2. Clear for $\alpha \pm \beta$.
$$\overline{\alpha}\,\overline{\beta} = \frac{N(\alpha)}{\alpha}\frac{N(\beta)}{\beta} = \frac{N(\alpha)N(\beta)}{\alpha\beta} = \frac{N(\alpha\beta)}{\alpha\beta} = \overline{\alpha\beta};$$
same proof for α/β. □

Quadratic irrationals

Definition

A quadratic irrational is an element of $\mathbb{Q}[\sqrt{d}] \setminus \mathbb{Q}$ *for some* $d \in \mathbb{Z}_{\geq 2}$*, i.e. of the form* $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathbb{R} \setminus \mathbb{Q}$ *with* $a, b, c \in \mathbb{Z}$ *with* $b, c \neq 0$*.*

Theorem (Euler + Lagrange)

Let $x \in \mathbb{R} \setminus \mathbb{Q}$*. Then* x *is a quadratic irrational iff. its continued fraction expansion is ultimately periodic.*

Quadratic irrationals

Theorem (Euler + Lagrange)

Let $x \in \mathbb{R} \setminus \mathbb{Q}$. Then x is a quadratic irrational iff. its continued fraction expansion is ultimately periodic.

Example

$$[1, 2, 3, 4, 5, 3, 4, 5, 3, 4, 5, \cdots] = [1, 2, \overline{3, 4, 5}] = \frac{103 + \sqrt{1297}}{97}.$$

$$\sqrt{6} = [2, 2, 4, 2, 4, 2, 4, 2, 4, \cdots] = [2, \overline{2, 4}].$$

Counter-example

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, \cdots].$$

$$\sqrt[3]{2} = [1, 3, 1, 5, 1, 1, 4, 1, 1, 8, 1, 14, 1, 10, 2, \cdots].$$

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, \cdots].$$

Ultimately periodic $\Longrightarrow$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1				
q_n	1	0				

Ultimately periodic $\Longrightarrow$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3			
q_n	1	0	1			

Ultimately periodic $\implies$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13		
q_n	1	0	1	4		

Ultimately periodic $\implies$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	
q_n	1	0	1	4	21	

Ultimately periodic $\implies$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	$68y+13$
q_n	1	0	1	4	21	$21y+4$

Ultimately periodic $\Longrightarrow$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	$68y+13$
q_n	1	0	1	4	21	$21y+4$

So $y = \dfrac{68y+13}{21y+4} \rightsquigarrow 21y^2 - 64y - 13 = 0 \rightsquigarrow y = \dfrac{32+\sqrt{1297}}{21}$.

Ultimately periodic $\implies$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	$68y+13$
q_n	1	0	1	4	21	$21y+4$

So $y = \dfrac{68y+13}{21y+4} \rightsquigarrow 21y^2 - 64y - 13 = 0 \rightsquigarrow y = \dfrac{32+\sqrt{1297}}{21}$.

Finally, $x = [1, 2, y]$,

n	-2	-1	0	1	2
a_n			1	2	y
p_n	0	1			
q_n	1	0			

whence

Ultimately periodic $\Longrightarrow$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	$68y+13$
q_n	1	0	1	4	21	$21y+4$

So $y = \dfrac{68y+13}{21y+4} \rightsquigarrow 21y^2 - 64y - 13 = 0 \rightsquigarrow y = \dfrac{32+\sqrt{1297}}{21}$.

Finally, $x = [1, 2, y]$,

n	-2	-1	0	1	2
a_n			1	2	y
p_n	0	1	1		
q_n	1	0	1		

whence

Ultimately periodic $\implies$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	$68y+13$
q_n	1	0	1	4	21	$21y+4$

So $y = \dfrac{68y+13}{21y+4} \rightsquigarrow 21y^2 - 64y - 13 = 0 \rightsquigarrow y = \dfrac{32+\sqrt{1297}}{21}$.

Finally, $x = [1, 2, y]$,

n	-2	-1	0	1	2
a_n			1	2	y
p_n	0	1	1	3	
q_n	1	0	1	2	

whence

Ultimately periodic $\implies$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	$68y+13$
q_n	1	0	1	4	21	$21y+4$

So $y = \dfrac{68y+13}{21y+4} \rightsquigarrow 21y^2 - 64y - 13 = 0 \rightsquigarrow y = \dfrac{32+\sqrt{1297}}{21}$.

Finally, $x = [1,2,y]$,

n	-2	-1	0	1	2
a_n			1	2	y
p_n	0	1	1	3	$3y+1$
q_n	1	0	1	2	$2y+1$,

whence

Ultimately periodic $\implies$ Quadratic irrational

Let $x = [1, 2, \overline{3, 4, 5}]$. Introduce $y = [\overline{3, 4, 5}] = [3, 4, 5, y]$.

n	-2	-1	0	1	2	3
a_n			3	4	5	y
p_n	0	1	3	13	68	$68y+13$
q_n	1	0	1	4	21	$21y+4$

So $y = \dfrac{68y+13}{21y+4} \rightsquigarrow 21y^2 - 64y - 13 = 0 \rightsquigarrow y = \dfrac{32+\sqrt{1297}}{21}$.

Finally, $x = [1, 2, y]$,

n	-2	-1	0	1	2
a_n			1	2	y
p_n	0	1	1	3	$3y+1$
q_n	1	0	1	2	$2y+1$,

whence

$$x = \frac{3y+1}{2y+1} = \frac{(117+3\sqrt{1297})/21}{(85+2\sqrt{1297})/21} = \frac{(117+3\sqrt{1297})(85-2\sqrt{1297})}{(85+2\sqrt{1297})(85-2\sqrt{1297})} = \frac{103+\sqrt{1297}}{97}.$$

Ultimately periodic $\implies$ Quadratic irrational

Suppose $x = [a_0, a_1, \cdots, a_r, \overline{b_0, b_1, \cdots, b_s}]$.

Let $y = [\overline{b_0, b_1, \cdots, b_s}] = [b_0, b_1, \cdots, b_s, y]$.

Then $y = \dfrac{yp_s + p_{s-1}}{yq_s + q_{s-1}}$ satisfies an equation of degree 2

$\rightsquigarrow y = \frac{-B \pm \sqrt{\Delta}}{2A} \in \mathbb{Q}[\sqrt{\Delta}]$. Besides, $y \in \mathbb{R}$ so $\Delta > 0$.

So $x = [a_0, a_1, \cdots, a_r, y] = \dfrac{yp_r + p_{r-1}}{yq_r + q_{r-1}} \in \mathbb{Q}[\sqrt{\Delta}]$,
and $x \notin \mathbb{Q}$ since its continued fraction expansion is infinite. □

Quadratic irrational $\implies$ Ultimately periodic

Let $x = \frac{a+b\sqrt{d}}{c}$ be a quadratic irrational.

Change the sign of $a, b, c \rightsquigarrow$ WLOG $b > 0$.

Then $x = \frac{a+\sqrt{b^2 d}}{c} = \frac{a|c|+\sqrt{b^2 c^2 d}}{c|c|} = \frac{R+\sqrt{D}}{S}$,
where $R = a|c|, S = c|c|$ satisfy

$R, S \in \mathbb{Z}$, $S \neq 0$, and $D - R^2 = b^2 c^2 d - a^2 c^2$ is divisible by S.

Imagine we begin the continued fraction: we get $x_1 = \frac{1}{x - \lfloor x \rfloor}$

$= \frac{1}{\frac{R+\sqrt{D}}{S} - \lfloor x \rfloor} = \frac{1}{\frac{R - \lfloor x \rfloor S + \sqrt{D}}{S}} = \frac{1}{\frac{-R'+\sqrt{D}}{S}} = \frac{R'+\sqrt{D}}{\frac{(-R'+\sqrt{D})(R'+\sqrt{D})}{S}} = \frac{R'+\sqrt{D}}{S'}$,
where $R' = \lfloor x \rfloor S - R$, $S' = \frac{D - R'^2}{S}$ satisfy again $R', S' \in \mathbb{Z}$,
$S' \neq 0$, and $S' \mid (D - R'^2)$ since $SS' = D - R'^2$.

Thus for all $n \geq 0$, $x_n = \frac{R_n + \sqrt{D}}{S_n}$ with $R_n, S_n \in \mathbb{Z}$ and D fixed;
furthermore $S_n S_{n+1} = D - R_{n+1}^2$.

Quadratic irrational $\Longrightarrow$ Ultimately periodic

Thus for all $n \geq 0$, $x_n = \frac{R_n + \sqrt{D}}{S_n}$ with $R_n, S_n \in \mathbb{Z}$ and D fixed; furthermore $S_n S_{n+1} = D - R_{n+1}^2$.

Now $x = [a_0, a_1, \cdots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}$. Solve for x_n:

$$x x_n q_{n-1} + x q_{n-2} = x_n p_{n-1} + p_{n-2}$$

$$\rightsquigarrow x_n = -\frac{x q_{n-1} - p_{n-1}}{x q_{n-2} - p_{n-2}} = -\frac{q_{n-1}}{q_{n-2}} \frac{x - \frac{p_{n-1}}{q_{n-1}}}{x - \frac{p_{n-2}}{q_{n-2}}}.$$

Take conjugates: $\dfrac{R_n - \sqrt{D}}{S_n} = \overline{x_n} = -\dfrac{q_{n-1}}{q_{n-2}} \dfrac{\overline{x} - \frac{p_{n-1}}{q_{n-1}}}{\overline{x} - \frac{p_{n-2}}{q_{n-2}}}$.

But when $n \to \infty$, $\dfrac{\overline{x} - \frac{p_{n-1}}{q_{n-1}}}{\overline{x} - \frac{p_{n-2}}{q_{n-2}}} \to \dfrac{\overline{x} - x}{\overline{x} - x} = 1$; so for n large enough,

$$\overline{x_n} < 0 \rightsquigarrow \frac{2\sqrt{D}}{S_n} = x_n - \overline{x_n} > 1 > 0 \rightsquigarrow S_n > 0.$$

Quadratic irrational $\Longrightarrow$ Ultimately periodic

For n large enough, $S_n > 0$; besides, $S_n S_{n+1} = D - R_{n+1}^2$.

Thus for n large enough, $|R_n| \leq \sqrt{D}$ and $S_n \leq D$.

$\rightsquigarrow$ The pair (R_n, S_n) takes finitely many values

$\rightsquigarrow$ There exist $n, m > 0$ such that

$$x_{n+m} = \frac{R_{n+m} + \sqrt{D}}{S_{n+m}} = \frac{R_n + \sqrt{D}}{S_{n+m}} = x_n,$$

and the process is periodic from there on. □

Quadratic irrational $\implies$ Ultimately periodic

Example

Let $x = \sqrt{6}$. We compute

n	0	1	2	3
x_n	$\sqrt{6}$			
a_n				

Quadratic irrational $\Longrightarrow$ Ultimately periodic

Example

Let $x = \sqrt{6}$. We compute

n	0	1	2	3
x_n	$\sqrt{6}$	$\frac{1}{\sqrt{6}-2} = \frac{2+\sqrt{6}}{2}$		
a_n	2			

Quadratic irrational $\implies$ Ultimately periodic

Example

Let $x = \sqrt{6}$. We compute

n	0	1	2	3
x_n	$\sqrt{6}$	$\frac{1}{\sqrt{6}-2} = \frac{2+\sqrt{6}}{2}$	$\frac{1}{\frac{2+\sqrt{6}}{2}-2} = 2+\sqrt{6}$	
a_n	2	2		

Quadratic irrational $\implies$ Ultimately periodic

Example

Let $x = \sqrt{6}$. We compute

n	0	1	2	3
x_n	$\sqrt{6}$	$\frac{1}{\sqrt{6}-2} = \frac{2+\sqrt{6}}{2}$	$\frac{1}{\frac{2+\sqrt{6}}{2}-2} = 2+\sqrt{6}$	$\frac{1}{2+\sqrt{6}-4} = x_1$
a_n	2	2	4	

Quadratic irrational $\implies$ Ultimately periodic

Example

Let $x = \sqrt{6}$. We compute

n	0	1	2	3
x_n	$\sqrt{6}$	$\frac{1}{\sqrt{6}-2} = \frac{2+\sqrt{6}}{2}$	$\frac{1}{\frac{2+\sqrt{6}}{2}-2} = 2+\sqrt{6}$	$\frac{1}{2+\sqrt{6}-4} = x_1$
a_n	2	2	4	

So the process repeats itself from there on.

$$\rightsquigarrow \sqrt{6} = \sqrt{6} = [2, 2, 4, 2, 4, 2, 4, 2, 4, \cdots] = [2, \overline{2, 4}].$$

The Pell-Fermat equation

The equation

Fix $d \in \mathbb{N}$, not a square.

We want to solve the Diophantine equation

$$x^2 - dy^2 = 1 \qquad (x, y \in \mathbb{Z})$$

Trivial solutions: $x = \pm 1$, $y = 0$. Are there more?

Remark

If $d = n^2$ were a square, then
$x^2 - dy^2 = x^2 - (ny)^2 = (x + ny)(x - ny) \rightsquigarrow$ not interesting.

Example

$d = 2$: are solutions of $x^2 - 2y^2 = 1$.

$d = 61$: The smallest solution to $x^2 - 61y^2 = 1$ is

The equation

Fix $d \in \mathbb{N}$, not a square.

We want to solve the Diophantine equation

$$x^2 - dy^2 = 1 \qquad (x, y \in \mathbb{Z})$$

Trivial solutions: $x = \pm 1$, $y = 0$. Are there more?

Remark

If $d = n^2$ were a square, then
$x^2 - dy^2 = x^2 - (ny)^2 = (x + ny)(x - ny) \rightsquigarrow$ not interesting.

Example

$d = 2$: $(\pm 3, \pm 2)$, $(\pm 17, \pm 12)$ are solutions of $x^2 - 2y^2 = 1$.

$d = 61$: The smallest solution to $x^2 - 61y^2 = 1$ is

The equation

Fix $d \in \mathbb{N}$, not a square.

We want to solve the Diophantine equation

$$x^2 - dy^2 = 1 \qquad (x, y \in \mathbb{Z})$$

Trivial solutions: $x = \pm 1$, $y = 0$. Are there more?

Remark

If $d = n^2$ were a square, then
$x^2 - dy^2 = x^2 - (ny)^2 = (x + ny)(x - ny) \rightsquigarrow$ not interesting.

Example

$d = 2$: $(\pm 3, \pm 2)$, $(\pm 17, \pm 12)$ are solutions of $x^2 - 2y^2 = 1$.

$d = 61$: The smallest solution to $x^2 - 61y^2 = 1$ is

$$x = 1766319049, \qquad y = 226153980.$$

Interpretation: units in real quadratic fields

Recall that $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$ is a ring.

Lemma

Let $\alpha \in \mathbb{Z}[\sqrt{d}]$. Then $\alpha \in \mathbb{Z}[\sqrt{d}]^\times$, i.e. $1/\alpha \in \mathbb{Z}[\sqrt{d}]$, iff. $N(\alpha) \in \mathbb{Z}^\times$, i.e. $N(\alpha) = \pm 1$.

Proof.

If $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ are such that $\alpha\beta = 1$, then

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1.$$

Conversely, if $N(\alpha) = \pm 1$, then

$$\frac{1}{\alpha} = \pm\frac{N(\alpha)}{\alpha} = \pm\frac{\alpha\overline{\alpha}}{\alpha} = \pm\overline{\alpha} \in \mathbb{Z}[\sqrt{d}].$$

□

Interpretation: units in real quadratic fields

Recall that $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$ is a ring.

Lemma

Let $\alpha \in \mathbb{Z}[\sqrt{d}]$. Then $\alpha \in \mathbb{Z}[\sqrt{d}]^\times$, i.e. $1/\alpha \in \mathbb{Z}[\sqrt{d}]$, iff. $N(\alpha) \in \mathbb{Z}^\times$, i.e. $N(\alpha) = \pm 1$.

Relation with the Pell-Fermat equation:

$$N(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2,$$

so $x^2 - dy^2 = 1 \iff x + y\sqrt{d}$ is a unit of norm $+1$.

Example

Trivial solutions $x = \pm 1,\ y = 0 \longleftrightarrow$ trivial units $\pm 1 \in \mathbb{Z}[\sqrt{d}]^\times$.

Dirichlet's theorem

Theorem (Dirichlet; accepted without proof)

Let $d \in \mathbb{N}$, not a square. There exists a fundamental unit $\varepsilon \in \mathbb{Z}[\sqrt{d}]^\times$, $\varepsilon \neq \pm 1$ such that

$$\mathbb{Z}[\sqrt{d}]^\times = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}.$$

Remark

$\varepsilon \neq \pm 1$, so $|\varepsilon| \neq 1$, so $\varepsilon^n \neq \pm 1$ unless $n = 0$; thus $\#\mathbb{Z}[\sqrt{d}]^\times = \infty$.

Dirichlet's theorem

Theorem (Dirichlet; accepted without proof)

Let $d \in \mathbb{N}$, not a square. There exists a fundamental unit $\varepsilon \in \mathbb{Z}[\sqrt{d}]^\times$, $\varepsilon \neq \pm 1$ such that

$$\mathbb{Z}[\sqrt{d}]^\times = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}.$$

Remark (How unique is ε?)

We could replace ε with $\pm \varepsilon^{\pm 1}$.
As $N(\varepsilon) = \pm 1$, if $\varepsilon = a + b\sqrt{d}$, then
$\varepsilon^{-1} = \pm N(\varepsilon)/\varepsilon = \pm \overline{\varepsilon} = \pm(a - b\sqrt{d})$, hence $\pm \varepsilon^{\pm 1} = \pm a \pm b\sqrt{d}$.

It is customary to choose $a, b > 0$, so that $\varepsilon > 1$.
Then for $n \in \mathbb{N}$, we have $\varepsilon^n = a_n + b_n\sqrt{d}$ with $a_n, b_n \in \mathbb{N}$ and increasing, so ε corresponds to the smallest solution to $x^2 - dy^2 = \pm 1$.

Dirichlet's theorem

Theorem (Dirichlet; accepted without proof)

Let $d \in \mathbb{N}$, not a square. There exists a <u>*fundamental unit*</u> $\varepsilon \in \mathbb{Z}[\sqrt{d}]^\times$, $\varepsilon \neq \pm 1$ *such that*

$$\mathbb{Z}[\sqrt{d}]^\times = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}.$$

Let $u = \pm \varepsilon^n \in \mathbb{Z}[\sqrt{d}]^\times$. Then $N(u) = N(\pm 1) N(\varepsilon)^n = N(\varepsilon)^n$, as $N(-1) = +1$. Thus

- If $N(\varepsilon) = +1$, then $N(u) = +1$ for all n
  $\rightsquigarrow$ Solutions of $x^2 - dy^2 = 1 \longleftrightarrow \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}$.
- If $N(\varepsilon) = -1$, then $N(u) = +1$ iff. n is even
  $\rightsquigarrow$ Solutions of $x^2 - dy^2 = 1 \longleftrightarrow \{\pm \varepsilon^{2n} \mid n \in \mathbb{Z}\}$.

Corollary

For all $d \in \mathbb{N}$ not square, $x^2 - dy^2 = 1$ has ∞ solutions.

Solving Pell-Fermat

If $x = a > 0$, $y = b > 0$ is a solution to $x^2 - dy^2 = \pm 1$, then

$$\left|\frac{a}{b} - \sqrt{d}\right| = \frac{\left|\frac{a}{b} - \sqrt{d}\right|\left|\frac{a}{b} + \sqrt{d}\right|}{\left|\frac{a}{b} + \sqrt{d}\right|} = \frac{\left|\frac{a^2}{b^2} - d\right|}{\frac{a}{b} + \sqrt{d}} = \frac{|a^2 - db^2|}{b(a + b\sqrt{d})} = \frac{1}{b(a + b\sqrt{d})}$$

is very small, so a/b approximates $\sqrt{d}$.

More specifically, since $a = \sqrt{db^2 \pm 1} \geq b\sqrt{d - 1/b^2} \geq b$, we have

$$\operatorname{Qual}_{\sqrt{d}}(a/b) = |a - b\sqrt{d}| = \frac{1}{a + b\sqrt{d}} < \frac{1}{a + b} \leq \frac{1}{2b},$$

so a/b is a convergent of $\sqrt{d}$!

$\rightsquigarrow$ All the solutions to $x^2 - dy^2 = \pm 1$, in particular the fundamental one, are among the convergents of $\sqrt{d}$.

Example: $x^2 - 3y^2 = 1$

Continued fraction expansion of $\sqrt{3}$:

n	x_n	a_n	p_n	q_n	$p_n^2 - 3q_n^2$
-2			0	1	
-1			1	0	
0	$\sqrt{3}$	1	1	1	-2 ✗
1	$\frac{1}{\sqrt{3}-1} = \frac{1+\sqrt{3}}{2}$	1	2	1	$+1$ ✓

$\rightsquigarrow$ The fundamental unit of $\mathbb{Z}[\sqrt{3}]$ is $\varepsilon = 2 + \sqrt{3}$, norm $+1$.

$\rightsquigarrow$ The fundamental solution to $x^2 - 3y^2 = 1$ is $x = 2$, $y = 1$.

Other solutions:

- $(2+\sqrt{3})^2 = 7 + 4\sqrt{3} \rightsquigarrow x = 7, \; y = 4.$
- $(2+\sqrt{3})^3 = 26 + 15\sqrt{3} \rightsquigarrow x = 26, \; y = 15.$
- $\vdots$

Example: $x^2 - 2y^2 = 1$

Continued fraction expansion of $\sqrt{2}$:

n	x_n	a_n	p_n	q_n	$p_n^2 - 2q_n^2$
-2			0	1	
-1			1	0	
0	$\sqrt{2}$	1	1	1	-1 ✓

$\rightsquigarrow$ The fundamental unit of $\mathbb{Z}[\sqrt{2}]$ is $\varepsilon = 1 + \sqrt{2}$, norm -1.

$\rightsquigarrow$ As $(1+\sqrt{2})^2 = 3 + 2\sqrt{2}$, the fundamental solution to $x^2 - 2y^2 = 1$ is $x = 3$, $y = 2$.

Other solutions:

- $(1+\sqrt{2})^4 = (3+\sqrt{2})^2 = 17 + 12\sqrt{2} \rightsquigarrow x = 17, \; y = 12.$
- $(1+\sqrt{2})^6 = (3+2\sqrt{2})^3 = 99 + 70\sqrt{2} \rightsquigarrow x = 99, \; y = 70.$
- $\vdots$