

CONTINUED FRACTIONS AND FACTORING

Niels Lauritzen

NIELS LAURITZEN
DEPARTMENT OF MATHEMATICAL SCIENCES
UNIVERSITY OF AARHUS, DENMARK

EMAIL: niels@imf.au.dk

URL: <http://home.imf.au.dk/niels/>

Contents

1	Factoring using continued fractions	1
1.0.1	The Fermat-Kraitchik method	1
2	Continued fractions	5
2.1	The game that might never stop	5
2.1.1	Rational numbers	6
2.2	Basic theory of continued fractions	7
2.3	Eulers rule and corollaries	8
2.4	Continued fraction for a real number	10
2.5	Quadratic irrationalities	11
2.5.1	Purely periodic continued fractions	12
2.6	The continued fraction for \sqrt{N}	15
2.7	A few words on Pells equation	16
3	Exercises	17
3.1	In class	17
3.2	Homework	17

Chapter 1

Factoring using continued fractions

The statement that every integer can be written as a product of prime numbers is a typical mathematical statement with a simple proof. Things become much more complicated when you (inspired by Gauss) ask for a good algorithm for factoring a given integer N . In a non-trivial factorization $N = ab$ one of the factors a and b must be $\leq \sqrt{N}$. If N is even 2 divides and we have found a factor. If N is odd we may find a factor of N , by starting with 3 and try dividing with odd numbers up to \sqrt{N} . This procedure is called *trial division*. The number of steps in trial division is proportional to the smallest prime factor p . This is extremely slow. If you want to factor a 100 digit number, which is the product of two 50 digit prime numbers, you must carry out approximately 10^{50} steps of trial division. If every step takes 10^{-10} seconds, you will have to wait for 10^{40} seconds (or approximately 10^{32} years). There are better algorithms.

1.0.1 The Fermat-Kraitchik method

Currently the most effective algorithms for factoring “difficult integers” originates in the historic fact that if an integer N can be written as the difference $x^2 - y^2$ between two squares, we have the factorization

$$N = x^2 - y^2 = (x + y)(x - y).$$

On the other hand if an odd number $N = uv$ is composite, then

$$N = \left(\frac{u+v}{2}\right)^2 - \left(\frac{u-v}{2}\right)^2.$$

This method of factoring goes back to Fermat. Suppose we wish to factor N . Fermat’s method would start with the function

$$S(x) = x^2 - N$$

and search for x , such that $S(x) = y^2$ is square. Usually one runs through $x = [\sqrt{N}], x = [\sqrt{N}] + 1, \dots$, where $[\sqrt{N}]$ denotes the integral part of \sqrt{N} . Putting $N = 2491$, one would find $S(49) = -90, S(50) = 9 = 3^2$. This means that $2491 = (50 + 3)(50 - 3) = 53 \cdot 47$. Of course using this method on a composite number (like 2^{1000}) works just as terribly as trial division. There is a beautiful variation of Fermat's method (due to M. Kraitchik (1882–1957)) using congruences. The insight is that it usually suffices that N divides $x^2 - y^2$ to find a factor of N . This means that

$$N \mid x^2 - y^2 = (x + y)(x - y).$$

Now if N does not divide any of $x + y$ and $x - y$, then we may conclude that $\gcd(x + y, N) > 1$ and use the Euclidean algorithm to find $\gcd(N, x + y)$, which is a non-trivial factor of N . So one should look for solutions x, y such that

$$\begin{aligned} x^2 &\equiv y^2 \pmod{N} \\ x &\not\equiv \pm y \pmod{N}. \end{aligned}$$

Suppose we have collected x_1, \dots, x_n , such that $x_1^2 \equiv a_1 \pmod{N}, \dots, x_n^2 \equiv a_n \pmod{N}$ for some integers a_1, \dots, a_n . If a subset a_{i_1}, \dots, a_{i_r} of a_1, a_2, \dots, a_n satisfies that $a_{i_1} \cdots a_{i_r}$ is a square, then

$$(x_{i_1} \cdots x_{i_r})^2 \equiv a_{i_1} \cdots a_{i_r} \pmod{N}$$

and we have our congruence $x^2 \equiv y^2 \pmod{N}$. This congruence may or may not satisfy $x \not\equiv \pm y \pmod{N}$. To tell if a number n is square we factor it

$$n = p_1^{n_1} \cdots p_r^{n_r}$$

using some predefined factor basis $P = \{p_1, \dots, p_r\}$ of (small) prime numbers. Now n is a square if and only if all the exponents n_1, \dots, n_r are even.

Exercise 1.0.1 Suppose that the prime factorizations of a_1, \dots, a_n over the factor basis P (assume all a 's factor completely using primes from P) are

$$\begin{aligned} a_1 &= p_1^{m_{11}} \cdots p_r^{m_{1r}} \\ a_2 &= p_1^{m_{21}} \cdots p_r^{m_{2r}} \\ &\vdots \\ a_n &= p_1^{m_{n1}} \cdots p_r^{m_{nr}}. \end{aligned}$$

Use linear algebra over $\mathbb{Z}/2\mathbb{Z}$ to find a subset i_1, \dots, i_r of $1, 2, \dots, n$ such that $a_{i_1} \cdots a_{i_r}$ is a square.

Let us apply this to the numbers we get from the function $S(x) = x^2 - N$. Notice that $x^2 \equiv S(x) \pmod{N}$. We wish to find values x_1, \dots, x_n , such that the product of a suitable subset of the numbers $S(x_1), \dots, S(x_n)$ is a square. For $N = 2041$ (this example is from [1]) we illustrate this in the table below

x	$x^2 - N$	Factorization	Marked
46	75	3×5^2	✓
47	168	$2^3 \times 3 \times 7$	✓
48	263	263	
49	360	$2^3 \times 3^2 \times 5$	✓
50	459	$3^3 \times 17$	
51	560	$2^4 \times 5 \times 7$	✓

The above table shows that $S(46)S(47)S(49)S(51) = 75 \cdot 168 \cdot 360 \cdot 560 = (2^5 \cdot 3^2 \cdot 5^2 \cdot 7)^2$ is a square. Putting $u = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7$, we get $u^2 = 50400^2 \equiv 1416^2 \pmod{2041}$. Now we know that $u^2 \equiv v^2 \pmod{2041}$ where $v = 46 \cdot 47 \cdot 49 \cdot 51 = 5402838 \equiv 311 \pmod{2041}$. Using the Euclidean algorithm one finds the greatest common divisor of $u - v = 1416 - 311 = 1105$ and 2041, which is 13. We have found the factorization $2041 = 13 \cdot 157$. Using the original method of Fermat we would have to wait until $x = 80$ before having a subset whose product is a square. The heavy part of the algorithm is factoring $S(x) = x^2 - N$. Around 1982 Pomerance discovered a nice trick to avoid this. The observation is that a prime power p^r divides $S(x)$ if and only if it divides $S(x + kp^r)$, where $k \in \mathbb{Z}$. So if one can locate a number x such that $p^r \mid S(x)$, then we know in advance that $p^r \mid S(x + p^r), S(x + 2p^r), \dots$. This is a so-called sieving procedure (like the sieve of Eratosthenes eliminating multiples of prime numbers). It leads to the factorization algorithm called the quadratic sieve. In [1] you can find a nice description of this and other sieving methods for factoring. These are currently the most effective factoring the challenges issued by RSA. In fact the RSA challenge with 155 digits was factored using sieving.

We will however describe the champion of factoring preceeding the quadratic sieve, the continued fraction algorithm. This is in order to get involved in some fantastic 19th century mathematics and show how an idea from the heart of mathematics can be applied in easing factoring.

The problem with Fermats method is that $S(x) = x^2 - N$ grows too rapidly. It takes longer and longer to factor $S(x)$. One can instead use "convergents" s_n/t_n in the continued fraction expansion of \sqrt{N} (or \sqrt{kN} , where $k \in \mathbb{N}$). Then one tries the above method for factoring successively using the numbers

$$\begin{aligned} x_n &= s_n \\ y_n &= s_n^2 - Nt_n^2 \end{aligned}$$

Clearly $x_n^2 \equiv y_n \pmod{N}$. From the theory of continued fractions one gets the inequality

$$|y_n| < 2\sqrt{N}.$$

Exercise 1.0.2 Prove this inequality after having read about continued fractions in the next chapter.

Chapter 2

Continued fractions

2.1 The game that might never stop

Let $[x]$ denote the largest integer $< x$, where $x \in \mathbb{R}$ is a real number. For a given real number ξ we wish to decide if ξ is rational. Clearly this is true if $\xi = [\xi]$. If not, we may write

$$\xi = [\xi] + \xi - [\xi] = [\xi] + \frac{1}{\frac{1}{\xi - [\xi]}}.$$

Now put $\xi_1 = \frac{1}{\xi - [\xi]}$. If $\xi_1 = [\xi_1]$, ξ was a rational number. If not we put

$\xi_2 = \frac{1}{\xi_1 - [\xi_1]}$ and write

$$\xi = [\xi] + \frac{1}{[\xi_1] + \frac{1}{\xi_2}}.$$

We continue this and cook up new real numbers ξ_3, ξ_4, \dots and stop if $\xi_n = [\xi_n]$ for some n . This game is called the continued fraction algorithm for a real number. The game never stops if ξ is an irrational number.

Exercise 2.1.1 Prove this!

Example 2.1.2 The first steps of the continued fraction algorithm for π leads

to the following “continued fraction”

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292 + \frac{1}{\xi}}}}},$$

where ξ is an irrational number.

Example 2.1.3 The continued fraction algorithm for $\sqrt{2}$ can be carried out by algebraic computations. Here is how. First we rewrite a bit

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2} - 1} = 1 + \frac{1}{\sqrt{2} + 1}$$

Now we have an expression for $\sqrt{2}$ that “bites its own tail”. Let us insert it into itself:

$$\sqrt{2} = 1 + \frac{1}{1 + \frac{1}{\sqrt{2} + 1} + 1} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}$$

We can repeat this to get the “continued fraction”

$$1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}}}$$

In this way we have proved that $\sqrt{2}$ is irrational or have we?

2.1.1 Rational numbers

The continued fraction algorithm for rational numbers turns out to be the classical Euclidean algorithm. This is quite easy to see. Consider a fraction a/b , where $b > 0$. Then $a = qb + r$ and $[a/b] = q$. Therefore

$$\frac{a}{b} = q + \frac{r}{b} = q + \frac{1}{\frac{b}{r}}$$

and the continued fraction algorithm continues with the fraction b/r . Ultimately this process will stop.

Example 2.1.4 Consider the fraction $103993/33102$. Division with remainder gives $103993 = 3 \cdot 33102 + 4687$. This implies that

$$\frac{103993}{33102} = 3 + \frac{4687}{33102} = 3 + \frac{1}{\frac{33102}{4687}}$$

Again $33102 = 7 \cdot 4687 + 293$, Therefore

$$3 + \frac{1}{\frac{33102}{4687}} = 3 + \frac{1}{7 + \frac{293}{4687}}$$

Continue with $4687 = 15 \cdot 293 + 292$:

$$3 + \frac{1}{7 + \frac{293}{4687}} = 3 + \frac{1}{7 + \frac{1}{\frac{4687}{293}}} = 3 + \frac{1}{7 + \frac{1}{15 + \frac{292}{293}}} = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292}}}}$$

2.2 Basic theory of continued fractions

A continued fraction is formally a sequence of integers $a_0, a_1, \dots, a_n, \dots$, where $a_i \in \mathbb{Z}$ and $a_i > 0$ for $i > 0$. There is a one to one correspondence between continued fractions and real numbers. This is displayed in the notation

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} \quad (*)$$

to be understood as the following sequence of numbers

$$a_0, a_0 + \frac{1}{a_1}, a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}}, \dots$$

Does this make sense? Does this sequence converge (to a real number)? We need to compute a bit more to answer this question.

2.3 Eulers rule and corollaries

The above sequence of (honest) fractions are called *convergents* for the continued fraction in (*). What are the fractions? Before we compute them let us make a subtle observation. Denote the numerator of the n -th convergent of a continued fraction $x_1; x_2, x_3, \dots$ by $[x_1, x_2, \dots, x_n]$. Then the n -th convergent is

$$\frac{[x_1, x_2, \dots, x_n]}{[x_2, \dots, x_n]} = x_1 + \frac{[x_3, \dots, x_n]}{[x_2, \dots, x_n]}.$$

Therefore

$$[x_1, x_2, \dots, x_n] = x_1[x_2, \dots, x_n] + [x_3, \dots, x_n].$$

Using this we get

$$\begin{aligned} [] &= 1 \\ [x_1] &= x_1 \\ [x_1, x_2] &= x_1x_2 + 1 \\ [x_1, x_2, x_3] &= x_1x_2x_3 + x_1 + x_3 \\ [x_1, x_2, x_3, x_4] &= x_1x_2x_3x_4 + x_3x_4 + x_2x_3 + x_1x_2 + 1 \\ [x_1, x_2, x_3, x_4, x_5] &= x_1x_2x_3x_4x_5 + x_3x_4x_5 + x_1x_4x_5 + x_1x_2x_5 + x_1x_2x_3 + x_1 + x_5 \end{aligned}$$

Notice that $[x_1, x_2, x_3, x_4, x_5] = [x_5, x_4, x_3, x_2, x_1]$. This is a very pleasant surprise and it holds in general! In fact we have the following result.

Proposition 2.3.1 (Eulers rule) $[x_1, x_2, \dots, x_n]$ is a sum of terms constructed from $x_1x_2 \cdots x_n$ by first deleting 0 consecutive variables, then deleting 2 consecutive variables, then 4 and so on.

Proof. Follows by induction using

$$[x_1, x_2, \dots, x_n] = x_1[x_2, \dots, x_n] + [x_3, \dots, x_n].$$

□

Corollary 2.3.2

$$[x_1, x_2, \dots, x_n] = [x_n, x_{n-1}, \dots, x_1].$$

Corollary 2.3.3

$$[a_0, a_1, \dots, a_n] = a_n[a_0, \dots, a_{n-1}] + [a_0, \dots, a_{n-2}].$$

Exercise 2.3.4 Write the continued fraction for a fraction u/v , where $u > v > 0$ as $[a_0, a_1, \dots, a_{n-1}, d]/[a_1, a_2, \dots, a_{n-1}, d]$, where $d = \gcd(u, v)$. Conclude that if the Euclidean algorithm requires precisely n steps for u and

v , then $u \geq dF_{n+2}$ and $v \geq dF_{n+1}$, where F_n denotes the n -th Fibonacci number. Here is the list of the first few Fibonacci numbers

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots$$

How many steps of the Euclidean algorithm do $u = F_{n+2}$ and $v = F_{n+1}$ take?

If we denote the numerator and denominator of the n -th convergent s_n and t_n respectively, then we have the inductive formula

$$s_n = a_n s_{n-1} + s_{n-2}$$

$$t_n = a_n t_{n-1} + t_{n-2},$$

where we put $s_{-2} = 0, s_{-1} = 1, t_{-2} = 1, t_{-1} = 0$.

Remark 2.3.5 The sequence of denominators (t_n) is a strictly increasing sequence of natural numbers.

Example 2.3.6 Here is the beginning of the continued fraction for $\sqrt{2}$.

i	-2	-1	0	1	2	3	4	5
a_i			1	2	2	2	2	2
s_i	0	1	1	3	7	17	41	99
t_i	1	0	1	2	5	12	29	70

Example 2.3.7 Here are the first convergents in the continued fraction for π (cf. Example 2.1.2).

i	-2	-1	0	1	2	3
a_i			3	7	15	1
s_i	0	1	3	22	333	355
t_i	1	0	1	7	106	113

We recognize in particular $\frac{22}{7}$ as the archimedian approximation to π . Less known is $\frac{355}{113}$, which is a much better approximation. In fact

$$\frac{355}{113} = 3.1415929\dots$$

whereas $\pi = 3.1415926535\dots$

Proposition 2.3.8

$$s_n t_{n+1} - s_{n+1} t_n = (-1)^{n+1}.$$

The numerator s_n and denominator t_n in a convergent s_n/t_n are relatively prime integers.

Proof. Write $s_{n+1} = a_n s_n + s_{n-1}$ and $t_{n+1} = a_n t_n + t_{n-1}$. Then

$$\begin{aligned} s_n t_{n+1} - s_{n+1} t_n &= s_n (a_n t_n + t_{n-1}) - (a_n s_n + s_{n-1}) t_n = \\ &= -(s_{n-1} t_n - s_n t_{n-1}) \end{aligned}$$

and the result follows by induction. Notice that $s_{-2} t_{-1} - s_{-1} t_{-2} = -1$. \square

Corollary 2.3.9 We have the following inequalities

$$\begin{aligned} \frac{s_0}{t_0} &\leq \frac{s_1}{t_1} \geq \frac{s_2}{t_2} \leq \dots \\ \frac{s_0}{t_0} &\leq \frac{s_2}{t_2} \leq \frac{s_4}{t_4} \leq \dots \\ \frac{s_1}{t_1} &\geq \frac{s_3}{t_3} \geq \frac{s_5}{t_5} \leq \dots \end{aligned}$$

The even convergents form an increasing sequence bounded above by s_1/t_1 and the odd convergents form a decreasing sequence bounded below by s_0/t_0 .

By elementary real analysis both sequences (s_{2n}/t_{2n}) and (s_{2n+1}/t_{2n+1}) have a limit. In fact they converge to the same number. This is a result of the following computation.

Lemma 2.3.10

$$\left| \frac{s_n}{t_n} - \frac{s_{n+1}}{t_{n+1}} \right| < \frac{1}{t_n^2}.$$

Proof.

$$\left| \frac{s_n}{t_n} - \frac{s_{n+1}}{t_{n+1}} \right| = \left| \frac{s_n t_{n+1} - t_n s_{n+1}}{t_n t_{n+1}} \right| < \frac{1}{t_n^2},$$

by Proposition 2.3.8 and since t_n is an increasing sequence of natural numbers. \square

2.4 Continued fraction for a real number

We pose a very relevant question. When we do the continued fraction algorithm for a real number ξ , we get a continued fraction. What does this continued fraction have to do with ξ ? The answer is that the convergents (surprise!) converge to ξ . Here is how to prove this. Consider the continued fraction algorithm for ξ after n steps

$$\xi = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots a_n + \frac{1}{\xi_n}}}}$$

This means that $\xi = [a_0, a_1, \dots, a_n, \xi_n]/[a_1, \dots, a_n, \xi_n]$. Similarly to Lemma 2.3.10, we get the following result showing that the convergents really do converge to ξ .

Proposition 2.4.1

$$\left| \xi - \frac{s_n}{t_n} \right| \leq \frac{1}{t_n^2}.$$

Proof. We may write

$$\xi = \frac{\xi_n s_n + s_{n-1}}{\xi_n t_n + t_{n-1}},$$

where $\xi_n > 0$. Using this, a small computation shows what we want. \square

2.5 Quadratic irrationalities

A quadratic irrationality α is a non rational real root in a quadratic equation

$$Ax^2 + Bx + C = 0, \quad (*)$$

where $A, B, C \in \mathbb{Z}$.

Definition 2.5.1 If α is a quadratic irrationality, which is a root of (*), then we let α' denote the other root of (*). The other root is called the (algebraic) conjugate of α .

Proposition 2.5.2 Let α be a quadratic irrationality and $q \in \mathbb{Z}$ an integer. Then

- i) $1/\alpha$ is a quadratic irrationality.
- ii) $\alpha + q$ is a quadratic irrationality.
- iii) $(\alpha + q)' = \alpha' + q$ and $(1/\alpha)' = 1/\alpha'$.

Proof. Exercise. \square

The above proposition shows that if α is a quadratic irrationality and

$$\alpha = q + \frac{1}{\alpha_1}$$

where $q = [\alpha]$, then α_1 is also a quadratic irrationality. In other words: all the steps in the continued fraction algorithm produce quadratic irrationalities when starting out with one. If α is a quadratic irrationality, then

$$\alpha = \frac{P \pm \sqrt{D}}{Q}$$

for $P, Q, D \in \mathbb{Z}$, where $D \geq 0$. To carry out the first step in the continued fraction algorithm, first observe that

$$[\alpha] = \left[\frac{P + [\pm\sqrt{D}]}{Q} \right].$$

Exercise 2.5.3 Prove this!

So if we have a good algorithm (we do) for finding “the floor” of the square root of an integer we are all set. Let us analyze the “inversion” step in the continued fraction algorithm. Here

$$\frac{1}{\frac{P + \sqrt{D}}{Q}} = \frac{P - \sqrt{D}}{P^2 - D}.$$

Notice that $Q \mid P^2 - D$, since $P = -B$, $D = B^2 - 4AC$ and $Q = 2A$, where $A\alpha^2 + B\alpha + C = 0$ and $A, B, C \in \mathbb{Z}$. These observations give a very explicit integer algorithm for computing the continued fraction of a quadratic irrationality. But we are not satisfied! We will dive into the mind blowing theory of continued fractions in the 19th century proving a beautiful result of Galois.

2.5.1 Purely periodic continued fractions

Definition 2.5.4 A quadratic irrationality α is called reduced if

- i) $\alpha > 1$
- ii) $-1 < \alpha' < 0$

Example 2.5.5 $\sqrt{2}$ is not reduced since $(\sqrt{2})' = -\sqrt{2} < -1$. But $1 + \sqrt{2}$ is reduced as $(1 + \sqrt{2})' = 1 - \sqrt{2}$. In general $q_0 + \sqrt{N}$ is reduced where $q_0 = [\sqrt{N}]$.

A continued fraction of the form $a_0, a_1, \dots, a_n, a_0, a_1, \dots$ is called purely periodic.

Example 2.5.6 Consider the real number φ given by the “simplest” purely periodic continued fraction $1, 1, 1, 1, \dots$

$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\dots}}}$$

Then $\varphi = 1 + \frac{1}{\varphi}$. Therefore $\varphi^2 - \varphi - 1 = 0$ and

$$\varphi = \frac{1 \pm \sqrt{5}}{2}.$$

Some will recognize the + part as the golden ratio. The golden ratio is a reduced quadratic irrational.

Lemma 2.5.7 If α is a reduced quadratic irrationality and

$$\alpha = q_0 + \frac{1}{\alpha_1},$$

where $q_0 = [\alpha]$. Then α_1 is a reduced quadratic irrationality.

Proof. Exercise. \square

Theorem 2.5.8 (Galois) $\xi \in \mathbb{R}$ has a purely periodic continued fraction if and only if ξ is a reduced quadratic irrational.

Proof. Suppose that $\xi \in \mathbb{R}$ has a purely periodic continued fraction. This means that

$$\xi = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots a_n + \frac{1}{\xi}}}}$$

for some n . Then

$$\xi = \frac{\xi s_n + s_{n-1}}{\xi t_n + t_{n-1}}$$

and ξ must be a quadratic irrationality, since

$$t_n \xi^2 + (t_{n-1} - s_n)\xi - s_{n-1} = 0.$$

But why is it reduced? This is tricky. In fact one has to pull out a genuine trick to solve this. Consider the number ξ_1 given by reversing the period of ξ :

$$\xi_1 = a_n + \frac{1}{a_{n-1} + \frac{1}{a_{n-2} + \frac{1}{\cdots a_0 + \frac{1}{\xi_1}}}}.$$

Then

$$\begin{aligned}\xi' &= \frac{[a_n, \dots, a_0, \xi_1]}{[a_{n-1}, \dots, a_0, \xi_1]} = \frac{[a_n, \dots, a_0]\xi_1 + [a_n, \dots, a_1]}{[a_{n-1}, \dots, a_0]\xi_1 + [a_{n-1}, \dots, a_1]} \\ &= \frac{s_n \xi_1 + t_n}{s_{n-1} \xi_1 + t_{n-1}}\end{aligned}$$

and

$$s_{n-1} \xi_1^2 + (t_{n-1} - s_n) \xi_1 - t_n = 0.$$

This shows that $\xi' = -1/\xi_1$, so that $-1 < \xi' < 0$. We have proved that a purely periodic continued fraction describes a reduced quadratic irrational. Let us prove the other way.

Suppose that ξ is a reduced quadratic irrational. Then

$$\xi = \frac{P + \sqrt{D}}{Q} \quad \text{and} \quad \xi' = \frac{P - \sqrt{D}}{Q}.$$

We may conclude first that $Q > 0$ (consider $\xi - \xi'$), then $P > 0$ and the important boundedness conditions

i) $P < \sqrt{D}$

ii) $Q < 2\sqrt{D}$

on P and Q by using that ξ is reduced. Let us run ξ through one step of the continued fraction algorithm. First let $q = [\xi]$. Then

$$\xi - q = \frac{P - qQ + \sqrt{D}}{Q}.$$

Next step is to compute the reduced (recall Lemma 2.5.7) quadratic irrationality

$$\xi_1 = \frac{1}{\frac{P - qQ + \sqrt{D}}{Q}} = \frac{Q}{P - qQ + \sqrt{D}} = \frac{Q(- (P - qQ) + \sqrt{D})}{D - (P - qQ)^2}.$$

So putting $P_1 = qQ - P$ and $Q_1 = (D - P_1^2)/Q$ we get

$$\xi_1 = \frac{P_1 + \sqrt{D}}{Q_1}.$$

Now we continue the algorithm with ξ_1 . Since there are only finitely many possibilities for P and Q (there are only finitely many pairs (P, Q) of natural numbers satisfying $P < \sqrt{D}$, $Q < 2\sqrt{D}$), we will eventually run into a repetition $\xi_m = \xi_n$ for $m < n$. We will prove that this implies $\xi_{m-1} = \xi_{n-1}$. This

leads to the purely periodic continued fraction $a_0, a_1, \dots, a_{n-m}, a_0, a_1, \dots$. In the n -th step of the continued fraction algorithm we have

$$\xi_n = [\xi_n] + \frac{1}{\xi_{n+1}}.$$

This implies that $[\xi_n] = [-\frac{1}{\xi'_{n+1}}]$, since $[\xi_n] < -1/\xi'_{n+1} < [\xi_n] + 1$. So if $\xi_m = \xi_n$, we get $[\xi_{m-1}] = [\xi_{n-1}]$ and therefore that $\xi_{m-1} = \xi_{n-1}$. This finally shows that a reduced quadratic irrationality has a purely periodic continued fraction. \square

2.6 The continued fraction for \sqrt{N}

Example 2.6.1 With enough patience one can compute that

$$\sqrt{14} = 3, \overline{1, 2, 1, 6}, 1, 2, 1, 6, \dots$$

$$\sqrt{19} = 4, \overline{2, 1, 3, 1, 2, 8}, 2, 1, 3, 1, 2, 8, \dots$$

The example shows a pattern in the continued fraction for the square root. It seems that it repeats itself after encountering $2a_0$. It also seems to be symmetric around a “middle”. This is no coincidence:

Theorem 2.6.2 Let N be a natural number, which is not a square. Then

$$\sqrt{N} = q_0 + \frac{1}{q_1 + \frac{1}{\dots + \frac{1}{q_n + \frac{1}{2q_0 + \frac{1}{q_1 + \frac{1}{\dots}}}}}}$$

where $q_1 = q_n, q_2 = q_{n-1}, \dots$

Proof. Let $q_0 = [\sqrt{N}]$. Then we know that $q_0 + \sqrt{N}$ has a purely periodic continued fraction by Theorem 2.5.8. Thus $\sqrt{N} + q_0 = 2q_0, q_1, \dots, q_n, 2q_0, q_1, \dots$. This proves the first statement. Consider now the conjugate $-\sqrt{N} + q_0$ of $\sqrt{N} + q_0$. Then

$$-\frac{1}{-\sqrt{N} + q_0} = q_n, q_{n-1}, \dots, q_1, 2q_0, q_n, \dots$$

This implies that

$$\sqrt{N} = q_0, q_n, q_{n-1}, \dots, q_1, 2q_0, q_n, \dots$$

By uniqueness of the continued fraction for \sqrt{N} we get $q_1 = q_n, q_2 = q_{n-1}, \dots$ \square

2.7 A few words on Pell's equation

This is the diophantine equation

$$x^2 - Ny^2 = 1, \quad (*)$$

where N is a natural number, which is not a square. It would be a shame not to mention the elegant way of giving integer solutions to $(*)$ using the continued fraction expansion of \sqrt{N} . Using the notation of Theorem 2.6.2, we get (in the usual way)

$$\sqrt{N} = \frac{(q_0 + \sqrt{N})s_n + s_{n-1}}{(q_0 + \sqrt{N})t_n + t_{n-1}}.$$

Multiplying this out leads to

$$\begin{aligned} s_{n-1} &= Nt_n - q_0s_n \\ t_{n-1} &= s_n - q_0t_n \end{aligned}$$

Now

$$s_{n-1}t_n - s_nt_{n-1} = (Nt_n - q_0s_n)t_n - s_n(s_n - q_0t_n) = Nt_n^2 - s_n^2.$$

We conclude that

$$s_n^2 - Nt_n^2 = -(s_{n-1}t_n - s_nt_{n-1}) = -(-1)^n = (-1)^{n+1}.$$

Example 2.7.1 Consider the equation $x^2 - 19y^2 = 1$. To find an integer solution we consider the continued fraction expansion for $\sqrt{19}$:

$$\sqrt{19} = 4, \overline{2, 1, 3, 1, 2, 8}, 2, 1, 3, 1, 2, 8, \dots$$

and compute the convergents

i	-2	-1	0	1	2	3	4	5	6
a_i			4	2	1	3	1	2	8
s_i	0	1	4	9	13	48	61	170	1421
t_i	1	0	1	2	3	11	14	39	326

One checks that

$$170^2 - 19 \cdot 39^2 = 1.$$

Chapter 3

Exercises

3.1 In class

1. Compute the continued fraction expansion of $\frac{55}{34}$.
2. Write down the exact steps in an integer algorithm for computing the continued fraction expansion of \sqrt{N} .
3. Compute the continued fraction expansions of $\sqrt{3}$ and $\sqrt{5}$.
4. Find an integer solution to the equation $x^2 - 11y^2 = 1$.

3.2 Homework

1. Solve all exercises in chapters 1 and 2 (don't forget the proofs).
2. Invent an integer algorithm to compute the continued fraction expansion for $\sqrt[3]{2}$. Compute the first 100 q's in the continued fraction. The sad state of affairs in mathematics is that it is unknown even if the q's are bounded.¹

¹Do this exercise if you have time to spare.

Bibliography

- [1] C. Pomerance, *A tale of two sieves*, Notices of the American Mathematical Society **43** (1996), 1473–1485.