Continued Fractions

A course at the Nesin Mathematics Village

David Pierce

August 13–19, 2018
Last edited August 22, 2018

Matematik Bölümü
Mimar Sinan Güzel Sanatlar Üniversitesi
dpierce@msgsu.edu.tr
http://mat.msgsu.edu.tr/~dpierce/
polytropy.com

Preface

Much of the present document is cannibalized from the notes I kept while teaching Elementary Number Theory II at METU in Ankara, Spring 2008. I edited those notes in the winter of this year. There were 33 hours of lectures for that course.

The present document reflects the content of the twelve hours of lectures constituting Continued Fractions, given at the Math Village, 8–10 A.M., Monday to Sunday (except Thursday), August 13–19, 2018. The order of presentation in class was often different, and I did not give all of the proofs.

I focussed on the practical problem of finding integer points of conic sections, especially hyperbolas, using continued fractions. I presented a complete method; in this sense, the course constituted a whole. I showed how to find *all* integer points from *one* nontrivial point. I did not prove that the point had to exist (though the proof is here); nor did I prove that such a point could be obtained from a convergent of a square root (though the proof is in the notes from ten years ago).

I had expected to work through the proof that, for nonsquare positive d,

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_{n-1}, 2a_0}],$$

where $a_k = a_{n-k}$ when $0 < k < n$. In the event, there was no time for the proof, and I doubted whether there was interest.

Since some students had little university experience, I ended up discussing the Euclidean Algorithm and its usual number-theoretic consequences, as in Chapter 1. For fun, I found the Pythagorean triples, as in Chapter 2.

The lectures actually started with the question of the meaning of $\sqrt{2}$ at the head of Chapter 3. One student described it as a supremum. He also had Euclid from the library, and this is a reason why I felt free to talk about Euclid's theories of proportion, as in Chapter 1; other students became curious here, though perplexed.

On Tuesday I had 16 students: five from Boğaziçi, four from ODTÜ, two from Bilkent, and one each from DPÜ (Dumlupınar?), CBÜ (Celal Bayar?), Galatasaray, and İTÜ, and one not yet at university. I know this because I had them write down the information; I then assigned each student a different number d for which to find the continued fraction expansion of $\sqrt{d}$. Most of them brought the correct solutions the next day. One of them had checked his work with me, the previous evening.

Most students were from English-language universities; but I spoke mainly in Turkish, while writing in English. Students asked questions in both languages.

On the last day, five students attended. Later in the day, I saw two who had not attended. One said that, even had he arisen in time for class, fields and lattices were alien to him; the other had been seeing off friends, though he was staying longer, and did I suggest he take my course of the next week (The Prime Number Theorem)?

The course might be called an introduction to quadratic fields. I avoided most suggestions of where further generalization might lead. I did point out we were finding integer points of curves of genus zero; the problem of genus one—elliptic curves—was harder.

Contents

1 The Euclidean Algorithm 7

2 The Circle 18

3 Irrational Numbers 20

3.1 Geometry 20

3.2 Dedekind Cuts 21

3.3 Cauchy Sequences 22

4 The Square Root of Two 23

5 The Pell Equation 26

6 Continued Fractions 30

7 Solubility of the Pell Equation 35

8 Quadratic Fields 37

9 Orders 44

10 Integers 53

Bibliography 56

List of Figures

3.1 A consequence of Thales's Theorem 21
4.1 Integer points of hyperbolas $x^2 - 2y^2 = \pm 1$ . . . 25
5.1 Integer points of hyperbola $x^2 - 2y^2 = 1$ 29
9.1 Hyperbola $(2x + \phi y)(2x + \phi' y) = 4$ 48
9.2 Small solutions of $4x^2 + 2xy - y^2 = 4$ 51
9.3 Solutions of $4x^2 + 2xy - y^2 = 4$ 52

List of Tables

4.1 Convergents of $\sqrt{2}$ 24
8.1 Terms of the Fibonacci sequence 41

1 The Euclidean Algorithm

For notation, we shall use

- $\mathbb{N}$ for the set $\{1, 2, 3, \dots\}$ of **counting numbers,**
- ω ("omega") for the set $\{0, 1, 2, \dots\}$ of **natural numbers,** and
- $\mathbb{Z}$ for the set $\{\dots, -2, -1, 0, 1, 2, \dots\}$ of **integers.**

Given two counting numbers a_0 and a_1, where $a_0 > a_1$, we define natural numbers a_{n+2} and x_n recursively by the rule

$$a_n = a_{n+1}x_n + a_{n+2} \ \ \& \ \ a_{n+2} < a_{n+1}.$$

This is the **Euclidean Algorithm.** Here ax means a, x times, so that x is the **multiplier,** and a the **multiplicand;** symbolically,

$$ax = \underbrace{a + \cdots + a}_{x}.$$

If $ax = b$, two conclusions are that a **measures** b, and x **divides** b. These are equivalent notions, since $ax = xa$. However, we are going to prove this, as Euclid does in the *Elements.*

Meanwhile, since the sequence of natural numbers a_n is decreasing, it must eventually stop. It stops when it reaches zero. If $a_{n+2} = 0$, then x_{n+1} cannot be defined. Thus we have

$$\begin{gathered} a_0 = a_1x_0 + a_2, \\ a_1 = a_2x_1 + a_3, \\ \dots\dots\dots\dots\dots \\ a_{n-1} = a_nx_{n-1} + a_{n+1}, \\ a_n = a_{n+1}x_n. \end{gathered}$$

Here a_{n+1} is the **greatest common measure** of a_0 and a_1, since

- a_{n+1} measures itself, and a_n, and then a_{n-1}, and so on to a_1 and a_0, and moreover
- any common measure of a_0 and a_1 measures also a_2, then a_3, and so on to a_{n+1}.

For example,

$$\begin{aligned} 151 &= 71 \cdot 2 + 9, \\ 71 &= 9 \cdot 7 + 8, \\ 9 &= 8 \cdot 1 + 1, \\ 8 &= 1 \cdot 8, \end{aligned}$$

and so the greatest common measure of 151 and 71 is 1, or in other words 151 and 71 are **prime to one another.** Moreover, working backwards through the computations, we have

$$\begin{aligned} 1 &= 9 - 8 \cdot 1 = 9 - (71 - 9 \cdot 7) \cdot 1 \\ &= 9 \cdot 8 - 71 \cdot 1 = (151 - 71 \cdot 2) \cdot 8 - 71 \cdot 1 \\ &= 151 \cdot 8 - 71 \cdot 17. \end{aligned}$$

In this way, we obtain:

Theorem 1 (Bézout)**.** *Counting numbers a and b are prime to one another if and only if the equation*

$$ax + by = 1$$

is soluble in $\mathbb{Z}$.

The Euclidean Algorithm is an application of what Euclid calls **anthyphaeresis** (*ἀνθυφαίρεσις*) or alternating subtraction. The Greek word comes from *anti* + *hypo* + *haire-* (*ἀντί*

+ ὑπό + αἱρέ-); the last two parts in Latin are *sub* + *tract.* Let the sequence of numbers x_n obtained above be called the **anthyphaeretic sequence** of the ordered pair (a_0, a_1).

For Euclid, a number is a "multitude of units," and units are implicitly magnitudes, all of the same size. There are several ways to express the same possible relation among four magnitudes a, b, c, and d:

- a, b, c, and d are **proportional,**
- the **ratio** of a to b is the same as that of c to d, or
- a is to b as c is to d.

For these, in modern symbolism we write

$$a : b :: c : d. \tag{1.1}$$

There is good evidence that, by the original definition, this means (a, b) and (c, d) have the same anthyphaeretic sequence. However, there are other possible definitions, and Euclid gives two of them: one for arbitrary magnitudes, and one for numbers alone.

Euclid's definition of proportion of arbitrary magnitudes is attributed to Eudoxus of Cnidus by a scholium in a manuscript of Euclid's text. By this definition, a ratio is what we now understand to be a *Dedekind cut,* because we know the ratio of A to B, once we know, for each pair (k, ℓ) of counting numbers, whether $Ak > B\ell$, or $Ak = B\ell$, or $Ak < B\ell$. (See page 21 for more on Dedekind cuts.)

Euclid defines four *numbers* to be in proportion if the first number is the same *multiple,* or *part,* or *parts,* of the second that the third is of the fourth. The words may seem ambiguous to us today, but I think the meaning can only be as follows.

Given the numbers a and b, we can find their greatest common measure, e, using the Euclidean algorithm. There are

then multipliers x and y such that

$$a = ex, \qquad\qquad b = ey.$$

- If $y = 1$, then a is a **multiple** of b;
- if $x = 1$, then a is a **part** of b;
- otherwise, a is **parts** of b.

In any case, x and y are prime to one another; otherwise, e would not be the greatest of their common measures. Thus the meaning of (1.1) for numbers is that, for some multipliers x and y,

$$a = ex, \qquad b = ey, \qquad c = fx, \qquad d = fy,$$

where

- e is the greatest common measure of a and b, and
- and f is the greatest common measure of c and d,

or equivalently

- x and y are prime to one another.

Thus every proportion of numbers can be written in the form

$$ex : ey :: fx : fy, \tag{1.2}$$

where again x and y are prime to one another.

Some modern mathematicians do not seem to think the condition on e and f (or on x and y) is implied by Euclid's words [5, 4]. One reason to think that it *is* implied is that, with the definition as I have stated it, we have immediately

$$a : b :: c : d \ \ \& \ \ c : d :: g : h \implies a : b :: g : h.$$

This is transitivity of sameness of ratio; and Euclid would not define any relation as a *sameness* of something, unless the relation were obviously transitive.

In Euclid's definition, as I interpret it, the pair (x, y) is uniquely determined by (a, b); moreover, again, x and y are prime to one another.

Even without the condition on e and f above, we immediately have that sameness of ratio is reflexive and symmetric:

$$a : b :: a : b,$$
$$a : b :: c : d \implies c : d :: a : b.$$

There is also another kind of symmetry:

$$a : b :: c : d \implies b : a :: d : c.$$

Thus, in (1.1), we may assume $a > b$, and also $a > c$, if this is convenient.

Lemma 1. *For all counting numbers a, b, c, and d,*

$$a : b :: c : d \implies a : b :: a \pm c : b \pm d.$$

Proof. If (a, b) and (c, d) have the same anthyphaeretic sequence, it will be the anthyphaeretic sequence of $(a + c, b + d)$ and $(a - c, b - d)$, since, for example,

$$(a + c) - (b + d) = (a - b) + (c - d).$$

However, Euclid's proof uses Euclid's official definition of proportion of numbers. By definition, as in the general form (1.2), we have

$$ax : ay :: cx : cy,$$
$$ax : ay :: (a \pm c)x : (a \pm c)y,$$

at least if x and y are prime to one another. We can conclude

$$ax : ay :: ax \pm cx : ay \pm cy,$$

by distributivity of multiplication over addition. This itself is a consequence of commutativity of addition:

$$(a+c)\cdot 2 = a+c+a+c = a+a+c+c = a\cdot 2 + c\cdot 2,$$

and so on. □

Lemma 2. *For all counting numbers a and c, for all multipliers x,*

$$a : c :: ax : cx. \tag{1.3}$$

Proof. By repeated application of Lemma 1 to the proportion

$$a : c :: a : c,$$

we have

$$a : c :: \underbrace{a+\cdots+a}_{x} : \underbrace{c+\cdots+c}_{x}.$$ □

Theorem 2 (Alternation)**.** *For all counting numbers a, b, c, and d,*

$$a : b :: c : d \implies a : c :: b : d.$$

Proof. Again by Euclid's definition,

$$a : ax :: c : cx.$$

We also have (1.3) in Lemma 2. This proves the claim in case a is part of b. For the general case, we use transitivity, which from (1.3) yields

$$ax : cx :: ay : cy,$$

while again from Euclid's definition,

$$ax : ay :: cx : cy, \tag{1.4}$$

if x and y are prime to one another. Since (1.4) then is the general form of a proportion, the proof is complete. □

Theorem 3. *Multiplication is commutative:*

$$ab = ba.$$

Proof. From the definition, and by Theorem 2,

$$1 : a :: b : ba,$$
$$1 : b :: a : ba.$$

Therefore, as b is the multiple of 1 by b, so ba must be the multiple of a by b, namely ab. □

If a measures b, or equivalently now if a divides b, we may write

$$a \mid b.$$

We usually refer to the greatest common measure of c and d as the **greatest common divisor,** writing this as

$$\gcd(c, d).$$

A counting number p is **prime,** simply, if it is not 1, and

$$p = ab \ \ \& \ \ p \neq a \implies p = b. \tag{1.5}$$

Since

$$a = bc \implies b \mid a,$$

and in $\mathbb{N}$ also

$$a \mid b \ \ \& \ \ b \mid a \implies a = b,$$

we can write (1.5) also as

$$p = ab \ \ \& \ \ p \nmid a \implies p \mid b. \tag{1.6}$$

Using Bézout's Theorem, we can prove the following strengthening of (1.6).

Theorem 4 (Euclid)**.** *For all primes p,*

$$p \mid ab \;\&\; p \nmid a \implies p \mid b. \tag{1.7}$$

Proof. If $p \nmid a$, then p and a are prime to one another, and therefore, for some x and y,

$$\begin{aligned} px + ay &= 1, \\ pbx + aby &= b. \end{aligned}$$

If $p \mid ab$, then p divides both terms on the left, and hence their sum; thus $p \mid b$. □

A subset R of $\mathbb{C}$ that is closed under addition, subtraction, and multiplication is called a **ring** (as also on page 44). Suppose p is a nonzero element with no inverse in R.

- If (1.6) holds in R, then p is **irreducible** in R;
- if (1.7) holds in R, then p is **prime** in R.

Thus irreducibles are always prime. We shall see (on page 38) an example where the converse fails.

Meanwhile, we give Euclid's proof of Theorem 4. We shall need a couple of lemmas.

Lemma 3. *For all counting numbers a, b, c, and d,*

$$ab = cd \implies a : c :: d : b.$$

Proof. Assuming $ab = cd$, and using transitivity, we have

$$\begin{aligned} a : c &:: ad : cd && \text{[by Lemma 2]} \\ &:: ad : ab && \text{[by assumption]} \\ &:: da : ba && \text{[by Theorem 3]} \\ &:: d : b. && \text{[by Lemma 2 again]} \end{aligned}$$

□

Lemma 4. *If* (1.1) *holds, and* a *and* b *are prime to one another, then* $a \mid c$.

Proof. If (1.1) holds, so that also

$$a : c :: b : d$$

by Theorem 2, then the Euclidean Algorithm has the same steps, whether applied to (a, c) or (b, d). Applying the Euclidean Algorithm to (1.1), by Lemma 1 we have

$$a : b :: \gcd(a, c) : \gcd(b, d),$$

and so by Theorem 2

$$a : \gcd(a, c) :: b : \gcd(b, d).$$

This means

$$a = \gcd(a, c)x = x \gcd(a, c), \quad b = \gcd(b, d)x = x \gcd(b, d)$$

for some x. If a and b are prime to one another, then $x = 1$, and $\gcd(a, c) = a$, so $a \mid c$. □

Euclid's proof of Theorem 4. Suppose now $pc = ab$, but $p \nmid a$. Then p and a are prime to one another, and also

$$p : a :: b : c$$

by Lemma 3, and therefore $p \mid b$ by Lemma 4. □

An important theoretical consequence of Theorem 4 that Euclid does *not* prove is the following.

Theorem 5 (Fundamental Theorem of Arithmetic)**.** *Every counting number is* uniquely *a product*

$$p_0 p_1 \cdots p_{n-1}$$

of primes, where

$$p_0 \leqslant p_1 \leqslant \ldots \leqslant p_{n-1}. \tag{1.8}$$

If $n = 0$, then the product in (1.8) is 1. A **square** number is any n^2, where n is an integer. A **nonsquarefree** number is one that is indivisible by the square of any prime.

Theorem 6. *If D is nonsquare, then the equation*

$$x^2 - Dy^2 = 0$$

has no solution in $\mathbb{N}$.

Proof. We may write

$$D = s^2 d,$$

where d is squarefree and greater than 1. It is then enough to show that

$$x^2 - dy^2 = 0 \tag{1.9}$$

is insoluble. If (a, b) is a solution, then $d \mid a^2$. However,

$$d = p_0 p_1 \ldots p_{n-1},$$

where

$$p_0 < p_1 < \cdots < p_{n-1}.$$

Thus in each case

$$p_k \mid a^2,$$

so by Theorem 4

$$p_k \mid a.$$

In particular then, for some x_k,

$$\begin{gathered}
a = p_0 x_0, \\
p_1 \mid x_0, \\
a = p_0 p_1 x_1, \\
\ldots\ldots\ldots\ldots, \\
a = p_0 p_1 \cdots p_{n-1} x_{n-1} = d x_{n-1}, \\
d^2 {x_{n-1}}^2 - d b^2 = 0, \\
d {x_{n-1}}^2 - b^2 = 0,
\end{gathered}$$

so (b, x_{n-1}) is a solution to (1.9). Also $b < a$. Continuing, we contain an infinite decreasing sequence of counting numbers, which is impossible. So (1.9) has no solution from $\mathbb{N}$. $\square$

2 The Circle

We find all integer solutions of

$$x^2 + y^2 = z^2, \tag{2.1}$$

The following are equivalent:

(i) (a, b, c) is a solution;
(ii) $(|a|, |b|, |c|)$ is a solution;
(iii) (na, nb, nc) is a solution for all nonzero n;
(iv) (b, a, c) is a solution.

Also, (2.1) is equivalent to

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

Suppose (a, b, c) is a solution of (2.1) such that $a, b, c > 0$ and $\gcd(a, b, c) = 1$. Then (a, b, c) may be called a **primitive solution,** and all solutions can be obtained from primitive solutions. Observe that not both a and b are even. Also, if $a, b \equiv 1 \pmod 2$, then $c^2 \equiv a^2 + b^2 \equiv 2 \pmod 4$, which is absurd. So exactly one of a and b is even. Say a is even. Then b and c are odd, and

$$\left(\frac{a}{2}\right)^2 = \left(\frac{c+b}{2}\right)\left(\frac{c-b}{2}\right).$$

Also $(c + b)/2$ and $(c - b)/2$ are co-prime, since their sum is c and their difference is b. Hence each must be a square, by Theorem 5; say

$$\frac{c+b}{2} = n^2, \qquad \frac{c-b}{2} = m^2,$$

where $n, m > 0$. Then

$$c = n^2 + m^2, \qquad b = n^2 - m^2, \qquad a = 2nm.$$

Moreover, n and m are co-prime, and exactly one of them is odd (since c is odd).

Conversely, suppose n and m are co-prime, exactly one of them is odd, and $0 < m < n$. Then the triple $(2nm, n^2 - m^2, n^2 + m^2)$ solves (2.1). Moreover, every common prime factor of $n^2 - m^2$ and $n^2 + m^2$ is a factor of the sum $2n^2$ and the difference $2m^2$, and is odd, so it is a common factor of n and m. Thus there is no common prime factor, and the triple is a *primitive* solution.

We conclude that there is a one-to-one correspondence between:

(i) pairs (m, n) of co-prime integers, where $0 < m < n$, and exactly one of m and n is odd;

(ii) primitive solutions (a, b, c) to (2.1), where a is even.

The correspondence is $(x, y) \mapsto (2xy, y^2 - x^2, y^2 + x^2)$.

3 Irrational Numbers

We say that the equation (1.9) has *real* solutions, such as $(\sqrt{d}, 1)$. For example, we say that the equation

$$x^2 = 2 \tag{3.1}$$

has the solution denoted by

$$\sqrt{2}.$$

what do we mean by this?

3.1 Geometry

One approach to solving (3.1) is to let the solution be the length of the diagonal of a square whose side has length 1. In this approach to arithmetic, we assume Euclidean geometry, in which there is a notion of congruence of line segments. Congruence being an equivalence relation, we can define the **length** of a segment to be the class of segments congruent to it. We can add two lengths in the obvious way, by placing two representative segments end to end. To multiply one segment by another, we can use what is called Thales's Theorem. Descartes did this in the *Geometry* [2], and Hilbert worked out the details rigorously in *The Foundations of Geometry* [3].

In a paper called "Thales and the Nine-point Conic" [6], I review what is needed, and suggest an alternative approach, making use of *areas,* as Apollonius did. The point is that,

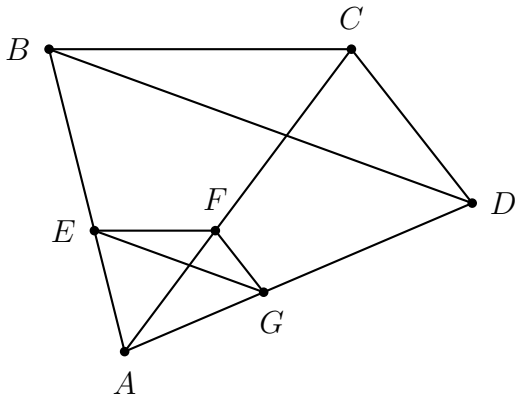

Figure 3.1: A consequence of Thales's Theorem

although Thales's Theorem is generally accepted today, it is nontrivial, because the concept of proportion is nontrivial. For example, in Figure 3.1, $AD = AC$, $AG = AF$, and $EF \parallel BC$. We can use Thales's Theorem to prove that $EG \parallel BD$. This result has nothing obvious to do with proportion, and yet it is not clear how to prove the result *without* using proportions.

3.2 Dedekind Cuts

An alternative approach to arithmetic is Dedekind's, worked out in *Continuity and Irrational Numbers* [1]. We start with the rational numbers as an **ordered field,** namely an ordered set equipped also with operations of addition and multiplication that are compatible with the ordering in the usual way. We obtain each real number as a **cut,** namely a partition of $\mathbb{Q}$ into two nonempty parts, each member of the first part being less than each member in the second part. Two such partitions are considered the same if they differ at a single point.

This point will be the greatest member of the first part of one partition, but the least member of the second part of the other partition. That point will be a rational number, which we can identify with the cut just described. In this way, every rational number becomes a real number; but some real numbers are not determined by rational numbers in this way.

Dedekind's procedure gives $\mathbb{R}$ as an ordered set satisfying the **Completeness Axiom,** whereby every nonempty set of real numbers that has an upper bound has a least upper bound, or supremum. We have to define addition and multiplication on $\mathbb{R}$ so that each of the functions

$$x \mapsto a + x, \qquad\qquad x \mapsto ax$$

is continuous. This will give us $\mathbb{R}$ as an ordered field. We can then define

$$\sqrt{2} = \sup\{x \in \mathbb{Q} \colon x^2 < 2\}.$$

Continuity will ensure that this solves (3.1).

3.3 Cauchy Sequences

There are other approaches to the real numbers. For example, we can define a real number to be an equivalence class of Cauchy sequences of rational numbers, two sequences being equivalent if the sequence of differences of their terms has limit 0.

4 The Square Root of Two

Without going into the details of any particular development of $\mathbb{R}$, we shall now find a sequence of rational numbers whose limit is $\sqrt{2}$. We note that

$$\sqrt{2} = 1 + (\sqrt{2} - 1), \qquad \frac{1}{\sqrt{2}-1} = \sqrt{2} + 1,$$

so that

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + \dfrac{1}{\sqrt{2}+1}} = 1 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{\sqrt{2}+1}}} \tag{4.1}$$

and so on. Replacing each instance of $1/(\sqrt{2}+1)$ with 0, we define

$$\frac{p_0}{q_0} = 1, \qquad \frac{p_1}{q_1} = 1 + \frac{1}{2} = \frac{3}{2}, \qquad \frac{p_2}{q_2} = 1 + \frac{1}{2 + \dfrac{1}{2}} = \frac{7}{5},$$

and in general

$$\frac{p_{n+1}}{q_{n+1}} = 1 + \frac{1}{1 + \dfrac{p_n}{q_n}} = \frac{p_n + 2q_n}{p_n + q_n}.$$

The equations alone do not define p_n and q_n separately. We require also that each of them be positive, and that the two of

n	0	1	2	3	4	5	6	7
p_n	1	3	7	17	41	99	239	577
q_n	1	2	5	12	29	70	169	408

Table 4.1: Numerators and denominators of convergents of $\sqrt{2}$

them be prime to one another. In this case,

$$\begin{aligned} p_0 &= 1, & p_1 &= 3, & p_{n+2} &= p_n + 2q_n, \\ q_0 &= 1, & q_1 &= 2, & q_{n+2} &= p_n + q_n. \end{aligned} \tag{4.2}$$

We compute some values in Table 4.1. Testing them suggests the following.

Theorem 7. *When p_n and q_n are as in (4.2), then*

$$p_n{}^2 - 2q_n{}^2 = (-1)^{n+1}, \tag{4.3}$$

so that

$$\left| \left(\frac{p_n}{q_n} \right)^2 - 2 \right| = \frac{1}{q_n{}^2}.$$

Since also the sequence of q_n increases without bound,

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \sqrt{2} < \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}, \tag{4.4}$$

and the sequence of p_n/q_n is Cauchy, with limit $\sqrt{2}$.

Proof. We use induction. The claim (4.3) holds when $n = 0$. If it holds when $n = m$, then

$$\begin{aligned} p_{m+1}{}^2 - 2q_{m+1}{}^2 &= (p_m + 2q_m)^2 - 2(p_m + q_m)^2 \\ &= -p_m{}^2 + 2q_m{}^2 = -(-1)^{m+1} = (-1)^{m+2}, \end{aligned}$$

so (4.3) holds when $n = m + 1$. □

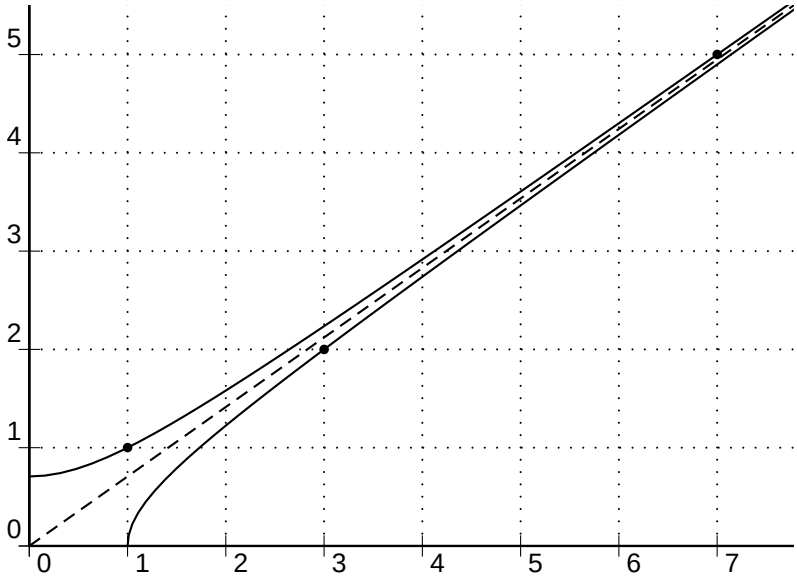

Figure 4.1: Integer points of hyperbolas $x^2 - 2y^2 = \pm 1$

We may now refer to the fractions p_n/q_n as **convergents** of $\sqrt{2}$. According to the theorem, (p_n, q_n) is a point on the hyperbola given by

$$x^2 - 2y^2 = 1, \tag{4.5}$$

when n is odd, and

$$2y^2 - x^2 = 1,$$

when n is even. Each hyperbola has asymptotes

$$y = \pm \frac{1}{\sqrt{2}} x,$$

as in Figure 4.1.

5 The Pell Equation

Equation (4.5) is an example of a **Pell equation.** The general form of a Pell equation is

$$x^2 - dy^2 = 1, \tag{5.1}$$

where d is a positive nonsquare integer. We are interested in integer solutions, and among these, **positive** solutions, meaning each entry is positive. There are trivial solutions, namely $(\pm 1, 0)$. Every other integer solution is $(-a, \pm b)$ or $(a, -b)$, where (a, b) is a positive solution.

Theorem 8. *If* (a, b) *is a solution to* (5.1) *and*

$$a + b\sqrt{d} > 1, \tag{5.2}$$

then (a, b) *is a* positive *solution to* (5.1).

Proof. We are given

$$1 = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}),$$

along with (5.2), and this implies

$$0 < a - b\sqrt{d} < 1 < a + b\sqrt{d}.$$

Hence b must be positive, and then a must be positive. □

There is more along the same lines:

Theorem 9. *If* (a, b) *and* (s, t) *are solutions to* (5.1)*, then so is*

$$(as + dbt, bs + at),$$

which is obtained from the equation

$$as + dbt + (bs + at)\sqrt{d} = (a + b\sqrt{d})(s + t\sqrt{d}).$$

Proof. Write the proposed solution as (ℓ, m). Then

$$\ell \pm m\sqrt{d} = (a \pm b\sqrt{d})(s \pm t\sqrt{d}),$$

and so

$$\begin{aligned} 1 &= (a^2 - db^2)(s^2 - dt^2) \\ &= (a + b\sqrt{d})(a - b\sqrt{d})(s + t\sqrt{d})(s - t\sqrt{d}) \\ &= (a + b\sqrt{d})(s + t\sqrt{d})(a - b\sqrt{d})(s - t\sqrt{d}) \\ &= (\ell + m\sqrt{d})(\ell - m\sqrt{d}) = \ell^2 - dm^2. \end{aligned}$$

Thus (ℓ, m) is a solution of (5.1). □

Theorem 10. *If, for some positive nonsquare* d*,* (5.1) *has a positive solution, then it has a positive solution* (a, b) *such that, for every positive solution* (s, t)*, for some positive* n*,*

$$s + t\sqrt{d} = (a + b\sqrt{d})^n.$$

Proof. We let (a, b) be the positive solution that minimizes $x + y\sqrt{d}$. Since $a + b\sqrt{d} > 1$, the sequence of $(a + b\sqrt{d})^n$ increases without bound, and so, for some n,

$$\begin{aligned} (a + b\sqrt{d})^n \leqslant s + t\sqrt{d} < (a + b\sqrt{d})^{n+1}, \\ 1 \leqslant (s + t\sqrt{d})(a - b\sqrt{d})^n < a + b\sqrt{d}. \end{aligned}$$

For some integers ℓ and m,

$$(s + t\sqrt{d})(a - b\sqrt{d})^n = \ell + m\sqrt{d}.$$

This makes (ℓ, m) a solution of (5.1), by Theorem 9. It cannot be a positive solution, by minimality of (a, b); therefore, by Theorem 8, (ℓ, m) is the trivial solution $(1, 0)$, so (s, t) is as claimed. □

By Theorem 13 on page 35, (5.1) *will* always have a positive solution. Meanwhile, we can just hunt for solutions in particular cases.

Example 1. We can see by inspection that $(3, 2)$ is the solution of (4.5) that minimizes $x + y\sqrt{2}$. Indeed,

$$4/3 < \sqrt{2} < 3/2, \qquad 3 + 2\sqrt{2} < 6,$$

so the only possible solutions to check are

$$1 + \sqrt{2}, \qquad 2 + \sqrt{2}, \qquad 4 + \sqrt{2}, \qquad 1 + 3\sqrt{2},$$

and none of these is actually a solution. By the theorem, we now know all positive solutions of (4.5): they are (a_n, b_n), where $n \in \mathbb{N}$ and

$$a_n + b_n\sqrt{2} = (3 + 2\sqrt{2})^n.$$

Allowing n to be also zero or negative, we obtain all solutions where $x > 0$. We have $(a + b\sqrt{d})^{-1} = a - b\sqrt{d}$ and

$$(3 \pm 2\sqrt{2})(x + y\sqrt{2}) = 3x \pm 4y + (\pm 2x + 3y)\sqrt{2}.$$

Applying the latter repeatedly, we can find all solutions just mentioned. See Figure 5.1. Alternatively, from (4.2) we obtain

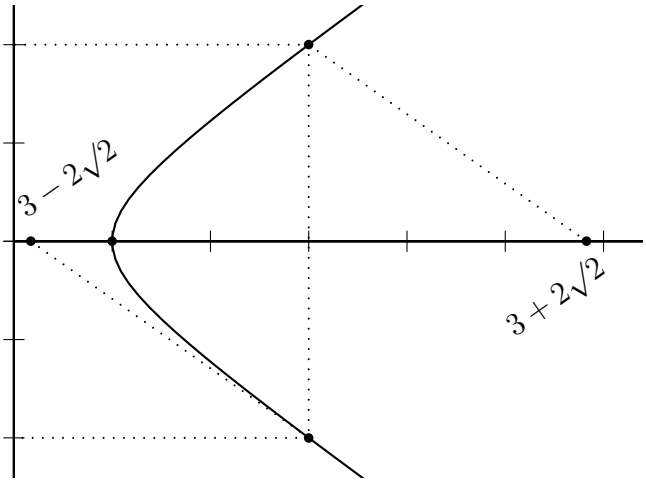

Figure 5.1: Integer points of hyperbola $x^2 - 2y^2 = 1$

$$p_{n+2} = p_{n+1} + 2q_{n+1} = p_n + 2q_n + 2(p_n + q_n) = 3p_n + 4q_n,$$
$$q_{n+2} = p_{n+1} + q_{n+1} = p_n + 2q_n + p_n + q_n = 2p_n + 3q_n,$$

and so, by induction,

$$(a_n, b_n) = (p_{2n-1}, q_{2n-1}).$$

Thus all positive solutions of (4.5) correspond to certain convergents of $\sqrt{2}$. We may note

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

This is meaningful, even if $n \leqslant 0$, and then it yields the remaining solutions of (4.5) in which $x > 0$; the solutions in which $x < 0$ are $(-a_n, -b_n)$, where $n \in \mathbb{Z}$.

6 Continued Fractions

The method of Example 1 will work for arbitrary positive non-square d in (5.1). Given any real number x, such as $\sqrt{d}$, we define sequences of real numbers a_n and ξ_n, where each a_n is an integer,

$$0 \leqslant \xi_n < 1,$$

and

$$x = a_0 + \xi_0 = a_0 + \frac{1}{a_1 + \xi_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \xi_2}}$$

and so on, as long as ξ_n is not zero (which it will never be, if x is irrational). In general,

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n + \xi_n}}}}, \tag{6.1}$$

and we may write this also as

$$a_0 + \frac{1}{a_1+}\ \frac{1}{a_2+}\cdots\ \frac{1}{a_{n-1}+}\ \frac{1}{a_n + \xi_n}.$$

Thus

$$a_0 = [x], \qquad \xi_0 = x - a_0,$$

square brackets denoting the greatest-integer function; and by recursion,

$$a_{n+1} = \left[\frac{1}{\xi_n}\right], \qquad \xi_{n+1} = \frac{1}{\xi_n} - a_{n+1},$$

where ξ_n must be non-zero for a_{n+1} to be defined. In (4.1) on page 23, we performed the computations when $x = \sqrt{2}$, obtaining $a_0 = 1$, but $a_n = 2$ when $n > 0$.

Example 2. When $x = \sqrt{6}$, we compute

$$\begin{aligned}
\sqrt{6} &= 2 + (\sqrt{6} - 2), \\
\frac{1}{\sqrt{6}-2} &= \frac{\sqrt{6}+2}{2} = 2 + \frac{\sqrt{6}-2}{2}, \\
\frac{2}{\sqrt{6}-2} &= \sqrt{6} + 2 = 4 + (\sqrt{6} - 2),
\end{aligned}$$

so that $a_n = 2$ when $n = 0$ or n is odd, and $a_n = 4$ when n is positive and even.

In the right-hand side of (6.1), if we replace ξ_n with 0, we obtain the number that we shall denote by

$$[a_0; a_1, \ldots, a_n].$$

Thus

$$[a_0] = a_0, \quad [a_0; a_1] = a_0 + \frac{1}{a_1}, \quad [a_0; a_1, a_2] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}}, \tag{6.2}$$

and so forth; the general term is given recursively by

$$[a_0; a_1, \ldots, a_{n+1}] = \left[a_0; a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right]. \tag{6.3}$$

By studying (6.1), we can see that, as in (4.4), so generally,

$$[a_0] < [a_0; a_1, a_2] < \cdots < x < \cdots < [a_0; a_1, a_2, a_3] < [a_0; a_1].$$

We shall work out a formal proof of this, by finding integers p_n and q_n such that

$$[a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}, \tag{6.4}$$

as we have already done when considering the example $x = \sqrt{2}$. From (6.2), we want

$$\frac{p_0}{q_0} = a_0, \qquad \frac{p_1}{q_1} = \frac{a_0a_1 + 1}{a_1}, \qquad \frac{p_2}{q_2} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1}.$$

Hence we may define

$$\begin{array}{lll} p_0 = a_0, & p_1 = p_0a_1 + 1, & p_2 = p_1a_2 + p_0, \\ q_0 = 1, & q_1 = a_1, & q_2 = q_1a_2 + q_0. \end{array}$$

Theorem 11. *For all n in ω, the definitions*

$$p_{n+2} = p_{n+1}a_{n+2} + p_n, \qquad q_{n+2} = q_{n+1}a_{n+2} + q_n$$

satisfy (6.4).

Proof. We use induction. We have just seen that the claim holds when $n = 0$. Supposing, for some m, the claim holds

when $n = m$, we have

$$\begin{aligned}
[a_0; a_1, \ldots, a_{m+3}] &= \left[a_0; a_1, \ldots, a_{m+1}, a_{m+2} + \frac{1}{a_{m+3}}\right] \\
&= \frac{p_{m+1} \cdot \left(a_{m+2} + \dfrac{1}{a_{m+3}}\right) + p_m}{q_{m+1} \cdot \left(a_{m+2} + \dfrac{1}{a_{m+3}}\right) + q_m} \\
&= \frac{p_{m+1}a_{m+2}a_{m+3} + p_{m+1} + p_m a_{m+3}}{q_{m+1}a_{m+2}a_{m+3} + q_{m+1} + q_m a_{m+3}} \\
&= \frac{p_{m+2}a_{m+3} + p_{m+1}}{q_{m+2}a_{m+3} + q_{m+1}} = \frac{p_{m+3}}{q_{m+3}}.
\end{aligned}$$

By induction, the claim holds for all n in ω. □

We now confirm the additional property that we wanted.

Theorem 12. *For all n in ω,*

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

Proof. We prove the equivalent statement

$$p_{n+1}q_n - p_n q_{n+1} = (-1)^n. \tag{6.5}$$

Again we use induction. We have

$$p_1 q_0 - p_0 q_1 = p_0 a_1 + 1 - a_0 a_1 = 1,$$

so the claim holds when $n = 0$. Supposing it holds when $n = m$, we have

$$\begin{aligned}
&p_{m+2}q_{m+1} - p_{m+1}q_{m+2} \\
&\quad = (p_{m+1}a_{m+2} + p_m)q_{m+1} - p_{m+1}(q_{m+1}a_{m+2} + q_m) \\
&\quad = p_m q_{m+1} - p_{m+1}q_m,
\end{aligned}$$

which is $-(-1)^m$, that is, $(-1)^{m+1}$. Thus the claim holds for all n in ω. □

Corollary. *p_n and q_n are prime to one another.*

Proof. Apply Theorem 1 to (6.5). □

Corollary. *The sequence of p_n/q_n is Cauchy, with limit x.*

The latter corollary justifies referring to the p_n/q_n as the **convergents** of x.

7 Solubility of the Pell Equation

As usual, d is a positive nonsquare.

Lemma 5. *For some positive k, the equation*

$$x^2 - dy^2 = k \tag{7.1}$$

has infinitely many solutions.

Proof. Let $(p_n/q_n \colon n \in \omega)$ be the sequence of convergents for $\sqrt{d}$. When n is odd, then

$$0 < \frac{p_n}{q_n} - \sqrt{d} < \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{1}{q_{n+1}q_n} < \frac{1}{{q_n}^2},$$
$$0 < \frac{p_n}{q_n} + \sqrt{d} < \frac{2p_n}{q_n}.$$

Multiplying gives

$$0 < \frac{{p_n}^2}{{q_n}^2} - d < \frac{2p_n}{{q_n}^3}, \qquad 0 < {p_n}^2 - d{q_n}^2 < \frac{2p_n}{q_n} < \frac{2p_1}{q_1}.$$

Thus there are finitely many possibilities for ${p_n}^2 - d{q_n}^2$, so one of them must be realized infinitely many times. □

Theorem 13. *The Pell equation* (5.1) *has a positive solution.*

Proof. By Lemma 5, we may let k be a positive integer such that (7.1) has infinitely many solutions. There are just finitely many pairs (a, b) such that $0 \leqslant a < k$ and $0 \leqslant b < k$. Hence

there must be one such pair for which (7.1) and the congruences

$$x \equiv a \ \ \& \ \ y \equiv b \pmod{k}$$

simultaneously have infinitely many solutions. Let (m, n) and (s, t) be two solutions. By computations as for Theorem 9,

$$k^2 = (m^2 - dn^2)(s^2 - dt^2) = (ms - dnt)^2 - d(mt - ns)^2. \quad (7.2)$$

Moreover, $m \equiv s$ and $n \equiv t$ *modulo* k, so that

$$ms - dnt \equiv m^2 - dn^2 \equiv 0, \quad mt - ns \equiv mn - nm \equiv 0.$$

Therefore, in (7.2) we can divide by k^2, obtaining

$$1 = \left(\frac{ms - dnt}{k}\right)^2 - d\left(\frac{mt - ns}{k}\right)^2.$$

Changing signs as needed gives a positive solution to (5.1). □

8 Quadratic Fields

We can write the Pell equation (5.1) as

$$(x + y\sqrt{d})(x - y\sqrt{d}) = 1. \tag{8.1}$$

We consider the factors here individually. We define

$$\{u + v\sqrt{d} \colon (u, v) \in \mathbb{Q}^2\} = \mathbb{Q}(\sqrt{d}) = K.$$

We define on K the operation $\xi \mapsto \xi'$, where

$$(u + v\sqrt{d})' = u - v\sqrt{d}.$$

We may assume d is a squarefree integer; it may be negative. In any case, $K \subseteq \mathbb{C}$. If $d < 0$, then $\xi' = \overline{\xi}$ (the complex conjugate of ξ). If $d > 0$, then $K \subseteq \mathbb{R}$.

Theorem 14. *K is closed under addition, subtraction, multiplication, and division. The operation $\xi \mapsto \xi'$ on K distributes over addition and multiplication, so that*

$$(\xi + \eta)' = \xi' + \eta', \qquad (\xi\eta)' = \xi'\eta'.$$

The proof is an exercise. In technical algebraic terminology, the theorem is that K is a **subfield** of $\mathbb{C}$, and $\xi \mapsto \xi'$ is an **automorphism** of K.

We now define two functions from K to $\mathbb{Q}$, called **trace** and **norm,** given respectively by

$$\mathrm{Tr}(\xi) = \xi + \xi', \qquad \mathrm{N}(\xi) = \xi\xi'.$$

Then

$$\mathrm{Tr}(\xi+\eta)=\mathrm{Tr}(\xi)+\mathrm{Tr}(\eta),\qquad \mathrm{N}(\xi)\,\mathrm{N}(\eta)=\mathrm{N}(\xi\eta).$$

For any two elements α and β of K, we define

$$\{\alpha x+\beta y\colon (x,y)\in\mathbb{Z}^2\}=\langle\alpha,\beta\rangle.$$

Normally $\alpha\neq 0$ and $\beta/\alpha\notin\mathbb{Q}$; this means, in $\mathbb{Z}$,

$$\alpha x+\beta y=0 \implies (x,y)=(0,0); \tag{8.2}$$

in this case, $\langle\alpha,\beta\rangle$ is a **lattice** of K. A lattice is closed under addition and subtraction, but not necessarily under multiplication. However, $\langle 1,\sqrt{d}\rangle$ is closed under multiplication. Now can give an example promised in Chapter 1.

Example 3. In $\langle 1,\sqrt{-5}\rangle$ we have

$$2\cdot 3=(1+5\sqrt{-5})(1-5\sqrt{-5}),$$

and therefore

$$2\mid(1+5\sqrt{-5})(1-5\sqrt{-5}),$$

although

$$2\nmid 1\pm 5\sqrt{-5}.$$

Thus 2 is not prime in $\langle 1,\sqrt{-5}\rangle$, according to the definition (1.7) on page 14. However, 2 is irreducible, according to (1.6). For suppose $2=\alpha\beta$. We have

$$4=\mathrm{N}(2)=\mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

Since in general

$$\mathrm{N}(x+y\sqrt{-5})=x^2+5y^2,$$

norms of nonzero elements of $\langle 1,\sqrt{-5}\rangle$ are positive integers, but never 2. Thus we may assume $\mathrm{N}(\alpha)=1$, and therefore $\alpha=\pm 1$, so $\beta=\pm 2$, and $2\mid\beta$.

We can write (8.1) as

$$\mathrm{N}(\xi) = 1 \;\;\&\;\; \xi \in \langle 1, \sqrt{d} \rangle \,. \tag{8.3}$$

That is, solutions to (5.1), or (8.1), and (8.3) are in one-to-one correspondence under the map

$$(x, y) \mapsto x + y\sqrt{d}.$$

The product of solutions of (8.3) is a solution, as we have seen in effect in Theorem 9 on page 27. Equation (5.1) may seem simpler than (8.3). However, in case $d > 0$, so that $K \subseteq \mathbb{R}$, the solutions to (5.1), known from Theorems 10 and 13, become, for (5.1), the solutions $\pm\alpha^n$, where $n \in \mathbb{Z}$, and α is the least solution that exceeds 1.

For our purposes, a **quadratic form** is a polynomial

$$ax^2 + bxy + cy^2, \tag{8.4}$$

where the coefficients a, b, and c are integers. The Pell equation (5.1) is just one example of an equation

$$f(x, y) = m, \tag{8.5}$$

where f is a quadratic form.

Example 4. We solve the quadratic Diophantine equation

$$4x^2 + 2xy - y^2 = 4. \tag{8.6}$$

We start by completing the square in x:

$$\begin{aligned} 4x^2 + 2xy = 4\left(x^2 + \frac{xy}{2}\right) &= 4\left(x^2 + \frac{xy}{2} + \frac{y^2}{16}\right) - \frac{y^2}{4}y \\ &= 4\left(x + \frac{y}{4}\right)^2 - \frac{y^2}{4}. \end{aligned}$$

Thus our equation becomes

$$\left(2x + \frac{y}{2}\right)^2 - 5\left(\frac{y}{2}\right)^2 = 4$$

and then

$$\left(2x + \frac{1+\sqrt{5}}{2}y\right)\left(2x + \frac{1-\sqrt{5}}{2}y\right) = 4.$$

We let $d = 5$, so that $K = \mathbb{Q}(\sqrt{5})$. We want then to solve

$$\mathrm{N}(\xi) = 4 \;\;\&\;\; \xi \in \left\langle 2, \frac{1+\sqrt{5}}{2} \right\rangle, \tag{8.7}$$

which resembles (8.3).

We shall develop a general method encompassing (8.3) and (8.7). Meanwhile, for the sake of solving (8.7) in particular, we define

$$\frac{1+\sqrt{5}}{2} = \phi;$$

this is the so-called **Golden Ratio.** It has an intimate connexion with the sequence $(\mathrm{F}_n \colon n \in \omega)$ of **Fibonacci numbers,** given by

$$\mathrm{F}_0 = 0, \qquad \mathrm{F}_1 = 1, \qquad \mathrm{F}_{n+2} = \mathrm{F}_n + \mathrm{F}_{n+1}.$$

We can continue the sequence backwards by writing the last rule as

$$\mathrm{F}_{n-2} = \mathrm{F}_n - \mathrm{F}_{n-1}.$$

Some terms of the bi-directional sequence are as in Table 8.1. It will be useful later (page 50) to note the following.

n	0	1	2	3	4	5	6	7	8	9	10	11
F_n	0	1	1	2	3	5	8	13	21	34	55	89
F_{-n}	0	1	-1	2	-3	5	-8	13	-21	34	-55	89

Table 8.1: Terms of the Fibonacci sequence

Theorem 15. *For all n in $\mathbb{Z}$,*

$$\phi^n = \mathrm{F}_{n-1} + \mathrm{F}_n\phi. \tag{8.8}$$

Proof. Trivially (8.8) holds when $n = 1$. Also, since

$$\phi^2 = 1 + \phi, \tag{8.9}$$

we have

$$(x + y\phi)\phi = x\phi + y\phi^2 = y + (x + y)\phi. \tag{8.10}$$

Hence, if (8.8) holds when $n = k$, then

$$\phi^{k+1} = (\mathrm{F}_{k-1} + \mathrm{F}_k\phi)\phi = \mathrm{F}_k + (\mathrm{F}_{k-1} + \mathrm{F}_k)\phi = \mathrm{F}_k + \mathrm{F}_{k+1}\phi,$$

so (8.8) holds when $n = k+1$. Therefore it holds for all positive n. Moreover, since

$$\phi^{-1} = \phi - 1,$$

we have

$$\begin{aligned}(x + y\phi)\phi^{-1} &= (x + y\phi)(\phi - 1)\\ &= -x + y\phi^2 + (x - y)\phi = y - x + x\phi,\end{aligned}$$

so that if (8.8) holds when $n = k$, it holds when $n = k-1$. □

One can understand Theorem 15 in terms of matrices. By (8.10), multiplication in $\langle 1, \phi \rangle$ by ϕ corresponds, under the map

$$x + y\phi \mapsto \begin{pmatrix} x \\ y \end{pmatrix},$$

to the multiplication given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x + y \end{pmatrix}.$$

Inverting the square matrix, we have

$$\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y - x \\ x \end{pmatrix},$$

corresponding to multiplication by ϕ^{-1}.

We generalize Example 4:

Theorem 16. *If f is the quadratic form in (8.4), where $a \neq 0$, and*

$$b^2 - 4ac = D,$$

where $D = s^2 d$, and d is a squarefree integer different from 1, then the solutions to (8.5) correspond, under the map

$$(x, y) \mapsto \alpha x + \beta y,$$

where

$$\alpha = a, \qquad \beta = \frac{b + \sqrt{D}}{2},$$

to the solutions from $\mathbb{Q}(\sqrt{d})$ of

$$\mathrm{N}(\xi) = am \ \ \& \ \ \xi \in \Lambda, \tag{8.11}$$

where

$$\Lambda = \langle \alpha, \beta \rangle. \tag{8.12}$$

Proof. We complete the square:

$$\begin{aligned} af(x,y) &= \Big((ax)^2 + b(ax)y + \frac{b^2y^2}{4}\Big) - \Big(\frac{b^2}{4} - ac\Big)y^2 \\ &= \Big(ax + \frac{by}{2}\Big)^2 - \frac{Dy^2}{4} \\ &= \Big(ax + \frac{b+\sqrt{D}}{2}\cdot y\Big)\Big(ax + \frac{b-\sqrt{D}}{2}\cdot y\Big) \\ &= (\alpha x + \beta y)(\alpha x + \beta' y) = \mathrm{N}\,(\alpha x + \beta y)\,. \end{aligned}$$ □

In Example 4, had we strictly followed the method of Theorem 16, we should have arrived at the system

$$\mathrm{N}\,(\xi) = 16 \;\;\&\;\; \xi \in \langle 4, 1 + 1\sqrt{5}\rangle\,.$$

By replacing ξ here with 2ξ, we obtain (8.7).

Suppose α is one solution of (8.11), and some ε in K is a solution of

$$\mathrm{N}\,(\eta) = 1 \;\;\&\;\; \eta\Lambda \subseteq \Lambda. \tag{8.13}$$

Then $\varepsilon^n\alpha$ is a solution of (8.11) whenever $n \in \mathfrak{o}$. We shall see that the same is true, even when $n \in \mathbb{Z}$, and moreover there is ε such that every solution is of the given form.

9 Orders

For some squarefree integer d, we let K is the field $\mathbb{Q}(\sqrt{d})$, and $\Lambda = \langle \alpha, \beta \rangle$ as in (8.12) for some α and β in K satisfying (8.2). We now define

$$\{\eta \in K : \eta\Lambda \subseteq \Lambda\} = \mathfrak{O}_\Lambda;$$

this is the **order** of Λ. We can rewrite (8.13) as

$$\mathrm{N}(\eta) = 1 \ \ \& \ \ \eta \in \mathfrak{O}_\Lambda. \tag{9.1}$$

We need to understand $\mathfrak{O}_\Lambda$. We note first that $\mathfrak{O}_\Lambda$ is closed under addition, subtraction, and multiplication; this means it is a **ring** (as also on page 14).

Theorem 17. *$\mathfrak{O}_\Lambda = \langle 1, a\tau \rangle$, where $\tau = \beta/\alpha$ and*

$$a\tau^2 + b\tau + c = 0, \tag{9.2}$$

where a, b, and c are integers prime to one another.

Proof. We have first

$$\begin{aligned} \theta \in \mathfrak{O}_\Lambda &\iff \theta \langle \alpha, \beta \rangle \subseteq \langle \alpha, \beta \rangle \\ &\iff \theta\alpha \in \langle \alpha, \beta \rangle \ \ \& \ \ \theta\beta \in \langle \alpha, \beta \rangle \\ &\iff \theta \in \langle 1, \tau \rangle \ \ \& \ \ \theta\tau \in \langle 1, \tau \rangle . \end{aligned}$$

Any element θ of $\langle 1, \tau \rangle$ is $x + y\tau$ for some x and y in $\mathbb{Z}$, and then

$$\begin{aligned} \theta\tau \in \langle 1, \tau \rangle &\iff x\tau + y\tau^2 \in \langle 1, \tau \rangle \\ &\iff y\tau^2 \in \langle 1, \tau \rangle \\ &\iff \frac{yb}{a}\tau + \frac{yc}{a} \in \langle 1, \tau \rangle \\ &\iff a \mid yb \ \ \& \ \ a \mid yc \\ &\iff a \mid y. \end{aligned}$$

In short, $\theta \in \mathfrak{O}_\Lambda \iff \theta \in \langle 1, a\tau \rangle$. □

Corollary. *$\mathfrak{O}_\Lambda$ is closed under $\xi \mapsto \xi'$, and therefore $\mathfrak{O}_\Lambda$ contains the inverse of its every element that has norm 1. Also, the trace of every element of $\mathfrak{O}_\Lambda$ is an integer.*

Proof. We rewrite (9.2) as

$$(a\tau)^2 + b(a\tau) + ac = 0. \tag{9.3}$$

For any element γ of K, we have

$$(x - \gamma)(x - \gamma') = x^2 - \mathrm{Tr}(\gamma)x + \mathrm{N}(\gamma). \tag{9.4}$$

In particular, $a\tau$ is a zero of the polynomial

$$x^2 - \mathrm{Tr}(a\tau)x + \mathrm{N}(a\tau).$$

Comparison with (9.3) shows

$$\mathrm{Tr}(a\tau) = -b,$$

which is in $\mathfrak{O}_\Lambda$. Since

$$a\tau' = \mathrm{Tr}(a\tau) - a\tau,$$

this is in $\mathfrak{O}_\Lambda$. □

Theorem 18. *When $d > 0$, then $\mathfrak{O}_\Lambda$ has an element whose integral powers are precisely the positive elements of $\mathfrak{O}_\Lambda$ having norm 1.*

Proof. For some positive integer c,

$$\langle 1, c\sqrt{d}\rangle \subseteq \mathfrak{O}_\Lambda.$$

If $\mathrm{N}\,(a + bc\sqrt{d}) = 1$ and $a + bc\sqrt{d} > 1$, this means precisely that (a, b) is a positive solution of the Pell equation

$$x^2 - dc^2y^2 = 1.$$

Such a solution (a, b) exists by Theorem 13. Let

$$a + bc\sqrt{d} = \varepsilon.$$

Then $\varepsilon\varepsilon' = 1$, so

$$\varepsilon^2 - \mathrm{Tr}(\varepsilon)\varepsilon + 1 = 0, \qquad 0 < \varepsilon^{-1} < 1 < \varepsilon.$$

Suppose n is an integer exceeding ε. Then

$$1 < \mathrm{Tr}(\varepsilon) = \varepsilon + \varepsilon' < n + 1.$$

Since, finally, $\mathrm{Tr}(\varepsilon)$ is an integer, only finitely many elements of $\mathfrak{O}_\Lambda$ having norm 1 can exceed 1, but not ε. Let ε_Λ be the least of them. As in the proof of Theorem 10, for any positive element γ of $\mathfrak{O}_\Lambda$, for some integer n,

$$\begin{aligned} {\varepsilon_\Lambda}^n \leqslant \gamma < {\varepsilon_\Lambda}^{n+1}, \\ 1 \leqslant \gamma {\varepsilon_\Lambda}^{-n} < \varepsilon_\Lambda. \end{aligned}$$

If $\mathrm{N}\,(\gamma) = 1$, then $\gamma = {\varepsilon_\Lambda}^n$. □

We can now state a method for solving systems (8.11) when $d > 0$. If γ is a solution, then so are all $\pm\gamma\varepsilon_\Lambda{}^n$, when ε_Λ is as in the proof of Theorem 18. Therefore we may assume

$$1 \leqslant \gamma < \varepsilon_\Lambda.$$

Say $\gamma = \alpha k + \beta\ell$. Then (k, ℓ) satisfies

$$1 \leqslant \alpha x + \beta y < \varepsilon_\Lambda,$$

that is, (k, ℓ) lies between the two straight lines given respectively by

$$1 = \alpha x + \beta y, \qquad\qquad \alpha x + \beta y = \varepsilon_\Lambda. \tag{9.5}$$

Moreover, from the proof of Theorem 16, (k, ℓ) lies on the hyperbola that can be given by

$$am = (\alpha x + \beta y)(\alpha x + \beta' y);$$

the asymptotes of this hyperbola are given respectively by

$$0 = \alpha x + \beta y, \qquad\qquad 0 = \alpha x + \beta' y.$$

Thus the straight lines given in (9.5) are parallel to the first asymptote and cut off a segment of one branch of the hyperbola. This segment lies in the parallelogram bounded by the parallel lines given in (9.5), by the second asymptote, and by the line parallel to this given by

$$am = \alpha x + \beta' y.$$

We can see how this works in the following.

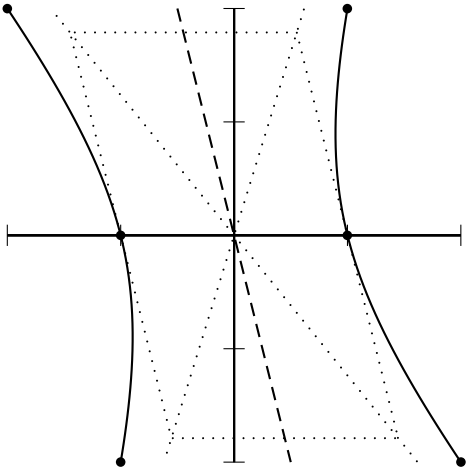

Figure 9.1: Hyperbola $(2x + \phi y)(2x + \phi' y) = 4$

Example 5. We continue with Example 4. In $\mathbb{Q}(\sqrt{5})$, we want to solve

$$\mathrm{N}(\xi) = 4 \ \ \& \ \ \xi \in \Lambda, \tag{9.6}$$

where

$$\Lambda = \langle 2, \phi \rangle .$$

Thus we are looking for $2x + \phi y$, where (x, y) lies on the hyperbola given by

$$(2x + \phi y)(2x + \phi' y) = 4,$$

shown in Figure 9.1. Since $\mathfrak{O}_\Lambda$ is also the order of $\langle 1, \phi/2 \rangle$, and

$$4\Big(\frac{\phi}{2}\Big)^2 - 2 \cdot \frac{\phi}{2} - 1 = 0,$$

we have by Theorem 17

$$\mathfrak{O}_\Lambda = \langle 1, 2\phi \rangle = \langle 1, \sqrt{5} \rangle .$$

We want elements of norm 1, and these come from solutions of

$$x^2 - 5y^2 = 1, \tag{9.7}$$

and these solutions come from convergents of $\sqrt{5}$ (though we have not proved this). We compute

$$\sqrt{5} = 2 + (\sqrt{5} - 2),$$
$$\frac{1}{\sqrt{5}-2} = \sqrt{5} + 2 = 4 + (\sqrt{5} - 2),$$

so

$$\sqrt{5} = [2; \overline{4}].$$

The first two convergents are 2 and $9/4$. We have

$$2^2 - 5 = -1, \qquad 9^2 - 5 \cdot 4^2 = 1.$$

Thus $(9, 4)$ is a positive solution of (9.7), and we can check that there are no positive solutions with

$$x + y\sqrt{5} < 9 + 4\sqrt{5}.$$

It will be useful to note

$$9 + 4\sqrt{5} = 5 + 8\phi.$$

By Theorem 18, every element of $\mathfrak{O}_\Lambda$ of norm 1 is $\pm(5 + 8\phi)^n$ for some n in $\mathbb{Z}$. This means, if γ is a solution of (9.6), then so is $\pm(5 + 8\phi)^n\gamma$. We may thus assume

$$1 < \gamma < 5 + 8\phi.$$

Let $\gamma = 2k + \ell\phi$. Then (k, ℓ) lies between the parallel lines given by

$$2x + y\phi = 1, \qquad 2x + y\phi = 5 + 8\phi$$

and the parallel lines given by

$$2x + y\phi' = 0, \qquad\qquad 2x + y\phi' = 4,$$

shown in Figure 9.2. There are finitely many integer points in that parallelogram; for every such point (x, y), we compute $\mathrm{N}(2x + y\phi)$. In fact, once we have computed the norms indicated in the figure, we can see that the only points for which the corresponding norm is 4 are $(1, 0)$, $(1, 2)$, and $(2, 6)$. Therefore the solutions to (8.6) are those (x, y) such that $2x + y\phi = \pm(5 + 8\phi)^n\gamma$, where $n \in \mathbb{Z}$ and $\gamma \in \{2, 2 + 2\phi, 4 + 6\phi\}$. Moreover, by Theorem 15,

$$\{2, 2 + 2\phi, 4 + 6\phi\} = \{2\phi^0, 2\phi^2, 2\phi^4\}.$$

Thus the solutions to (9.6) are $\pm 2\phi^{2k}$, where $k \in \mathbb{Z}$; hence these solutions are

$$\pm(2\mathrm{F}_{2k-1} + 2\mathrm{F}_{2k}\phi).$$

Under the correspondence $(x, y) \mapsto 2x + y\phi$ between solutions to (8.6) and solutions from $\langle 2, \phi\rangle$ to (9.6), the solutions of the former, shown in Figure 9.3, are $(\pm\mathrm{F}_{2k-1}, \pm 2\mathrm{F}_{2k})$. As suggested in the figure, we can form these into a single bidirectional sequence. Since

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

the solutions to (8.6) are

$$\pm 2 \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

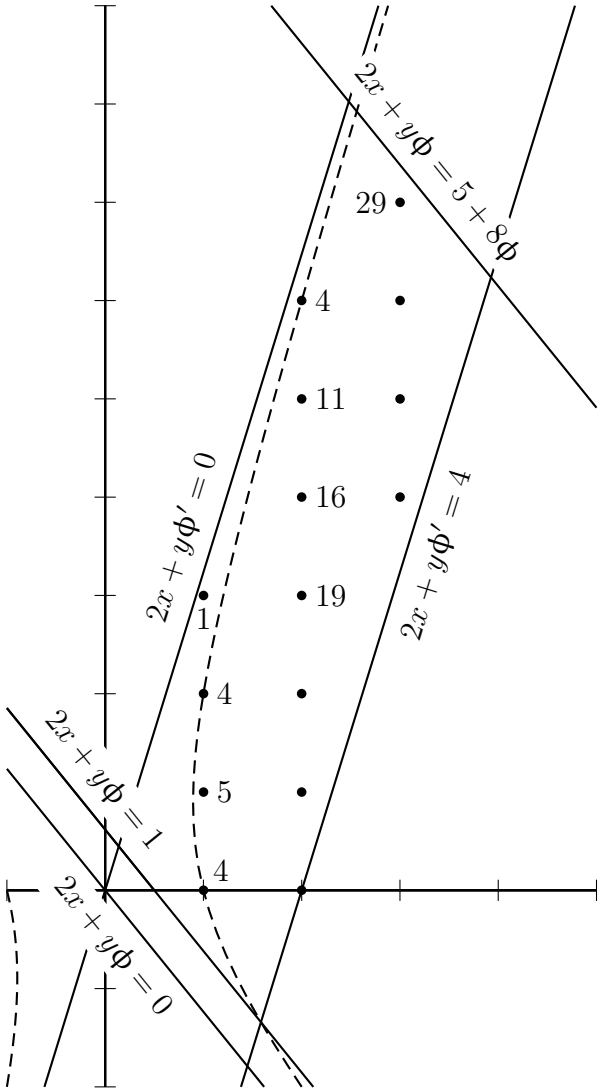

Figure 9.2: Small solutions of $4x^2 + 2xy - y^2 = 4$

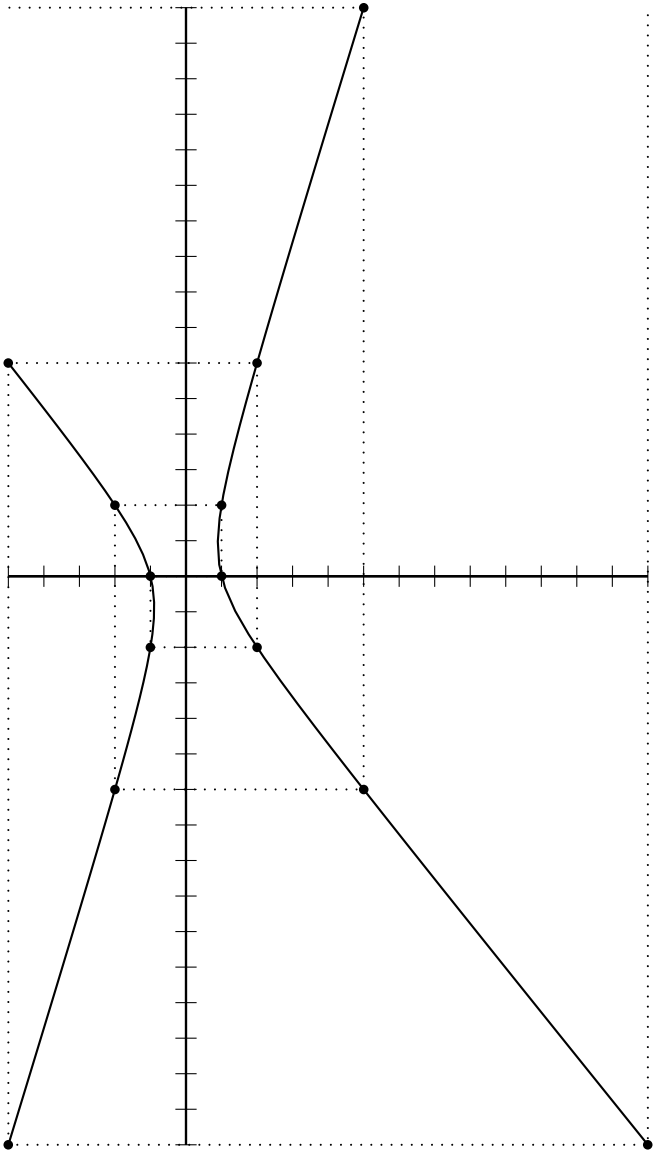

Figure 9.3: Solutions of $4x^2 + 2xy - y^2 = 4$

10 Integers

We define yet another subset of K; it will turn out to be an order that includes all others. Meanwhile, the definition is

$$\{\xi \in K\colon\ \mathrm{Tr}(\xi) \in \mathbb{Z}\ \ \&\ \ \mathrm{N}(\xi) \in \mathbb{Z}\} = \mathfrak{O}_K.$$

The elements of $\mathfrak{O}_K$ are called the **integers** of K. The elements of $\mathbb{Z}$ can henceforth be called **rational integers.**

Example 6. $\langle 1, \sqrt{d}\rangle \subseteq \mathfrak{O}_K$; but when $d = 5$, then $\phi \in \mathfrak{O}_K$.

Theorem 19. *The integers of K are precisely the solutions in K of polynomial equations*

$$x^2 + bx + c = 0,$$

where b and c are rational integers.

Proof. We need only look at (9.4) in the proof of the corollary of Theorem 17. □

Lemma 6. *For every lattice Λ of K,*

$$\mathfrak{O}_\Lambda \subseteq \mathfrak{O}_K.$$

Proof. This also follows from the proof of the corollary of Theorem 17. □

In order to characterize $\mathfrak{O}_K$ more precisely than in the definition or Theorem 19, we define

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2 \text{ or } 3 \pmod 4; \\ \dfrac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{10.1}$$

We continue to assume that d is squarefree. In either case of (10.1),

$$\langle 1, \sqrt{d} \rangle \subseteq \langle 1, \omega \rangle . \tag{10.2}$$

Theorem 20. $\mathfrak{O}_K = \langle 1, \omega \rangle$, *and this is closed under multiplication.*

Proof. Let α be an element $a + b\sqrt{d}$ of K, so that α is a zero of the polynomial

$$x^2 - 2ax + a^2 - b^2 d. \tag{10.3}$$

Suppose first $\alpha \in \mathfrak{O}_K$. Then $2a$ and $a^2 - b^2 d$ are in $\mathbb{Z}$ by Theorem 19. There are two cases.

(i) If $2a$ is even, then $a \in \mathbb{Z}$, so $b^2 d \in \mathbb{Z}$, and hence $b \in \mathbb{Z}$ since d is square-free; consequently $\alpha \in \mathbb{Z}[\sqrt{d}]$, and so $\alpha \in \langle 1, \omega \rangle$ by (10.2).

(ii) Suppose $2a$ is odd. *Modulo* 4 we have $4a^2 \equiv (2a)^2 \equiv 1$. But also $4a^2 - 4b^2 d \equiv 0$, so that $(2b)^2 d \equiv 4b^2 d \equiv 4a^2 \equiv 1$. Since $2b \in \mathbb{Z}$, again because d is square-free, we have $(2b)^2$ congruent to 0 or 1, and therefore $(2b)^2 \equiv 1$. We conclude both that $2b$ is odd and that $d \equiv 1$. Again we obtain $\alpha \in \langle 1, \omega \rangle$.

Suppose conversely $\alpha \in \langle 1, \omega \rangle$. *Modulo* 4, if d is not congruent to 1, then a and b are rational integers, so the polynomial in (10.3) is over $\mathbb{Z}$, and thus $\alpha \in \mathfrak{O}_K$. If d *is* congruent to 1,

then both $2a$ and $2b$ must be integers, and moreover $2a \equiv 2b \pmod 2$, so that

$$4(a^2 - b^2 d) \equiv (2a)^2 - (2b)^2 \equiv 0 \pmod 4,$$

and again the polynomial in (10.3) is over $\mathbb{Z}$.

Finally, in case $d \equiv 1$ *modulo* 4, so that $d = 4k+1$ for some integer k, we have

$$\omega^2 = \frac{1 + 2\sqrt{d} + d}{4} = \frac{2k + 1 + \sqrt{d}}{2} = k + \omega,$$

which is in $\mathfrak{O}_K$. □

The invertible elements of a ring are called its **units.** Then the invertible elements of $\mathfrak{O}_K$ (and therefore also of every $\mathfrak{O}_\Lambda$, by the corollary of Theorem 17) are just the elements having norm ± 1.

Bibliography

[1] Richard Dedekind. *Essays on the Theory of Numbers. I: Continuity and Irrational Numbers. II: The Nature and Meaning of Numbers*. Dover Publications, New York, 1963. Authorized 1901 translation by Wooster Woodruff Beman of "Stetigkeit und irrationale Zahlen" and "Was sind und was sollen die Zahlen" (second edition, 1893; first, 1887).

[2] René Descartes. *The Geometry of René Descartes*. Dover Publications, New York, 1954. Translated from the French and Latin by David Eugene Smith and Marcia L. Latham, with a facsimile of the first edition of 1637.

[3] David Hilbert. *The Foundations of Geometry*. Authorized translation by E. J. Townsend. Reprint edition. The Open Court Publishing Co., La Salle, Ill., 1959. Based on lectures 1898–99. Translation copyrighted 1902. Project Gutenberg edition released December 23, 2005 (`www.gutenberg.net`).

[4] Barry Mazur. How did Theaetetus prove his theorem? In P. Kalkavage and E. Salem, editors, *The Envisioned Life: Essays in honor of Eva Brann*. Paul Dry Books, 2007. `www.math.harvard.edu/~mazur/preprints/Eva.pdf`, accessed September 20, 2012.

[5] David Pengelley and Fred Richman. Did Euclid need the Euclidean algorithm to prove unique factorization? *Amer. Math. Monthly*, 113(3):196–205, 2006.

[6] David Pierce. Thales and the nine-point conic. *The De Morgan Gazette*, 8(4):27–78, 2016. education.lms.ac.uk/2016/12/thales-and-the-nine-point-conic/, accessed June 1, 2017.