

Chapter 1

Introduction

The Euclidean algorithm is the epitome of elegance in computational mathematics: it is clean and simple, much faster than factoring the inputs one by one and then casting out common factors, and requires little memory. As mathematics it shines too: there are numerous fruitful generalizations, it can be used to prove things outside its own orbit, and tools from the wide reaches of mathematics are needed to ferret out its deeper aspects. It even lends itself to striking graphics.

The algorithm goes back to antiquity and was known to Euclid. It takes as input a pair of integers, not both zero, and returns their *greatest common divisor* $\gcd[a, b]$. Many books express algorithms in pseudocode. Here we sometimes use *Mathematica* in place of pseudocode. This has the advantage of being executable on a machine.

```
EuclideanAlgorithmGCD[p_Integer,q_Integer]:=Module[{a,b},
  If[p==0,
    If[q==0,Return[Infinity]];
    Return[Abs[q]]
  ];
  a=Abs[p];b=Abs[q];
  While[a>0,{a,b}={Mod[b,a],a}];
  b]
```

This book is about that algorithm, and about the deep and intricate theory that has grown up in association with it. For all its origin in antiquity and its accessibility to schoolchildren, there is still an open research frontier. For instance, it is not known whether, for every $b \geq 2$, there exists $a < b$ so that every approximation c/d to a/b with $0 < d < b$ satisfies $|c/d - a/b| > 1/(10d^2)$, and it has only recently been established that the number of steps

needed to complete the algorithm, averaged over pairs (a, b) with $a, b \leq x$, has asymptotically a Gaussian distribution.

The greatest common divisor of two integers, not both zero, has been of interest to mathematicians for millennia. For $a, b \in \mathbb{Z}$, not both zero, $\gcd[a, b]$ is the largest integer d so that $d \mid a$ and $d \mid b$. An equivalent definition is that it is the least positive integer d in $\Lambda(a, b) := \{ja + kb : j, k \in \mathbb{Z}\}$, for if $d \mid a$ and $d \mid b$, then $d \mid ja + kb$. In the other direction, if u is the least positive element of $\Lambda(a, b)$, then u divides all the rest because otherwise, there would be an element $v \in \Lambda(a, b)$ not divisible by u . But then $v \bmod u \in \Lambda(a, b)$ and $0 < v < u$, a contradiction.

One can also speak of the gcd of a set of integers, and again, the two definitions, as the greatest integer that divides them all, and as the least positive element of the set of finite integer linear combinations of them, are equivalent.

The gcd algorithm given above (in Mathematica code) discards potentially valuable ancillary information. There are variants of the algorithm which keep and return this information. Our first variant starts with a pair $(p_0, q_0) := (p, q)$ of positive integers, sorted so that $p \leq q$, and generates a list of working pairs (p_j, q_j) of non-negative integers. It halts when $p_n = 0$. The loop generates successive pairs using the rule

$$(p_{n+1}, q_{n+1}) := (q_n \bmod p_n, p_n).$$

Equivalently,

$$\begin{aligned} a_{n+1} &:= \lfloor q_n/p_n \rfloor \\ (p_{n+1}, q_{n+1}) &:= (q_n - a_{n+1}p_n, p_n). \end{aligned}$$

It also keeps a working matrix M_j defined by $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $M_{j+1} = M_j \begin{pmatrix} 0 & 1 \\ 1 & a_{j+1} \end{pmatrix}$. The algorithm terminates when $p_n = 0$ and returns a list with five integer entries: (d, u, v, p', q') , where $d = \gcd(p, q)$, (u, v) is a pair of integers so that $qu - pv = (-1)^n d$, $0 \leq u < q$, $0 \leq v < p$, and $p' = p/d, q' = q/d$. Here, $d = p_n$ while $M_n = \begin{pmatrix} u & p' \\ v & q' \end{pmatrix}$.

The reason the algorithm returns the gcd is that with each step, $d \mid p_j$ and $d \mid q_j$ if and only if $d \mid q_j - kp_j$ and $d \mid p_j$ so that in particular $d \mid p_{j+1}$ and $d \mid q_{j+1}$ if and only if $d \mid p_j$ and $d \mid q_j$. Thus,

$$\gcd(p_{j+1}, q_{j+1}) = \gcd(p_j, q_j).$$

At the end, the working pair is $(0, q_n) = (0, d)$ which clearly has greatest common divisor d . The reason the algorithm is fast is that $p_{j+1}q_{j+1} < (1/2)p_jq_j$. (The reader will see the proof as readily by thinking about it a bit, as by reading about it.)

There are various modified versions of this algorithm which achieve slightly improved efficiency, at the price of slightly greater complexity and a certain loss of elegance. But inasmuch as the algorithm is a workhorse of computational number theory, every bit of efficiency counts. Instead of taking the remainder $a \bmod b$ to be the non-negative integer $a' \equiv a \pmod{b}$, one can take the integer, positive or negative, nearest zero and in the required congruence class. This sometimes gets us two steps for the price of one.

The *centered algorithm*, which is another way to present this same idea, proceeds by replacing a working pair (u, v) of integers satisfying $0 \leq u < v$ by the pair $(|v - nu|, u)$, where $n = \lfloor v/u \rfloor + 1/2$, until $u = 0$. It is on average faster than the classical algorithm by a factor of $\log(2)/\log(\phi)$, where $\phi = (1 + \sqrt{5})/2$.

Division of one large integer by another, to obtain the quotient and remainder, is the most time-consuming part of executing the classic Euclidean algorithm on large integer input pairs. This can be circumvented with the *binary shift* Euclidean algorithm.

Suppose we are representing our integers in binary notation, as strings of 0's and 1's. Extracting common factors of two is then trivial. The binary shift Euclidean algorithm takes up where stripping out the 0's leaves off, accepting inputs of the form (u, v) where u and v are odd positive integers with $0 < u \leq v$. The algorithm has a double loop structure. Let $\text{Val}_2(n)$ denote the largest b so that $2^b \mid n$.

The algorithm takes as input a pair (u_0, v_0) of odd positive integers with $u_0 \leq v_0$. It terminates when $u_n = v_n$, returning u_n , and if desired, performance statistics such as n . If $u_n < v_n$, the outer loop passes the current pair (u_n, v_n) to an inner loop.

The inner loop generates a list $w_{n,j}$ beginning with $w_{n,0} := v_n$ which proceeds while $w_{n,j} > u_n$ by

$$\begin{aligned} x &:= (w_{n,j} - u_n) \\ b_{n,j} &:= \text{Val}_2(x) \\ w_{n,j+1} &:= 2^{-b_{n,j}} x \end{aligned}$$

and exits when $w_{n,j} \leq u_n$, returning $(u_{n+1}, v_{n+1}) := (w_{n,j}, u_n)$ to the outer

loop.

Performance bounds are easy. Since each step of the inner loop reduces the number of bits in w by at least one, the sum of the bit-string lengths of the pair being processed decreases with each step, so that the total number of subtractions effected by the inner loop is on the order of $\log v_0$ or less. Clearly there are no more exchanges than subtractions, so the total number of steps is also $O(\log v_0)$.

A more exact analysis has recently been made by Vallée [Va2], who showed that the number of subtraction steps, averaged over all odd input pairs (u, v) with $v \leq x$, is asymptotically $A \log x$ where A is a positive constant related to a certain linear operator. She has a similar result about the number of exchanges.

There are other variations on this theme. To determine whether or not n is a quadratic residue mod p (Legendre symbol), one uses the Kronecker-Jacobi symbol $\left(\frac{a}{p}\right)$. The Kronecker algorithm (see p 29 of [Co]) has at its heart a cycle of steps of the form $(a, b) \rightarrow (b \bmod a, a)$, but with additional steps which remove powers of 2 from a and b between divisions, so that all divisions involve a pair of odd numbers. Vallée discusses averages related to this algorithm in [Va2].

1.1 The Additive Subgroup of the Integers Generated by a and b

Another way to look at what is achieved by computing the gcd of two integers is that the set of all integer linear combinations of a and b forms an additive subgroup of the integers, this subgroup has a single generator, and we find it by finding a series of pairs that generate the same subgroup, culminating in the pair $(0, d)$. At first sight, this amounts to nothing better than throwing around big words, but there is an important fact implicit in this perspective. Our output d belongs to the subgroup, so there must exist integers x and y so that $ax + by = d$. The basic Euclidean algorithm, unlike the matrix-based version, does not provide this ancillary information, but it can be readily adapted to do so. The *extended gcd* algorithm takes input (a, b) with $0 \leq a \leq b$ and returns d , x , and y .

Algorithm 1.1 Extended gcd algorithm. Inputs: Nonnegative integers a and b . Outputs: Integers x and y , and a positive integer d , so that $d = \gcd(a, b)$ and $ax + by = d$, with $|x| \leq b/d$, $|y| \leq a/d$. (If a and b are both zero, which they should not be, rather than crash the algorithm we

specify that it return ∞ for d , and $(0, 0)$ for x and y .)

Input a, b . Set $p' = 1, p = 0, q' = 0$, and $q = 1$. Set $u = a, v = b$, and $r = 0$.

While $u > 0$, set $c = \lfloor v/u \rfloor$, $(u, v) \leftarrow (v - cu, u)$, $(p', p) \leftarrow (p, cp + p')$, and $(q', q) \leftarrow (q, cq + q')$. Increment: $r \leftarrow r + 1$.

If r is even, return $(-q', p', v)$ as the values of (x, y, d) . If r is odd, return $(q', -p', v)$ as values of (x, y, d) .

Variant: Keep track of p, q , and c . Set $r = 1, p_{-1} := 1, p_0 := 0, q_{-1} := 0$ and $q_0 := 1$. Then while $u > 0$ set $a_r := \lfloor v/u \rfloor$, $p_r := a_r p_{r-1} + p_{r-2}$, and $q_r := a_r q_{r-1} + q_{r-2}$. Return the lists (a_1, \dots, a_r) , $(p_1 \dots p_r)$, and (q_1, \dots, q_r) , as well as the final value of v , which is the gcd of a and b .

Remark 1.1 *This algorithm carries over without significant modification to the case of polynomials in one variable over a field. When working over, for instance, the field \mathbb{Q} , there is a practical difficulty in that the coefficients can become so unwieldy as to obviate the formal speed and simplicity of the algorithm. In a finite field, where exact arithmetic is realizable in practice as well as in principle, the algorithm is generally simpler than with integers, mainly because all polynomials of the same degree are of the same size, in the sense that the number of congruence classes modulo such polynomials depends only on the degree and on the underlying field, see [FriHe].*

The list (p_j, q_j) of intermediate values of p and q , and the list (a_j) of values of c , give valuable information. Suppose $0 < a < b$. The fractions $p_j/q_j, 1 \leq j < r$ are especially good approximations p/q of a/b with $q \leq b$. The final p_r/q_r is the reduced value of a/b . The value of r is the number of steps needed to execute the algorithm. The identity $p_{r-1}q_r - p_rq_{r-1} = (-1)^r$, together with $p_r = a/\gcd[a, b]$ and $q_r = b/\gcd[a, b]$, give x and y so that $ax + by = d = \gcd[a, b]$.

An important special case is $d = 1$. Two randomly chosen positive integers will, more likely than not, be relatively prime. This goes back to Euler, who calculated the fraction of such pairs to be $\prod_p \text{prime} (1 - p^{-2}) = 6/\pi^2$. Now there is scant point in computing the gcd of numbers a and b if they are known to be relatively prime. But when we get x and y , we will have found $a^{-1} \pmod{b}$ (that is x), and vice-versa. This algorithm thus lies at the heart of computational number theory, for it allows us to find multiplicative inverses in finite fields of prime order. (For finite fields of order $q = p^n$, finding the multiplicative inverse of an element amounts to solving a system of n linear equations in n variables, in the ground field $\mathbb{Z}/p\mathbb{Z}$. Straight Gaussian reduction suffices.)

1.2 Continuants

The denominator q_r of the finite continued fraction

$$[\mathbf{u}] = [u_1, \dots, u_r] = [0; u_1, \dots, u_r] = \frac{1}{u_1 + \frac{1}{u_2 + \frac{1}{\ddots + 1/u_r}}}$$

is a function of the integer list $\mathbf{u} = (u_1, u_2, \dots, u_r)$. We call this number the *continuand* of \mathbf{u} and write $|(u_1, u_2, \dots, u_r)|$ or, if there is no risk of confusion, simply $|\mathbf{u}|$. The continuants satisfy a number of useful identities. By convention, the continuand of the empty list is 1. For $\mathbf{u} \in \mathbb{Z}^{+r}$, we write \mathbf{u}^- for $(u_1, u_2, \dots, u_{r-1})$ and \mathbf{u}_- for (u_2, \dots, u_r) . We write $\{\mathbf{u}\}$ for the continued fraction $[u_r, \dots, u_1]$. (When dealing with a single real number x , we use $\{x\}$ as usual to denote the fractional part of x .) For the empty list $\mathbf{z} = ()$, we declare $|\mathbf{z}| = 1$, $[\mathbf{z}] = \{\mathbf{z}\} = 0$.

Proposition 1.1 *Suppose $\mathbf{u} = (u_1, u_2, \dots, u_r)$ and $\mathbf{v} = (v_1, \dots, v_s)$ are lists of positive integers. Let \mathbf{uv} denote the concatenation $(u_1, \dots, u_r, v_1, \dots, v_s)$ of \mathbf{u} and \mathbf{v} . Then*

$$\begin{aligned} (i) \quad |\mathbf{u}| &= \begin{vmatrix} u_1 & 1 & 0 & 0 \dots \\ -1 & u_2 & 1 & 0 \dots \\ 0 & -1 & u_3 & 1 \dots \\ \vdots & & & \\ 0 & 0 & \dots & -1 & u_r \end{vmatrix} = q_r, \\ (ii) \quad |\mathbf{uv}| &= |\mathbf{u}||\mathbf{v}| + |\mathbf{u}^-||\mathbf{v}_-| = |\mathbf{u}||\mathbf{v}|(1 + \{\mathbf{u}\}[\mathbf{v}]), \\ (iii) \quad p_r &= |\mathbf{u}_-| = [\mathbf{u}||\mathbf{u}|, \\ (iv) \quad q_{r-1} &= |\mathbf{u}^-| = \{\mathbf{u}\}|\mathbf{u}|, \\ (v) \quad |u_1, u_2, \dots, u_r| &= |u_r, u_{r-1}, \dots, u_1|. \end{aligned}$$

The proof is by induction. The identity $q_{j+1} = u_{j+1}q_j + q_{j-1}$ determines the successive denominators, together with $q_0 := 1$ and $q_{-1} := 0$. Clearly, the determinant obeys this same recursion, and agrees with q_r for $r = 1$ and $r = 2$. Item (ii) is an immediate consequence of (i) and basic properties of determinants. Item (iii) is a consequence of the construction of p_r , which is governed by the same recursion as for q_r but beginning with u_2 . Items (iv) and (v) are an immediate consequence of (i).

1.3 The Continued Fraction Expansion of a Real Number

The gcd algorithm is closely related to the continued fraction expansion of a real number. Given a rational number $\alpha = a/b$ with $0 < a < b$, if c_1, c_2, \dots, c_r are the partial quotients in the continued fraction expansion of a/b , then $a/b = [(c_1, c_2, \dots, c_r)] = 1/(c_1 + 1/(c_2 + 1/(c_3 + \dots + 1/c_r)))$ is exactly $p_r/q_r = a/b$. Truncating the expansion at some earlier value $r' < r$ gives $p_{r'}/q_{r'}$, a rational approximation of a/b by a simpler rational number.

For general real numbers α , a relentlessly constructivist approach would be to insist that since we know real numbers by their rational approximations, we should ask for the continued fraction expansion of a rational interval, and then take limits. This is actually not such a bad idea, for it forces us to consider something we should eventually have to think through in any case: what is the quality of the approximations $p_r/q_r = 1/(c_1 + 1/(c_2 + \dots + 1/c_r))$ as we go along? But this author is not a relentless constructivist. Here is the conventional continued fraction expansion algorithm for a real number:

Algorithm 1.2 (Continued fraction expansion of a real number α .) Input α , and a limit R to your patience. Set $p_{-1} = 1$, $p_0 = \lfloor \alpha \rfloor$, $q_{-1} = 0$, and $q_0 = 1$. Set $a_0 = \lfloor \alpha \rfloor$, and set $\alpha_0 = \alpha - a_0$ so that $0 \leq \alpha_0 < 1$. Set $r = 0$. While $\alpha_r > 0$ and $r \leq R$, set $\beta = 1/\alpha_r$, $a_{r+1} = \lfloor \beta \rfloor$, and $\alpha_{r+1} = \beta - a_{r+1}$. Set $p_{r+1} := a_{r+1}p_r + p_{r-1}$ and $q_{r+1} = a_{r+1}q_r + q_{r-1}$. Increment r . Return the lists $(a_0, a_1, a_2, \dots, a_R)$, $(p_0, p_1, p_2, \dots, p_R)$, and $(q_0, q_1, q_2, \dots, q_R)$.

Remark 1.2 *The list $(a_0, a_1, a_2, \dots, a_r)$ gives the continued fraction expansion of α to depth r : $\alpha = a_0 + 1/(a_1 + 1/(a_2 + 1/(a_3 + 1/(a_4 + \dots))))$. The integers p_r and q_r are the numerators and denominators respectively of the rational numbers $a_0 + 1/(a_1 + 1/(a_2 + 1/(a_3 + \dots + 1/a_r)))$. Both this algorithm, and most of the associated results below, carry over without significant modification to the case of power series with coefficients over \mathbb{Q} or over a finite field, on taking the stance that higher powers of z are ‘smaller’.*

Theorem 1.1 *The integers a_r , p_r , and q_r for the continued fraction expansion of a rational number $\alpha = a/b$ are the same as the corresponding numbers generated by the gcd algorithm given input (a, b) . For both rational*

and irrational α , and for all relevant r ,

- (i) $p_{2r}/q_{2r} < \alpha < p_{2r+1}/q_{2r+1}$,
- (ii) $\alpha = \frac{p_r + \alpha_r p_{r-1}}{q_r + \alpha_r q_{r-1}}$,
- (iii) $\alpha_r = [a_{r+1}, a_{r+2}, \dots]$,
- (iv) $\frac{1}{(2 + a_{r+1})q_r^2} < \left| \alpha - \frac{p_r}{q_r} \right| < \frac{1}{a_{r+1}q_r^2}$,
- (v) $0 \leq \alpha_r < 1$.

The proofs are straightforward induction. The estimate for $|\alpha - p/q|$ can be given a sharper constant. Hurwitz [Sc1] proved in 1891 that for every irrational number α there are infinitely many distinct rationals p/q with $|\alpha - p/q| < 1/(\sqrt{5}q^2)$. The constant $\sqrt{5}$ is best possible; any real number with arbitrarily long strings of consecutive $a_r = 1$ in its continued fraction expansion provides a counterexample to the form the result would take with a smaller constant in place of $1/\sqrt{5}$.

1.4 Quadratic Irrationals

There is a nice analogy: Terminating binary decimal expansions \leftrightarrow dyadic rationals, periodic binary expansions \leftrightarrow rational numbers: terminating continued fraction expansion \leftrightarrow rational number, periodic continued fraction expansion \leftrightarrow quadratic irrational.

Theorem 1.2 *Given an eventually periodic (infinite) continued fraction*

$$u_0 + [\mathbf{u}\bar{\mathbf{v}}] = u_0 + [\mathbf{u}\mathbf{v}\mathbf{v} \dots] = [u_0; u_1, u_2, \dots, u_s, v_1, \dots, v_t, v_1, \dots, v_t, \dots]$$

the corresponding real number $\alpha = \alpha(\mathbf{u}, \mathbf{v})$ is a quadratic irrational $\alpha = a + b\sqrt{d}$ where a and b are rational and d is square-free, and conversely.

Proof. Let $\alpha = u_0 + [\mathbf{u}\bar{\mathbf{v}}]$. Since every rational number has a terminating continued fraction expansion, α is irrational. Now $\alpha = u_0 + [\mathbf{u} + \beta]$ where $\beta = [\mathbf{v} + \beta]$. From theorem 1.1,

$$\beta = (p_t + \beta p_{t-1}) / (q_t + \beta q_{t-1})$$

so that

$$q_{t-1}\beta^2 + (q_t - p_{t-1})\beta - p_t = 0.$$

Thus β is a quadratic irrational and hence α is as well. In the other direction, suppose α is a quadratic irrational, with $\alpha = \theta + \phi\sqrt{w}$, θ and ϕ rational and w a non-square positive integer, and $0 < \alpha < 1$. We leave as an exercise for the reader, to put α first in the form $(s \pm \sqrt{t})/r$ with integer s, t and $r \neq 0$, and then in the form $\alpha = (a \pm \sqrt{d})/b$ with integers a, b and d , $d > 0$, $b > 0$, and $b \mid (d - a^2)$.

Consider first the case in which $x = (\sqrt{d} + a)/b$ with $b > 0$, $b \mid (a^2 - d)$, $d > a^2$ and $0 < x < 1$. A single step

$$x \rightarrow \{1/x\} = 1/x - \lfloor 1/x \rfloor = 1/x - k$$

takes x to $x' = (\sqrt{d} + (-a - kb'))/b'$ where $b' = (d - a^2)/b > 0$. Let $a' = -a - kb'$. Then $0 < x' < 1$ so

$$\sqrt{d} + a' > 0, \quad a' > -\sqrt{d}.$$

On the other hand, $-a < \sqrt{d}$ so $-a - kb' < \sqrt{d}$ so $|a'| < \sqrt{d}$, and trivially $b' \mid (d - a'^2)$. Thus all subsequent iterates of $x \rightarrow \{1/x\}$ will again be of this form. Since there are only finitely many pairs (a, b) of integers with $a^2 < d$ and $b \mid (d - a^2)$, some value of $x = (\sqrt{d} - a)/b$ must eventually repeat, and thereafter, the continued fraction expansion of x will be periodic.

This proof has the advantage that it gives an upper bound to the length of the period, and to the size of the integers $a_j := \lfloor 1/x_j \rfloor$ that occur in the periodic part of the expansion, in terms of d alone.

Next, consider the case $(x = a \pm \sqrt{d})/b$, with $a^2 > d$ but as before with $0 < x < 1$, $b > 0$, and $b \mid (a^2 - d)$. This time, $b' = (a^2 - d)/b$ and $a' = a - kb'$ where $k = \lfloor 1/x \rfloor$, so that $x' = (a' \pm \sqrt{d})/b'$. Since $a' < a$, there can be but finitely many consecutive steps $x \rightarrow \{1/x\}$ of this type, and after that, we are in the first case, in which the number of steps needed to finish is bounded by $O(d)$ [this could be sharpened but we have other fish to fry]. Therefore, the expansion must go into a loop. \square

Proposition 1.2 *The purely periodic expansions are those in which the loop begins immediately. That is, if x_0 is the quadratic irrational to be expanded, and $x_{j+1} := \{1/x_j\}$, $a_{j+1} := \lfloor 1/x_j \rfloor$, then $a_{j+p} = a_j$ and $x_{j+p} = x_j$ for all $j \geq 0$. The expansion of x is purely periodic if and only if the algebraic conjugate $\bar{x} = (a \mp \sqrt{d})/b$ of $x = (a \pm \sqrt{d})/b$ with $0 < x < 1$ satisfies $\bar{x} < -1$.*

Proof. If x satisfies the conditions, then $x_{j+1} = 1/x_j - a_{j+1}$ so that $\overline{x_{j+1}} = 1/\overline{x_j} - a_{j+1}$. Inductively, then, x_j satisfies the same conditions. Now because x_0 is a quadratic irrational, the sequence (x_j) is at any rate

eventually periodic. But if $x_j = x_{j+p}$ for some p , then $\overline{x_j} = \overline{x_{j+p}}$. But $\overline{x_j} < -1$ and $\overline{x_j} = 1/\overline{x_{j-1}} - a_j$ and likewise $\overline{x_{j+p}} = 1/\overline{x_{j+p-1}} - a_{j+p}$. On the other hand, since $\overline{x_{j-1}} < -1$, $-1 < 1/\overline{x_{j-1}} < 0$ so that $a_j = \lfloor -\overline{x_j} \rfloor$ and $a_{j+p} = \lfloor -\overline{x_{j+p}} \rfloor$. Thus $a_j = a_{j+p}$ and so $\overline{x_{j-1}} = \overline{x_{j-1+p}}$ so $x_{j-1} = x_{j-1+p}$. From this it follows that $x_{j+p} = x_j$ for all $j \geq 0$ as claimed.

In the other direction, if x has a purely periodic expansion, then $x = [a_1, a_2, \dots, a_{r-1}, a_r + x]$ for some $r \geq 1$ and some list of r positive integers. Thus $x = (p_r + xp_{r-1})/(q_r + xq_{r-1})$. Consequently,

$$x = \frac{(p_{r-1} - q_r) \pm \sqrt{q_r^2 - 2q_r p_{r-1} + 4q_{r-1} p_r + p_{r-1}^2}}{2q_{r-1}}$$

and since $-2q_r p_{r-1} + 4q_{r-1} p_r = 2q_r p_{r-1} + 4(-1)^{r-1}$,

$$x = \frac{(p_{r-1} - q_r) \pm \sqrt{(q_r + p_{r-1})^2 + 4(-1)^{r-1}}}{2q_{r-1}}$$

The $+$ in \pm gives x , which we already know to lie between 0 and 1, while the $-$ in \pm gives the conjugate. But with this minus sign, for $r \geq 2$ at any rate, $(p_{r-1} + q_r)^2 - 4 > (p_{r-1} + q_r - 1)^2$ and so the conjugate satisfies $\overline{x} < -(q_r - 1)/q_{r-1} \leq -1$ as required. If the base period of the continued fraction is one, one nevertheless has $x = [a_1, a_1 + x]$ so the argument still works. \square

1.4.1 Pell's equation

We can use this to solve Pell's equation, $X^2 - DY^2 = 1$. This is linked to the continued fraction expansion of \sqrt{D} . The numerators and denominators p_n and q_n in the continued fraction convergents p_n/q_n to \sqrt{D} serve as reasonable candidates for integers x and y , and it turns out that one need only extract this expansion to the depth of a full-period.

The continued fraction expansion of $n + \sqrt{D}$, where $n = \lfloor \sqrt{D} \rfloor$, is purely periodic. That is,

$$n + \sqrt{D} = 2n + 1 / (a_1 + 1 / (a_2 + \dots + 1 / (a_r + 1 / (2n + 1 / (a_1 + 1 / (a_2 + \dots))))))$$

so that if $\xi := n + \sqrt{D}$ and (x_r/y_r) is the r th convergent to $\sqrt{D} - n$ then

$$\xi = 2n + \frac{x_r + \xi^{-1} x_{r-1}}{y_r + \xi^{-1} y_{r-1}}.$$

From this it follows that

$$\sqrt{D} - (n + x_r/y_r) = (\sqrt{D} - n) - x_r/y_r = \frac{(-1)^r}{\xi y_r + y_{r-1}}$$

Thus

$$|(x_r + ny_r)^2 - Dy_r^2| < \frac{(x_r + ny_r) + \sqrt{D}y_r}{(n + \sqrt{D})y_r} < 2,$$

this last because $x_r < y_r$. Thus taking $X := x_r + ny_r$ and $Y = y_r$ gives the fundamental solution to $X^2 - Dy^2 = \pm 1$.

For instance, to solve $x^2 - 76y^2 = \pm 1$ in integers, one calculates the continued fraction expansion of $\sqrt{76}$. In these calculations there is no need of decimal approximations, and we can proceed with exact calculations. Thus,

$$\sqrt{76} = 8 + (\sqrt{76} - 8) = 8 + 1/((\sqrt{76} + 8)/12)$$

Continuing in this vein, we obtain a series of identities of the form $\sqrt{76} = a_0 + 1/(a_1 + 1/(a_2 + \dots + 1/(\sqrt{76} + u_r)/v_r) \dots)$ where $q_r \mid (76 - u_r^2)$, $v_r > 0$, $0 < u_r < \sqrt{76}$, and where $p_r^2 - 76q_r^2 = (-1)^r v_r$. The continued fraction expansion is periodic, (and would be purely periodic if we started with $8 + \sqrt{76}$), and one eventually reaches $u_r = \lfloor \sqrt{76} \rfloor$, $v_r = 1$ which gives the fundamental unit. As it happens, the continued fraction expansion is that $\sqrt{76} = 8 + [1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16, \dots]$. The sequence is purely periodic, and the numerator and denominator 57799 and 6630 respectively of $[1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1]$ give the fundamental units $57799 \pm 6630\sqrt{76}$.

What we have done here is not the last word in computing solutions to the Pell equation, though. For large D , the approach taken here requires too many steps. There are better ways. For further information, see [Vardi].

1.4.2 Linear recurrence relations

The continued fraction algorithm uses the recurrence relations $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$ to generate the numerator and denominator sequences (p_n) and (q_n) for the convergents to a real number α . In the special case that the sequence (a_n) of partial quotients for α is constant, this provides, forthwith, a second order linear recurrence with constant coefficients for the corresponding (p_n) and (q_n) . If the (a_n) vary, then there is no such second order linear recurrence. But this does not foreclose the

possibility of a higher order linear recurrence with constant coefficients governing (p_n) and (q_n) . A recent result of Lenstra and Shallit [LeSh] provides a nice counterpart to our other characterization of quadratic irrationals, as numbers with an ultimately periodic continued fraction expansion. A linear recurrence with constant complex coefficients, for a sequence (z_n) , is a recurrence of the form $z_n = \sum_{k=1}^N \lambda_k z_{n-k}$, with fixed complex numbers $\lambda_k, 1 \leq k \leq N$, that holds for $n > N$.

Theorem 1.3 *Let α be an irrational number, with continued fraction expansion $\alpha = [a_0; a_1, a_2, \dots]$. Let (p_n) and (q_n) be the numerator and denominator sequences of the convergents to α . If either (p_n) or (q_n) satisfy a linear recurrence with constant complex coefficients, then α is a quadratic irrational, and conversely, if α is a quadratic irrational, then both (p_n) and (q_n) satisfy a linear recurrence with constant complex coefficients.*

It may come as a bit of a surprise that this was not known since classical times, but the only known proof requires a difficult result of van der Poorten, known as the Hadamard Quotient Theorem. [vdP2; vdP3].

1.5 The Tree of Continued Fraction Expansions

The continued fraction expansion of a real number is a path along a tree. At each step, the tree branches countably many ways, with one branch for each positive integer. The vertices of this rooted tree are the finite lists of positive integers $[a_1, a_2, \dots, a_r]$, of whatever length, and the edges go from each vertex (list) to each list got by appending a single positive integer to the original list. The root of this tree is the empty list. The set $I_{\mathbf{a}} = I_{(a_1, a_2, \dots, a_r)}$ of all real numbers $\alpha, 0 \leq \alpha < 1$ such that the continued fraction expansion begins with the list $\mathbf{a} = \langle a_1, a_2, \dots, a_r \rangle$ is an interval with endpoints $p_r/q_r = [\mathbf{a}]$ and $(p_r + p_{r-1})/(q_r + q_{r-1}) = [\mathbf{a}, 1]$, closed at the former end and open at the latter. If r is odd, the open end of the interval is its lower end and $I_{\mathbf{a}}$ has the form $(x, y]$, while if r is even, the interval $I_{\mathbf{a}}$ has the form $[x, y)$. The length of $I_{\mathbf{a}}$ is $1/(q_r(q_r + q_{r-1})) = 1/|\mathbf{a}|^2(1 + \{\mathbf{a}\})$.

Every interval $(p/q, p'/q')$ of length $1/qq'$ occurs as the interior of $I_{\mathbf{a}}$ for a unique list \mathbf{a} of positive integers; $[0, 1)$ is the interval corresponding to the empty list.

The union of all the intervals corresponding to lists of length r is the whole interval $[0, 1)$, and for any r and any list $\mathbf{a} = \langle a_1, a_2, \dots, a_r \rangle$, the

set of extensions of this list to arbitrary fixed depth generate a partition of the interval $I_{\mathbf{a}}$. If α is rational, the number α will appear as p_r/q_r for some r ; as we have already observed, in this case generating the continued fraction expansion of α , and finding the gcd of the pair of integers whose ratio is α together with the auxiliary information, are essentially identical computations. The expansion terminates when this fraction is reached, which will also be when $\alpha_r = 0$.

For irrational α , the expansion is infinite, and there is then a one-to-one correspondence between paths to infinity in the tree (that is, infinite sequences of positive integers), and irrational numbers.

1.6 Diophantine Approximation

Diophantine approximation takes for its subject the approximation of real numbers or vectors by rational numbers or vectors. The particular case of real numbers (dimension 1) is particularly well understood because of its connection to continued fractions.

Given an irrational number α , and given a positive integer Q , the list

$$(x_1, x_2, \dots, x_Q) := (\alpha \bmod 1, 2\alpha \bmod 1, \dots, Q\alpha \bmod 1)$$

has an element nearest zero mod 1. (That is, the distance $\|r\alpha\|$ from the fractional part of one of these numbers $r\alpha \bmod 1$, to 0 or 1 whichever is closer, is minimal among the numbers in the list.) Consider the sequence of successive minima of $\|r\alpha\|$. This sequence, it turns out, is just another facet of the continued fraction expansion of α . [L]. The *discrepancy* of the list ($n\alpha \bmod 1$, $1 \leq n \leq N$) is also essentially governed by the continued fraction expansion of α . Discrepancy is a measure of how unevenly the list is distributed in the unit interval, but we defer further discussion until the necessary background is in place.

Proposition 1.3 *For all positive integers Q , there exists integer q , $1 \leq q \leq Q$ so that $\|q\alpha\| < 1/Q$.*

Proof. The sequence $q\alpha$, $0 \leq q \leq Q$ has $Q+1$ elements. Some two entries, say $q_1\alpha$ and $q_2\alpha$, must fall within the same interval $[k/Q, (k+1)/Q) \bmod 1$, and these two will differ by strictly less than $1/Q$. Take $q = |q_1 - q_2|$. \square

Remark 1.3 *If $\alpha = a/b$ is rational, and if $Q \geq b$, the result reduces to the trivial observation that $\|b(a/b)\| = 0$.*

From theorem 1.1(iv), it follows that the continued fraction convergents p_r/q_r furnish approximations to α that satisfy $\|q_r\alpha\| < 1/q_r$, and that the ratio by which q_r undercuts this bound, is effectively given by a_{r+1} . It can happen that fractions of the form $(ap_r + p_{r-1})/(aq_r + q_{r-1})$, with $1 \leq a < a_{r+1}$, also slip under the wire. That is, in certain cases, there do exist positive integers a and r , with $1 \leq a < a_{r+1}$ so that $\|(aq_r + q_{r-1})\alpha\| < 1/(aq_r + q_{r-1})$. In any event, for these a , as a consequence of our upcoming Theorem 1.4,

$$\|q_{r+1}\alpha\| < \|(aq_r + q_{r-1})\alpha\| < \|q_{r-1}\alpha\|.$$

Furthermore, we have at least this result to the effect that good approximations come only from convergents:

Proposition 1.4 *Let $\alpha \in (0, 1/2)$ be a real number, and p and q be positive integers. Let $(0/1, p_1/q_1, p_2/q_2, \dots)$ be the convergents of α . If $q > q_1$ and $|\alpha - p/q| \leq 1/(2q^2)$, then p/q is a continued-fraction convergent of α .*

Proof. Assume p/q is not a convergent, yet $|\alpha - p/q| \leq 1/(2q^2)$. Choose $j \geq 2$ such that $q_{j-1} < q < q_j$. Since $q > q_1$, we can do this. Consider the open interval A with endpoints p_{j-1}/q_{j-1} and p_{j-2}/q_{j-2} . We must have $p/q \in A$, because otherwise either $|p/q - \alpha| > |p_{j-1}/q_{j-1} - p/q|$ or $|p/q - \alpha| > |p/q - p_{j-2}/q_{j-2}|$, and in either case, the latter difference is at least $1/qq_{j-1}$ and thus more than $1/2q^2$.

Thus, (p, q) can be written as

$$(p, q) = c(p_{j-1}, q_{j-1}) + d(p_{j-2}, q_{j-2})$$

with integers $c, d > 0$. Now there is a positive integer n such that

$$(p_j, q_j) = n(p_j - 1, q_{j-1}) + (p_{j-2}, q_{j-2}),$$

and $\theta \in (0, 1)$ such that

$$\alpha = \frac{(n + \theta)p_{j-1} + p_{j-2}}{(n + \theta)q_{j-1} + q_{j-2}}.$$

Since $q < q_j$, $c < n$ so $n \geq 2$. Now

$$\left| \frac{(n + \theta)p_{j-1} + p_{j-2}}{(n + \theta)q_{j-1} + q_{j-2}} - \frac{cp_{j-1} + dp_{j-2}}{cq_{j-1} + dq_{j-2}} \right| = \frac{(n + \theta)d - c}{q((n + \theta)q_{j-1} + q_{j-2})}.$$

This exceeds $1/2q^2$ because on expanding and clearing fractions, the claim amounts to $2(cq_{j-1} + dq_{j-2})((n + \theta)d - c) > (n + \theta)q_{j-1} + q_{j-2}$. The worst

case is $d = 1$, but even then, the coefficients for both q_{j-1} and q_{j-2} are greater on the left hand side than on the right, in view of $1 \leq c \leq n - 1$ and $0 < \theta < 1$. \square

Now let $\rho_j := q_j\alpha - p_j$, with $\rho_{-1} := -1$ and $\rho_0 := \alpha$, be the signed distance from $q_j\alpha$ to the nearest integer. Note that the distances to the nearest integer, though not the sign, are identical for α and $1 - \alpha$.

Theorem 1.4 For $0 < \alpha < 1/2$ and $j \geq 1$,

- (i) $\|q_j\alpha\| = (-1)^j \rho_j$,
- (ii) If $1 \leq q < q_j$ then $\|q\alpha\| > |\rho_j|$,
- (iii) $\rho_j = a_j \rho_{j-1} + \rho_{j-2}$,
- (iv) $\rho_j = -\frac{\alpha_j}{q_j + \alpha_j q_{j-1}}$,
- (v) $\frac{1}{3(a_{j+1}q_j)} < |\rho_j| < \frac{1}{a_{j+1}q_j}$,
- (vi) $a_j = \lfloor |\rho_{j-1}/\rho_{j-2}| \rfloor$,
- (vii) For $1 \leq k < a_j$, $|k\rho_{j-1} + \rho_{j-2}| > |\rho_{j-1}|$.

Note: Taken together, (i) and (ii) say that the nearest approaches to 0 mod 1 in the sequence $\langle q\alpha \rangle$ are alternately from the right and the left, and that the sequence of integers q_j at which successive minima of the unsigned distance occur, is the same sequence as that generated by the continued fraction algorithm.

Proof. We begin with (iii). The recurrence follows from the fact that $\langle p_j \rangle$ and $\langle q_j \rangle$ obey that recurrence, and ρ_j is a linear combination of these. Now (vi) follows from (iii), and (vii) from (vi).

For (ii), we have a calculation beginning with

$$\alpha = \frac{p_j + \alpha_j p_{j-1}}{q_j + \alpha_j q_{j-1}}.$$

Thus $(q_j + \alpha_j q_{j-1})\alpha = (p_j + \alpha_j p_{j-1})$, so $(q_j\alpha - p_j) = -\alpha_j(q_{j-1}\alpha - p_{j-1})$ as required.

Part (iv) holds by induction. For $j = 1$, $q_1 = a_1$, $q_0 = 1$, $\rho_1 = a_1\alpha - 1$, and $\alpha_1 = 1/\alpha - a_1$ so that

$$\frac{(-1)\alpha_1}{q_1 + \alpha_1 q_0} = \frac{(-1)(1/\alpha - a_1)}{a_1 + (a/\alpha - a_0)} = a_1\alpha - 1$$

as required. Now suppose the inductive hypothesis holds for $j - 1$. Then

$$\rho_j = -\alpha_j \rho_{j-1} = \frac{-\alpha_j (-1)^{j-1} \alpha_{j-1}}{q_{j-1} + \alpha_{j-1} q_{j-2}}$$

and we must show that this is equal to $(-1)^j \alpha_j / (q_j + \alpha_j q_{j-1})$. Equivalently, we need to show that $\alpha_j = (q_{j-1} + \alpha_{j-1} q_{j-2}) / (q_j + \alpha_j q_{j-1})$. But

$$\begin{aligned} q_j + \alpha_j q_{j-1} &= (a_j q_{j-1} + q_{j-2}) + \alpha_j q_{j-1} = \\ &= q_{j-1} / \alpha_{j-1} + q_{j-2} = \frac{q_{j-1} + \alpha_{j-1} q_{j-2}}{\alpha_{j-1}} \end{aligned}$$

as needed.

The inequalities, parts (i) and (v) here, are as usual the more difficult parts. An heuristic argument for (i) both lends plausibility to the conclusion, and motivates the proof. The plausibility argument begins with the observation that since $\|q_j \alpha\|$ is small, $nq_j \alpha \pmod{1} = n\rho_j$ for n small. Thus, the sequence $(nq_j \alpha \pmod{1})$ marches across the unit interval in steps of directed magnitude ρ_j , heading for the opposite end. That value of n so that $- \rho_{j-1} \pmod{1}$ lies between $n\rho_j$ and $(n+1)\rho_j$ provides the first n so that $\|(nq_j + q_{j-1})\alpha\| \|n\rho_j + \rho_{j-1}\| < |\rho_j|$. A little calculation shows that $n = a_{j+1} = \lfloor 1/\alpha_j \rfloor$. But while it is clear that this affords *one* way to find values of q for which $\|q\alpha\| < |\rho_j|$, we have as yet no guarantee that no smaller choice of q works.

Suppose, then, for purposes of deriving a contradiction, that such a q exists. Let q' be the least integer between q_j and q_{j+1} so that $\|q'\alpha\| < |\rho_j|$. Let p' be the integer nearest $q'\alpha$. If $q'\alpha - p'$ and $q_j \alpha - p_j$ have the same sign, then $|(q_j - q')\alpha - (p_j - p')| < |\rho_j|$, a contradiction. If, on the other hand, $q'\alpha - p'$ and $q_j \alpha - p_j$ have opposite signs, then $q_{j-1}\alpha - p_{j-1}$ and $q'\alpha - p'$ have the same sign, with $|q'\alpha - p'| < |q_{j-1}\alpha - p_{j-1}|$. Thus (q', p') lies in the positive cone of the vectors (q_{j-1}, p_{j-1}) and $(1, \alpha)$ and so it is a positive integer combination of (q_{j-1}, p_{j-1}) and (q_j, p_j) . But for $n < a_{j+1}$, $\|(nq_j + q_{j-1})\alpha\| > |\rho_j|$ which eliminates the most promising candidate linear combinations. What of the less promising ones?

If $1 \leq n < a_{j+1}$ and $m > 1$, then

$$(nq_j + mq_{j-1}, np_j + mp_{j-1}) = (nq_j + q_{j-1}, np_j + p_{j-1}) + (m-1)(q_{j-1}, p_{j-1}).$$

Since both vectors lie on the same side of the ray $t(1, \alpha)$, $t \geq 0$, the vertical distance from $n(q_j, p_j) + m(q_{j-1}, p_{j-1})$ to the ray $t(1, \alpha)$ is $\|(nq_j + mq_{j-1})\alpha\|$, and it is greater than the vertical height of the parallelogram with vertices

0, (q_j, p_j) , (q_{j-1}, p_{j-1}) and $(q_j, p_j) + (q_{j-1}, p_{j-1})$ which is $1/q_{j-1} > |\rho_{j-1}|$. Thus, $\|(nq_j + q_{j-1})\alpha\| > \|q_{j-1}\alpha\| = |\rho_{j-1}|$, a contradiction. This proves (i). Finally for the inequality (v), we first note that

$$|\rho_j| = \frac{\alpha_j}{q_j + \alpha_j q_{j-1}} = \frac{1}{q_j/\alpha_j + q_{j-1}}$$

Now $a_{j+1} \leq 1/\alpha_j$ so

$$|\rho_j| < \frac{1}{a_{j+1}q_j + q_{j-1}} < \frac{1}{a_{j+1}q_j}$$

In the other direction, we need $q_j/\alpha_j + q_{j-1} < 3a_{j+1}q_j$. But $q_{j-1} < q_j$, so $q_j/\alpha_j + q_{j-1} < (1 + 1/\alpha_j)q_j$. Thus it will suffice that $1/\alpha_j < 2a_{j+1}$. But $1/2 < \alpha_j a_{j+1}$ because $1/2 < \alpha_j(1/\alpha_j - \{1/\alpha_j\})$ where $\{u\}$ (in this context) denotes the fractional part of u . \square

There is a remarkable recent elementary result due to F.E. Su [Su] concerning the distribution of $\{n\alpha : 1 \leq n \leq q_k\} \bmod 1$, where (p_k/q_k) are the successive convergents to an irrational α . The result is simplest in the case where the fractional part of α is less than $1/2$, so we make that assumption.

As we have seen in Theorem 1.4, the successive minima of $\|q\alpha\|$, $q \geq 1$ occur at $q = q_j$, $j \geq 0$ and are given by $\|q_j\alpha\| = |\rho_j|$. Su's result begins with the notion of dividing the open unit interval $(0, 1)$ into countably many half-open intervals, or *bins* B_j , $j \geq 0$, with $B_j := [|\rho_j|, |\rho_{j-1}|)$. Next, Su asks: how do the numbers $q\alpha \bmod 1$ distribute themselves into these bins for $1 \leq q \leq q_j$? Following his notation, we let $N_\alpha(m, n)$ denote the number of q with $1 \leq q \leq m$ so that $q\alpha \bmod 1 \in B_\alpha(n)$.

Consider the illustrative example $\alpha = \sqrt{2}$. All partial quotients a_j are 2. By convention, $q_{-1} = 0$ and $q_0 = 1$. The next few q_j are 2, 5, 12, 29 and 70, while the first few ρ_j are a conventional $\rho_0 = -1$ followed by $\rho_1 = \sqrt{2} - 1$, $\rho_2 = 2\sqrt{2} - 3$, $\rho_3 = 5\sqrt{2} - 7$ and $\rho_4 = 12\sqrt{2} - 17$, so that the bins are

$$\dots (17 - 12\sqrt{2}, 5\sqrt{2} - 7], (5\sqrt{2} - 7, 3 - 2\sqrt{2}], (3 - 2\sqrt{2}, \sqrt{2} - 1], (\sqrt{2} - 1, 1]$$

The numbers $k\sqrt{2} \bmod 1$, $1 \leq k \leq 12$ fall into bins 0, 1, 1, 1, 2, 0, 2, 1, 1, 2, 0, and 3 respectively. One number fell into bin 3, three into bin 2, five into bin 1, and three into bin 0. Thus for $q = 12 = q_3$ the answer to Su's question can be given as a list

$$(\dots 0, \dots 0, 1, 3, 5, 3)$$

We form a similar list for each q_j and arrive at a table of which the preceding calculation forms the basis for the entries in the fourth row.

								q_j
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	1	2
0	0	0	0	0	1	3	1	5
0	0	0	0	0	1	3	5	3
0	0	0	0	0	1	3	5	15
0	0	0	0	0	1	3	5	33
0	0	0	0	1	3	5	15	33
0	0	0	0	1	3	5	15	83
0	0	0	1	3	5	15	33	83
0	0	0	1	3	5	15	33	197
0	0	0	1	3	5	15	33	479

Inspection reveals an apparent recurrence relation and Su proves it. The details of the result are these: Put a conventional row for q_{-1} on top, with a single nonzero entry: $N_\alpha(q_{-1}, 0) := -1$. Observe that $N_\alpha(q_0, 0) = 1$ while $N_\alpha(q_j, k) = 0$ if $k > j$ and $N_\alpha(q_j, j) = 1$ for $j \geq 1$. The recurrence relation applies to the non-trivial entries in the table. Column zero (the rightmost column as we have displayed it) lists the number of $q \leq q_j$ for which $\|q\alpha\|$ falls in bin 0, the interval $[\alpha, 1)$. It is governed by the recurrence

$$N_\alpha(q_{j+1}, 0) = a_{j+1}(N_\alpha(q_j, 0) + ((-1) + (-1)^j)/2) + N_\alpha(q_{j-1}, 0)$$

while for $k \geq 1$, the recurrence relation is

$$N_\alpha(q_{j+1}, k) = a_{j+1}(N_\alpha(q_j, k) + (-1)^{j-k}) + N_\alpha(q_{j-1}, k).$$

Although this result is of interest in its own right, Su had an application in mind. A *random walk* on the circle starts somewhere and moves clockwise or counterclockwise, each with probability $1/2$, by an angle $2\pi\alpha$. If α is rational, the walk is a discrete walk and the distribution of frequencies with which the walk is in any one state converges to $1/N$ where N is the denominator of α . But if α is irrational, the walk has a dense orbit with probability one, and the appropriate measure of the extent to which the distribution after r moves differs from uniform, is the *discrepancy* of the sequence. (See section 3.3) If α is badly approximable, and in particular if it is a quadratic irrational, then the discrepancy of the distribution is comparable to best possible. This result has been generalized to the case of a random walk in which the step size is chosen at random from a list of n possible steps; here one does best to take the list to be a *badly approximable vector*[HenSu]. These are discussed in Chapter 6.

1.7 Other Known Continued Fraction Expansions

Let ϕ be the golden mean constant $(1 + \sqrt{5})/2$. Then

$$\alpha := \sum_{n=1}^{\infty} 2^{-\lfloor n/\phi \rfloor} = [0; 2^0, 2^1, 2^1, 2^2, 2^3, 2^5, 2^8, 2^{13} \dots]$$

where the exponents are the Fibonacci numbers. This result, and a generalization, goes back to Böhmer[B]. There is a nice proof of the more general result in [AB]. One key tool is an old observation of H. J. S. Smith, Note on continued fractions, Messenger Math. 6 (1876), 1-14. We quote this result from [AB]:

Let α be an irrational number with $0 < \alpha < 1$. Let $\alpha = [0, a_1, a_2, \dots]$ and $p_n/q_n = [0, a_1, a_2, \dots, a_n]$, $n \geq 0$, where p_n, q_n are relatively prime non-negative integers. (As usual, we put $p_{-1} = 0, p_0 = 1, q_{-1} = 1, q_0 = 0$, so that $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$ for all $n \geq 1$.) For $n \geq 1$, define $f_\alpha(n) = \lfloor (n+1)\alpha \rfloor - \lfloor n\alpha \rfloor$, and consider the infinite binary sequence $f_\alpha(n)_{n \geq 1}$, which is sometimes called the *characteristic sequence* of α . Define binary words X_n , $n \geq 0$, by $X_0 = 0$, $X_1 = 0^{a_1-1}1$, $X_n = X_{n-1}^{a_n} X_{n-2}$ for $n \geq 2$, where X^a denotes the word X repeated a times, and $X_1 = 1$ if $a_1 = 1$. Then for each $n \geq 1$, X_n is a prefix of f_α . That is, $X_n = f_\alpha(1)f_\alpha(2) \dots f_\alpha(s)$ where s is the length of X_n .

Remark 1.4 *The proof of this last statement is a matter of attention to detail once the key is at hand: the progression of $(n\alpha) \bmod 1$ brings one back to near zero for each q_k , so that the further progress of the sequence will duplicate its initial segment, until such time as the difference between $q_k \alpha \bmod 1$, and exactly zero, becomes large enough to affect the result.*

There is another more recently discovered class of particular numbers defined in some other way than by their continued fraction expansion, for which the continued fraction is known. The best known instance is

$$\beta := \sum_{n=0}^{\infty} 2^{-2^n} = [0; 1, 4, 2, 4, 4, 6, 4, 2, 4, 6, 2, 4, 6, 4, 4, 2, \dots]$$

due originally to M. Kmošek [Km] and independently by J. Shallit [Sh1]. The most recent work along these lines of which the author is aware is H. Cohn's paper [Ch]. Some of the key ideas can be stated briefly. First, one

may study the more general situation

$$\sum_{n=0}^{\infty} 1/f^n(x)$$

where $f^n(x)$ denotes the n -fold iteration of f on x , and f is a polynomial function which takes integer values at integers. Secondly, there is a *folding lemma* at the heart of these expansions.

Folding Lemma: If $p_n/q_n = [a_0, \vec{w}]$, $\overleftarrow{v} = (-w_n, -w_{n-1}, \dots, -w_1)$, and $0 < x < 1$ then

$$\frac{p_n}{q_n} + \frac{(-1)^n}{xa_n^2} = [a_0, \vec{w}, x, \overleftarrow{v}].$$

This lemma is also used in an analysis of the intriguing number, call it the van der Poorten-Shallit constant,

$$\sum_{n=0}^{\infty} 2^{-F_n} = [1, 10, 6, 1, 6, 2, 14, 4, 124, 2, 1, 2, 2039, 1, 9, 1, 1, 1, 262111, \dots].$$

It is unusual to find numbers outside the familiar classes of rational and quadratic irrational, defined other than by their continued fraction expansions, for which that continued fraction expansion is atypical of randomly chosen real numbers. This one results from taking the special case $X = 2$ in a formal identity for the continued fraction expansion of the Laurent series $\sum X^{-F_j}$ [vdPS].

One application of this to matters outside the immediate topic of continued fractions is a proof that every prime p of the form $p = 4n + 1$ is the sum of two squares. See [CELV] for a very simple and clear proof. The basic idea is that corresponding to every integer $2 \leq b < p/2$ there is a list (a_1, a_2, \dots, a_r) so that $[a_1, a_2, \dots, a_r] = b/p$. Since there are $2n - 1$ such lists, (one for each value of b) and since $2n - 1$ is odd, if we pair each off with its reversal $(a_r, a_{r-1}, \dots, a_1)$ there must be one case of a list paired with itself. That list will be palindromic, reading the same forward and backward, and with a little more work, one sees that it must have $r = 2s$ even. Thus, $p = |a_1, a_2, \dots, a_s, a_s, a_{s-1}, \dots, a_1|$ and $p = |a_1, a_2, \dots, a_s|^2 + |a_1, a_2, \dots, a_{s-1}|^2$. While this proof does not give any efficient way to find the two squares, another continued-fraction idea does. Half the residues mod p are quadratic nonresidues. Take a random $1 < b < p$ and check whether it is a quadratic nonresidue by checking whether $b^{(p-1)/2} \equiv -1 \pmod{p}$. Half the time, this will be the case, so with reasonable luck, such a b can be found quickly.

Retrieve $n = b^{(p-1)/4} \pmod p$, and observe that $n^2 \equiv -1 \pmod p$. The lattice generated by $(n, 1)$ and $(p, 0)$ is a set of integer pairs (u, v) such that $u^2 + v^2 \equiv 0 \pmod p$. It has determinant p , so the shortest nonzero vector in the lattice lies within the square $-\sqrt{p} < x < \sqrt{p}, -\sqrt{p} < y < \sqrt{p}$. The Gauss lattice reduction algorithm is an efficient method for finding this shortest vector, and the resulting (u, v) will satisfy $u^2 + v^2 = p$.

1.7.1 Notes

Edward R. Burger [Bg] shows that there are real numbers for which all the denominators of convergents are squares, cubes, or values of other such polynomials, or even prime. Unsolved is whether these things can be achieved using real numbers for which the continued fraction expansion has bounded partial quotients.

Glyn Harman and Kam C. Wong [HW] show that almost all real α have infinitely many even numbered convergents with even numerator, and they give a natural generalization.