Hamburger Beiträge
zur Angewandten Mathematik

On the number 50

Dedicated to Marie Luise and Reiner Lauterbach on the occasion of their 50th birthday

Gerhard Opfer

This paper has been submitted to the
Mitteilungen der Mathematischen Gesellschaft in Hamburg
and will be published as Volume 24(2005), p. 151-174
The final form may differ from this preprint

Reihe A
Preprint 188
October 2005

Hamburger Beiträge zur Angewandten Mathematik

Reihe A	Preprints
Reihe B	Berichte
Reihe C	Mathematische Modelle und Simulation
Reihe D	Elektrische Netzwerke und Bauelemente
Reihe E	Scientific Computing
Reihe F	Computational Fluid Dynamics and Data Analysis

On the number 50

Gerhard Opfer

Dedicated to Marie Luise and Reiner Lauterbach
on the occasion of their 50th birthday

Abstract. We make some observations concerning the number 50. We conjecture that this number shares a special property only with one other number. In another context it appears to be unique. We mention also a special property of the number 50 with respect to the current calendar. It turns out that in a certain context Pell's equation plays a fundamental role. We will treat it from an algebraic point of view (quadratic forms) and from an analytic point of view (continued fractions for algebraic numbers of degree two).

Keywords. Pell's equation, Padé approximations, consecutive integers, sandwiched integers, calendar periods.

2000 MSC. 01, 11Axx, 11D09, 41A21.

§1. A significant property of the number 50

If someone reaches the age of 50, then one year long he or she was 49 years of age. This is a trivial observation. In mathematical terms the natural number 50 is the successor of 49 and 49 is the predecessor of 50. And now, the important observation, 49 is a square and 50 is twice a square. If we set $50 = 2m^2$, where $m = 5$ and $49 = n^2$, where $n = 7$ the two numbers m, n satisfy the equation

$$f(m,n) := 2m^2 - n^2 = 1. \tag{1}$$

We are of course interested in whether this equation has some other solutions in the set of pairs of natural numbers $(m, n) \in \mathbb{N}^2$, where $\mathbb{N} := \{1, 2, \ldots\}$. At a first glance we see, that $m = n = 1$ is a solution. Then we also see, that solutions must be located in a certain cone of the (m, n)-plane.

Lemma 1. *Let $(m, n) \in \mathbb{N}^2$. Then (m, n) can solve (1) only if*

$$\frac{1}{2}\sqrt{2}\,n < m \le n.$$

Proof: Let $\frac{1}{2}\sqrt{2}\,n \ge m$. Then, $2m^2 \le n^2$ and thus, $f(m, n) = 2m^2 - n^2 \le 0$, and (m, n) cannot solve (1). Now, assume that $m > n$. Then $f(m, n) = 2m^2 - n^2 > 2n^2 - n^2 = n^2 \ge 1$ and again, (m, n) cannot be a solution to (1). □

If we generalize the above f to any quadratic form in two integer variables m, n with integer coefficients, then, it is clear that the equation $f(m, n) = d$, where d is any fixed integer has no or at most finitely many solutions $(m, n) \in \mathbb{Z}^2$ if f is a definite form. Since the above f is indefinite there is a chance that infinitely many solutions exist. We introduce a new notion, called an observation. It has the character of a theorem but the proof is by inspection, either in the literal sense, or by application of a simple computer program. The word simple should indicate that the program is easy and quick to write and that the running time is not important. As such, an observation should not be followed by a formal proof.

Observation 2. *The following natural pairs (m, n) given in Table 3 solve equation (1) and there are no other solutions for $n \le 10^7 - 1$.*

Table 3. First ten solutions of equation (1) and difference $\frac{m}{n} - s$ where $s = \frac{1}{2}\sqrt{2}$

No.	m	n	$\frac{m}{n} - s$	No.	m	n	$\frac{m}{n} - s$
1	1	1	$2.9\cdot10^{-1}$	6	5 741	8 119	$5.4\cdot10^{-9}$
2	5	7	$7.2\cdot10^{-3}$	7	33 461	47 321	$1.6\cdot10^{-10}$
3	29	41	$2.1\cdot10^{-4}$	8	195 025	275 807	$4.6\cdot10^{-12}$
4	169	239	$6.2\cdot10^{-6}$	9	1 136 689	1 607 521	$1.4\cdot10^{-13}$
5	985	1 393	$1.8\cdot10^{-7}$	10	6 625 109	9 369 319	$4.0\cdot10^{-15}$

If we plot these solutions in an (m, n) plane we see that they are located, optically, on a straight line with slope approximately $\sqrt{2}$. Because such a line is not interesting, we do not present it here. However, a glance at Lemma 1, reveals that the given solutions are not exactly located on that line. We also see from Table 3 that the quotients $\frac{m}{n}$ provide a sequence of approximations for $\frac{1}{2}\sqrt{2}$ with increasing precision.

Now we have to find a means to compute these pairs. From equation (1) we deduce

$$m = \sqrt{\frac{1}{2}(n^2+1)} = \frac{1}{2}\sqrt{2}\,n\sqrt{1+\frac{1}{n^2}}. \tag{2}$$

Let us for a while neglect the restriction, that n is a natural number and assume only that $1/n^2 < 1$ which is true for all $n > 1$. Then we can employ Taylor's theorem for the square root on the right hand side of (2) and obtain

$$m = \frac{1}{2}\sqrt{2}\,n\Big(1+\frac{1}{2n^2}+R_2(n^2)\Big), \tag{3}$$

where

$$R_2(n^2) = \frac{-1}{8n^4\Big(1+\dfrac{\theta}{n^2}\Big)^{3/2}}, \quad 0 \le \theta \le 1. \tag{4}$$

Theorem 4. *Put $s := \frac{1}{2}\sqrt{2}$ and assume that $\frac{m}{n}$, $m, n \in \mathbb{N}$ is any approximation of s with $s = \frac{m}{n} + \varepsilon$. Then (m,n) solves (1) if and only if*

$$\varepsilon = -s\Big(\frac{1}{2n^2}+R_2(n^2)\Big). \tag{5}$$

Proof: (i) Let (m,n) be a solution of (1). Then the formulae (2), (3) follow and therefore, we obtain

$$\frac{m}{n} = s\Big(1+\frac{1}{2n^2}+R_2(n^2)\Big) = s + s\Big(\frac{1}{2n^2}+R_2(n^2)\Big) = s - \varepsilon$$

and (5) is valid. (ii) Let (m,n) be an approximation of s such that (5) is valid. Then by using (5) we have $m = n(s-\varepsilon) = ns\Big(1+\frac{1}{2n^2}+R_2(n^2)\Big)$ and $2m^2 = n^2\Big(1+\frac{1}{2n^2}+R_2(n^2)\Big)^2$. Now, using $R_2(n^2) = \sqrt{1+\frac{1}{n^2}} - \big(1+\frac{1}{2n^2}\big)$, it takes few algebraic steps to show that $2m^2 = n^2+1$. $\square$

If we evaluate the right hand side of (5) we obtain an ε for every n. It is sort of a miracle that for some of these ε we can find an integer m such that $\frac{m}{n}$ is an approximation for s with just this ε as approximation error.

Example 5. In the special case of solution No. 2 of Table 3, namely $m = 5, n = 7$ we have $s = \frac{5}{7} + \varepsilon = \frac{5}{7} - 7.1789 \cdot 10^{-3}$. The remainder term is $R_2(7^2) = -5.1537 \cdot 10^{-5}$. And equation (5) (using exact representations of ε, and of $R_2(7^2)$) is valid. Let us take $(m, n) = (12, 17)$. Here we have $s = \frac{12}{17} - 1.2244 \cdot 10^{-3}$ and $R_2(17^2) = -1.4940 \cdot 10^{-6}$. However, a numerical inspection already shows that (5) is not valid.

Instead of solving (1) for m we can solve (1) for n as well and obtain

$$n = \sqrt{2m^2+1} = \sqrt{2}\, m \sqrt{1 + \frac{1}{2m^2}}.$$

Taylor's theorem is applicable for $m \geq 1$ and we have

$$n = \sqrt{2}\, m \Big(1 + \frac{1}{4m^2} + R_2(2m^2)\Big),$$

where R_2 is already defined in (4). The following theorem is not surprising.

Theorem 6. *Let $\sigma := \sqrt{2}$ and assume that $\frac{n}{m}$, $m, n \in \mathbb{N}$ is an approximation of σ with $\sigma = \frac{n}{m} + \vartheta$. Then (m, n) solves (1) if and only if*

$$\vartheta = -\sigma\Big(\frac{1}{4m^2} + R_2(2m^2)\Big).$$

Proof: Essentially repeat the proof of Theorem 4. □

Let us assume that (m, n) solves (1) and that $s = \frac{m}{n} + \varepsilon$ and $\sigma = \frac{n}{m} + \vartheta$. Then $1 = s\sigma = (\frac{m}{n} + \varepsilon)(\frac{n}{m} + \vartheta) = 1 + \frac{m}{n}\vartheta + \varepsilon\frac{n}{m} + \varepsilon\vartheta$ or

$$\frac{m}{n}\vartheta + \varepsilon\frac{n}{m} + \varepsilon\vartheta = 0.$$

We assume that (m, n) is large enough so we can neglect the term $\varepsilon\vartheta$ and obtain

$$\vartheta \approx -2\varepsilon,$$

where we have also replaced $\frac{n^2}{m^2}$ by two. Let us take solution No. 5, $(m, n) = (985, 1393)$ as an example. Then $s - \frac{m}{n} = \varepsilon = -1.82201\,82285 \cdot 10^{-7}$, $\sigma - \frac{n}{m} = \vartheta = 3.64403\,55200 \cdot 10^{-7}$ and $-2\varepsilon = 3.64403\,64570 \cdot 10^{-7}$ which agrees with ϑ for 7 digits.

What we have learned here is that not all approximations $\frac{m}{n}$ of $\frac{1}{2}\sqrt{2}$ are solutions of equation (1).

§2. Quadratic forms in two variables and Pell's equation

Number theorists are very much interested in integer solutions and the properties of algebraic equations with integer coefficients. One such problem is the solution of $f(\mathbf{x}) = d$ where f represents a quadratic form in n variables $\mathbf{x}$ with integer coefficients and d is any fixed integer. We will give a short exposé for the case of two variables. To some extent we follow SCHOLZ & SCHOENEBERG [1961, p. 122–126]. Let

$$\mathbf{A} := \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \in \mathbb{Z}^{2\times 2}$$

be a symmetric matrix with integer entries and $\mathbf{x} := (x_1, x_2)^{\mathrm{T}}$. Then the quadratic form reads

$$f(\mathbf{x}) := \frac{1}{2}\mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x} = ax_1^2 + bx_1x_2 + cx_2^2 =: (a, b, c),$$

where (a, b, c) is another (inconsistent but common) abbreviation for the quadratic form with coefficients a, b, c. Since $\mathbf{A}$ is symmetric, the two eigenvalues λ_1, λ_2 of $\mathbf{A}$ are real. According to Vieta's theorem, the product $\lambda_1\lambda_2$ of these eigenvalues is the constant term of the characteristic polynomial of $\mathbf{A}$ which coincides with the determinant of $\mathbf{A}$. Therefore, we have

$$D := \lambda_1\lambda_2 = \det(\mathbf{A}) = 4ac - b^2.$$

So we have the following classification, already known from school mathematics, see SCHÜLKE [1959, p. 41]:

$$D \begin{cases} > 0: & \mathbf{A} \text{ is definite, elliptic case,} \\ < 0: & \mathbf{A} \text{ is indefinite, hyperbolic case,} \\ = 0: & \mathbf{A} \text{ is semi definite, parabolic case.} \end{cases}$$

The elliptic case is the least interesting case. In this case, the solution set of $f(\mathbf{x}) = d$ for a fixed, real d regarded as an equation in $\mathbb{R}^2$ is either the circumference of an ellipse, one point, or empty. Therefore, the corresponding integer case has either no solution or only finitely many solutions.

It is reasonable to study only so-called primitive forms (a, b, c) which means that a, b, c do not have a factor (different from 1) in common since $(ta, tb, tc) = t(a, b, c)$ for all integers t.

We want to study the solutions of $f(\mathbf{x}) = d$ for a fixed d and we will see that a whole equivalence class of quadratic forms will have exactly the same solution behavior. An integer matrix $\mathbf{T}$ will be called unimodular if $\det \mathbf{T} = \pm 1$. This implies that the inverse $\mathbf{T}^{-1}$ exists and has also integer entries. Let

$$\mathbf{T} := \begin{pmatrix} r & v \\ s & w \end{pmatrix} \in \mathbb{Z}^{2\times 2} \tag{6}$$

be a unimodular matrix and

$$\mathbf{U} := \begin{pmatrix} w & -v \\ -s & r \end{pmatrix}, \text{ then, } \mathbf{T}^{-1} = \begin{cases} \mathbf{U} & \text{if } \det(\mathbf{T}) = 1, \\ -\mathbf{U} & \text{if } \det(\mathbf{T}) = -1. \end{cases} \tag{7}$$

If we put

$$\mathbf{u} := \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} := \mathbf{T}\mathbf{x}, \tag{8}$$

then,

$$\begin{aligned} f(\mathbf{x}) = f(\mathbf{T}^{-1}\mathbf{u}) =: \varphi(\mathbf{u}) &:= \frac{1}{2}(\mathbf{T}^{-1}\mathbf{u})^{\mathrm{T}}\mathbf{A}\mathbf{T}^{-1}\mathbf{u} \\ &= \frac{1}{2}\mathbf{u}^{\mathrm{T}}\left\{(\mathbf{T}^{-1})^{\mathrm{T}}\mathbf{A}\mathbf{T}^{-1}\right\}\mathbf{u} =: Au_1^2 + Bu_1u_2 + Cu_2^2, \end{aligned} \tag{9}$$

where

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \mathbf{M}\begin{pmatrix} a \\ b \\ c \end{pmatrix}, \text{ with } \mathbf{M} := \begin{pmatrix} r^2 & rs & s^2 \\ 2rv & rw + sv & 2sw \\ v^2 & vw & w^2 \end{pmatrix}. \tag{10}$$

The matrix $\mathbf{M}$ has the same determinant as $\mathbf{T}$ and is therefore also unimodular: the inverse exists and has integer entries. If we find the solutions of $\varphi(\mathbf{u}) = d$ we also have the solutions of $f(\mathbf{x}) = d$ and vice versa. In particular, the determinant

$$D_1 := 4AC - B^2 = (4ac - b^2)(rw - sv)^2 = D$$

remains unchanged. The connection between $\mathbf{u}$ and $\mathbf{x}$ is via $\mathbf{T}$ in (8). The two quadratic forms $f(\mathbf{x}) = (a, b, c)$ and $\varphi(\mathbf{u}) = (A, B, C)$ are called equivalent which defines an equivalence relation in the ordinary sense. We will mention only in passing that D or $D+1$ is always divisible by 4 and that all integers with this property can occur as determinants. We will see that those values of determinants D for which $-D$ is a square: $0, -1, -4, -9, -16, -25, \ldots$ do not yield a solution.

Let f be a given quadratic form and $d \in \mathbb{Z}$ a given integer. A theorem which gives precise information on the question whether $f(\mathbf{x}) = d$ has an integer solution $\mathbf{x}$ is apparently lacking. However, there is a theorem of the following type: Let D be the determinant of a quadratic form and $d \in \mathbb{Z}$. Then one can find a quadratic form f with determinant D such that $f(\mathbf{x}) = d$ has a solution if and only if certain conditions (depending only on D, d) are fulfilled, cf. Scholz & Schoeneberg [1961, p. 105]. Thus, if these conditions are not met, then all equations $f(\mathbf{x}) = d$ where the determinant of f is D have no solutions.

Now, we try to find those transformations $\mathbf{T}$ which keep the given quadratic form fixed. The idea is to choose a unimodular matrix $\mathbf{T}$ such that

$$\mathbf{A} = \mathbf{T}^{\mathrm{T}} \mathbf{A} \mathbf{T} \tag{11}$$

which yields (see (9))

$$\varphi(\mathbf{u}) = f(\mathbf{u}).$$

A comparison of the matrix elements in (11) yields three equations (the two off diagonal elements yield the same equation) which can be put into the form

$$\mathbf{P} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \mathbf{0}, \text{ where } \mathbf{P} := \begin{pmatrix} r^2 - 1 & rs & s^2 \\ 2rv & rw + sv - 1 & 2sw \\ v^2 & vw & w^2 - 1 \end{pmatrix} = \mathbf{M} - \mathbf{I},$$

where $\mathbf{M}$ is defined in (10). In other words, we have to look for unimodular $\mathbf{T}$ such that all eigenvalues of $\mathbf{M}$ are one. Rather than comparing the two sides of (11) we can also compare the elements of either side of

$$\mathbf{A}\mathbf{T}^{-1} = \mathbf{T}^{\mathrm{T}} \mathbf{A}$$

which is a little easier and implies ($\mathbf{T}^{-1}$ is given in (7))

$$sb = (w - r)a; \quad -vb = (w - r)c; \quad sc = -va \text{ for } \det \mathbf{T} = 1, \tag{12}$$

$$r = -w; \quad br = av - cs \text{ for } \det \mathbf{T} = -1. \tag{13}$$

Since all numbers in (12) are integers, the equations (12) imply that s is a multiple of a and v is a multiple of c (using that the form (a, b, c) is primitive and $ac \neq 0$). So if we set

$$au_1 = s, \quad u_2 = r + w \tag{14}$$

we obtain from (12)

$$r = \frac{1}{2}(u_2 - bu_1), \quad s = au_1, \quad v = -cu_1, \quad w = \frac{1}{2}(u_2 + bu_1). \tag{15}$$

Any integer pair u_1, u_2 would solve the problem of finding a matrix $\mathbf{T}$ with property (11) and $\det \mathbf{T} = 1$. Now, only a little computation is necessary to finding the decisive equation

$$4(rw - sv) = u_2^2 + Du_1^2 = 4. \tag{16}$$

In number theory an equation of type $u_2^2 + Du_1^2 = 4$ is called Pell's equation.[1)] If we put $u_1 = 2v_1, u_2 = 2v_2$, then Pell's equation would read $v_2^2 + Dv_1^2 = 1$. The equations (13) are treated by Scholz & Schoenberg [1961, p. 123/124]. Another questions leads to another type of Pell's equation. If we require that (a, b, c) and $(-a, -b, -c)$ are equivalent we have to find a unimodular $\mathbf{T}$ with $\det \mathbf{T} = -1$ with $\mathbf{T}^{\mathrm{T}}\mathbf{A} = (-\mathbf{A})\mathbf{T}^{-1}$ or equivalently, $-\mathbf{A} = \mathbf{T}^{\mathrm{T}}\mathbf{A}\mathbf{T}$. With the same reasoning as in the case of equations (12) we obtain by using (14) the same equations as (15) but

$$4(rw - sv) = u_2^2 + Du_1^2 = -4. \tag{17}$$

This is another type of Pell's equation. We find (Scholz & Schoeneberg, [1961, p. 123, 126]) the following information: Pell's equation (16) has solutions for all $D < 0$ if $-D$ is not a square. Pell's equation (17) has solutions if $-D = p$ and p is a prime number such that $p - 1$ is a multiple of four ($p = 5, 13, 17, 29, 37, 41, ...$). There is no solution if $-D$ has a prime factor p such that $p - 3$ is a multiple of four ($p = 3, 7, 11, \ldots$).

[1)] John Pell, 1611 (Southwick) – 1685 (London). The name Pell's equation is probably based on an error of L. Euler, see Gottwald et alii [1990, p. 363/364] for more details. Henrici [1977, p. 499] writes: "... among the mathematicians who contributed to the theory of Pell's equation we find Archimedes, Fermat, Euler (but no Pell)."

Example 7. Let $\mathbf{A} := \begin{pmatrix} 2 & 4 \\ 4 & 4 \end{pmatrix}$. Then $D := \det \mathbf{A} = -8$. Pell's equation (16) has a solution $u_1 = 12, u_2 = 34$. And by means of (6), (15) we find $\mathbf{T} = \begin{pmatrix} -7 & -24 \\ 12 & 41 \end{pmatrix}$ which indeed solves (11) and has determinant one. Pell's equation (17) has a solution $u_1 = 29, u_2 = 82$ which implies $\mathbf{T} = \begin{pmatrix} -17 & -58 \\ 29 & 99 \end{pmatrix}$, $\det \mathbf{T} = -1$, and $\mathbf{T}^{\mathrm{T}}\mathbf{A}\mathbf{T} = -\mathbf{A}$.

Since with $\mathbf{T}$ also any power $\mathbf{T}^j$ is unimodular with $\det \mathbf{T}^j = (\det \mathbf{T})^j$, $j = 0, 1, \ldots$ we have a very convenient tool to compute all solutions of Pell's equation if we only know one solution, because from any $\mathbf{T}$ we can recover the solution of Pell's equation by applying (14). In particular, if $\det \mathbf{T} = -1$ the powers $\mathbf{T}^j$ solve the two types (16), (17) of Pell's equation alternatively. Let $\mathbf{T}$ be a given unimodular matrix which satisfies $\det \mathbf{T} = -1$ and $-\mathbf{A} = \mathbf{T}^{\mathrm{T}}\mathbf{A}\mathbf{T}$. Then, we have $-\mathbf{A} = (\mathbf{T}^{\mathrm{T}})^j \mathbf{A}\mathbf{T}^j$ for odd j and $\mathbf{A} = (\mathbf{T}^{\mathrm{T}})^j \mathbf{A}\mathbf{T}^j$ for even j. Let

$$\mathbf{T}^0 := \begin{pmatrix} r_0 & v_0 \\ s_0 & w_0 \end{pmatrix} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{T} := \begin{pmatrix} r_1 & v_1 \\ s_1 & w_1 \end{pmatrix}, \ \mathbf{T}^j := \begin{pmatrix} r_j & v_j \\ s_j & w_j \end{pmatrix}, \ j \geq 1.$$

For any unimodular matrix we deduce from (7) that $\mathbf{T} + \det\, \mathbf{T}\mathbf{T}^{-1} = (r+w)\mathbf{I}$ which implies here

$$\mathbf{T}^{j+1} - \mathbf{T}^{j-1} = (\mathbf{T} - \mathbf{T}^{-1})\mathbf{T}^j = (r_1 + w_1)\mathbf{T}^j.$$

By (14) we put

$$u_1^{(0)} := 0,\ u_2^{(0)} := 2; \quad a u_1^{(j)} := s_j,\ u_2^{(j)} := r_j + w_j,\ j \geq 0$$

and obtain finally

$$(18) \quad u_1^{(j+1)} := u_2^{(1)} u_1^{(j)} + u_1^{(j-1)}, \quad u_2^{(j+1)} := u_2^{(1)} u_2^{(j)} + u_2^{(j-1)}, \quad j = 1, 2, \ldots$$

The pairs $(u_1^{(2j)}, u_2^{(2j)})$, $j = 1, 2, \ldots$ solve Pell's equation (16) and the pairs $(u_1^{(2j+1)}, u_2^{(2j+1)}), j = 0, 1, 2, \ldots$ solve Pell's equation (17). For $D = -8$ we obtain as solutions of equation (16) the pairs $(0, 2), (2, 6), (12, 34), \ldots$, and $(1, 2)$, $(5, 14), (29, 82), \ldots$ for (17).

The following lemma is implied by the recursion (18).

Lemma 8. *Let there exist a positive solution* $(u_1 > 0, u_2 > 0)$ *of Pell's equation (17). Then both Pell's equations (16), (17) have infinitely many positive solutions. If* $D < 0$*, then,* $\lim_{j\to\infty} \frac{u_2^{(j)}}{u_1^{(j)}} = \sqrt{-D}$.

Proof: The recursion (18) implies that both sequences $\{u_1\}, \{u_2\}$ are strictly increasing. Therefore $u_1^{(j)} \to \infty, u_2^{(j)} \to \infty$ and the final result follows from dividing (16), (17) by $(u_1^{(j)})^2$. □

We return to our original equation (1). If we multiply it by -4 we obtain $4n^2 - 8m^2 = -4$. If we put $2n := \tilde{n}$ we obtain Pell's equation of the form (17), namely

$$\tilde{n}^2 - 8m^2 = -4. \tag{19}$$

It is clear that all solutions $(m, \tilde{n})$ of (19) must have the property that $\tilde{n}$ is even, so that a solution $(m, \tilde{n})$ of (19) implies a solution $(m, \tilde{n}/2) = (m, n)$ of (1).

Theorem 9. *Equation (1) has infinitely many solutions* $(m, n) \in \mathbb{N}^2$ *and* $\frac{m}{n} \to \frac{1}{2}\sqrt{2}$.

Proof: Apply Lemma 8 using that $(m, n) := (1, 2)$ is a positive solution of (17). □

A connection between Pell's equation and the approximation of a square root is furnished by the theory of rational approximations by Padé approximations and continued fractions. This topic will be treated in the next chapter.

So far we have not yet exploited all the properties of the magic number 50. It is not only the double of a square, but the square is a square of a prime number. And the predecessor, the number 49 is the square of a prime number as well.

So we have to pose our problem again: Are there integer solutions $(m, n) \in \mathbb{N}^2$ of equation (1) where both m, n are primes.

Observation 10. *For all* 664 579 *primes* $n \le 10^7$ *(the last is* 9 999 991*) equation (1) has only two solutions* $(m, n) = (5, 7)$, $(m, n) = (29, 41)$ *where* m *is also prime. There are two additional solutions where only* n *is prime, but not* m*, namely the solutions No. 4 and No. 10 of Table 3.*

Only as aperçu we mention, that the second solution $(m, n) = (29, 41)$, leading to an age of 1682 years would never have been the starting point of a paper dedicated to some person's birthday.

Conjecture 11. *Equation (1) has only two pairs of solutions for which both components are prime. These solutions are given in Observation 10.*

The problem, to compare and investigate two neighbors in the set of natural numbers with respect to a certain property also contains the famous Catalan problem (Catalan [1844]) which was only solved recently, Mihăilescu [2004]. The proof by Mihăilescu even gave rise to an article by Bethge [2002] in the German political magazine Der Spiegel. An overview can be found in Metsänkylä [2004]. Catalan's problem was, to prove that the two neighbors eight and nine were the only neighbors in the set of natural numbers which were powers: $8 = 2^3, 9 = 3^2$. Also in a recent paper, Opfer & Ripken [1998] have shown that Catalan's problem has an extension to the complex integers (Gaussian numbers) and an example is $12167\mathbf{i} = (-23\mathbf{i})^3$, $12168\mathbf{i} = (78+78\mathbf{i})^2$.

It is also common to investigate three consecutive integers $n-1, n, n+1$ for certain properties. One says that n is sandwiched[2)] by $n-1$ and by $n+1$. See Singh [1997, p. 63], [1998, p. 84] for many interesting problems and a historical context. A famous problem belonging to this class is Fermat's problem of the number 26 which is the only number sandwiched by a square $25 = 5^2$ and a cube $27 = 3^3$. In this case, the number 26 itself is characterized by its neighbors alone without using any properties of 26. Problems of similar type are treated in a book by Mordell [1969, Ch.26]. Some history of the 26-Problem by Fermat can be found in Mahoney [1973].

So we may also take the number 50 as being sandwiched by 49 and by 51. One property of 51 is that is has only two prime factors. But this does not lead to an interesting problem. Therefore, we introduce another problem, where also the middle number - the number to be sandwiched - has to obey certain rules.

Definition 12. Let N_1, N_2 be any two non empty subsets of $\mathbb{N}$. The problem of finding $(n_1, n_2) \in N_1 \times N_2$ such that $n_2 = n_1 + 2$ will be called sandwich problem. If in the sandwich problem we require, in addition, that $n = n_1 + 1$ belongs to another third subset $N \subset \mathbb{N}$, then this problem will be called strong sandwich problem.

Let p be an integer not divisible by three. Then, it is an easy exercise to

[2)] J. Montagu, 4th Earl of Sandwich, 1718–1792 introduced sandwiches for himself in order not to interrupt his passion for gambling.

show that $p^2 + 2$ is always divisible by three. Now, with $n = 50$ there is the following strong sandwich problem:

Problem 13. Find all integers $n \geq 2$ which are sandwiched by a square and a product of three and a prime and where n itself is the double of a square.

Some preliminary computer tests indicate that besides the solution $n = 50$ there is either no solution or a solution with a very large n. Therefore we dare the following conjecture.

Conjecture 14. *The above Problem 13 has only the solution $n = 50$. This is at least true for all $n \leq 10^8$.*

§3. Rational approximations for square roots, Padé approximations, and continued fractions

Rational functions have an important link to continued fractions and to Padé approximations. Let r_0, r_1 be arbitrary polynomials and r_1 not the zero polynomial. Then all functions of the type

$$r := \frac{r_0}{r_1}$$

are called rational functions. We assume that r_0, r_1 do not have common non-constant polynomial factors. The representation of the rational function r by the two polynomials r_0, r_1 is not unique because we can multiply r_0, r_1 by any non zero constant without changing r. This will be used for some normalization and simplification. Any rational function can be written in the form of a continued fraction. We first take an example from Opfer, [2002, p. 29]:

$$\begin{aligned} r(x) &= \frac{4x^2 + 3x - 2}{2x^2 - 4x + 5} \\ &= 2 + \frac{11x - 12}{2x^2 - 4x + 5} \\ &= 2 + \cfrac{11}{\cfrac{2x^2 - 4x + 5}{x - \cfrac{12}{11}}} \end{aligned}$$

$$= 2 + \cfrac{11}{2x - \cfrac{20}{11} + \cfrac{\frac{365}{11^2}}{x - \cfrac{12}{11}}}$$

$$= 2 + \cfrac{\frac{11}{2}}{x - \cfrac{10}{11} + \cfrac{\frac{365}{2\cdot 11^2}}{x - \cfrac{12}{11}}} = q_0 + \cfrac{c_1}{q_1 + \cfrac{c_2}{q_2}}.$$

The multiplications have been carried out in such a way that all occurring polynomials $q_1, q_2, \ldots$ have leading coefficient one. The evaluation of the given continued fraction requires 2 divisions, whereas the original rational function (using the Horner scheme) requires 4 multiplications and one division.

Now we describe the general case. Let the degree of any polynomial p be denoted by ∂p. If p is a constant$\neq 0$, then we write $\partial p = 0$. Let $r := \frac{r_0}{r_1}$ with $\partial r_0 \geq \partial r_1$ and apply Euclid's division algorithm

$$\begin{aligned} r_0 &= q_0 r_1 + r_2, \quad && \partial r_2 < \partial r_1, \\ r_1 &= q_1 r_2 + r_3, \quad && \partial r_3 < \partial r_2, \\ r_2 &= q_2 r_3 + r_4, \quad && \partial r_4 < \partial r_3, \\ &\ \vdots \\ r_{k-1} &= q_{k-1} r_k + r_{k+1}, \quad && 0 = \partial r_{k+1} < \partial r_k, \\ r_k &= q_k r_{k+1}, && r_{k+2} = 0. \end{aligned} \tag{20}$$

Since the polynomial degrees ∂r_k are strictly decreasing, this algorithm must terminate. If $\partial r_0 < \partial r_1$, then we write r in the form

$$r = \frac{r_0}{r_1} = \cfrac{c}{\cfrac{c r_1}{r_0}},$$

where c is chosen in such a way, that cr_1 an r_0 have the same leading coefficient and we apply the division algorithm to cr_1/r_0. In general, the continued fraction derived from Euclid's division algorithm has the form

$$r = \frac{r_0}{r_1} = q_0 + \frac{r_2}{r_1} = q_0 + \cfrac{1}{\cfrac{r_1}{r_2}} = q_0 + \cfrac{1}{q_1 + \cfrac{r_3}{r_2}} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cfrac{r_2}{r_3}}} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{r_4}{r_3}}} = \cdots$$

which can be written as

$$r = \frac{r_0}{r_1} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots \, q_{k-2} + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}. \tag{21}$$

In our example we have applied one additional multiplication in each step of Euclid's division algorithm in order to obtain polynomials

$$\tilde{q}_j := \alpha_j q_j, \ j = 1, 2, \ldots, k,$$

with leading coefficient one. In this case, the evaluation of a rational function $r := r_0/r_1$ with numerator degree ∂r_0 and denominator degree ∂r_1 at a specific value x requires $\max(\partial r_0, \partial r_1)$ multiplications or divisions when using the representation (22) as continued fraction (Opfer, [2002, p. 31]). If r is evaluted by evaluating r_0, r_1 separately by Horner's scheme, then, $\partial r_0 + \partial r_1 + 1$ multiplications/divisions are needed. Then (21) takes the more general form

$$r = \frac{r_0}{r_1} = q_0 + \cfrac{c_1}{\tilde{q}_1 + \cfrac{c_2}{\tilde{q}_2 + \cfrac{c_3}{\ddots \, \tilde{q}_{k-2} + \cfrac{c_{k-1}}{\tilde{q}_{k-1} + \cfrac{c_k}{\tilde{q}_k}}}}}. \tag{22}$$

Since the form (22) is space consuming and akward to write it is common to use the simpler notation,

$$r = q_0 + \frac{c_1}{\tilde{q}_1 +} \quad \frac{c_2}{\tilde{q}_2 +} \quad \frac{c_3}{\tilde{q}_3 +} \quad \cdots \quad \frac{c_{k-1}}{\tilde{q}_{k-1} +} \quad \frac{c_k}{\tilde{q}_k}. \tag{23}$$

Such a continued fraction is determined by two vectors $c := (c_1, c_2, \ldots, c_k)$, $q := (q_0, \tilde{q}_1, \ldots, \tilde{q}_k)$. Besides the backwards evaluation formula, there is also a forward evaluation formula in matrix form named after Euler and Wallis. It computes all subfractions

$$\frac{A_j}{B_j} := q_0 + \frac{c_1}{\tilde{q}_1 +} \frac{c_2}{\tilde{q}_2 +} \frac{c_3}{\tilde{q}_3 +} \cdots \frac{c_{j-1}}{\tilde{q}_{j-1} +} \frac{c_j}{\tilde{q}_j}, \quad j = 0, 1, \ldots, k, \tag{24}$$

of (23). The forward evaluation formula reads as follows:

$$\begin{aligned} &\begin{pmatrix} A_j & A_{j-1} \\ B_j & B_{j-1} \end{pmatrix} = \begin{pmatrix} A_{j-1} & A_{j-2} \\ B_{j-1} & B_{j-2} \end{pmatrix} \begin{pmatrix} \tilde{q}_j & 1 \\ c_j & 0 \end{pmatrix}, \; j = 1, 2, \ldots, k, \\ &\begin{pmatrix} A_0 & A_{-1} \\ B_0 & B_{-1} \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}, \quad r = \frac{A_k}{B_k}. \end{aligned} \tag{25}$$

This form has the advantage that it can be applied to continued fractions of infinite length and that it can be terminated at all intermediate positions. However, it has the disadvantage that it needs roughly 4.5 times more flops than the backwards evaluation. This formula has another simple, but important consequence, namely

$$A_j B_{j-1} - A_{j-1} B_j = \det \begin{pmatrix} A_j & A_{j-1} \\ B_j & B_{j-1} \end{pmatrix} = (-1)^{j+1} c_1 c_2 \cdots c_j, \; j = 0, 1, \ldots, k. \tag{26}$$

So far we have associated a continued fraction to a rational function. However, this concept carries over to general functions f which are sufficiently smooth. Ordinarily one assumes that f is even analytic in a given interval. Then, a rational function $r = r_0/r_1$ with prescribed numerator and denominator degree $\partial r_0, \partial r_1$, respectively, is associated to f by requiring that the Taylor expansions of f and of r agree as far as possible. Let us denote

$$\partial r := \partial r_0 + \partial r_1 + 1 \tag{27}$$

and call it the **degree of** r. Then the above requirement can be written as

$$f(x) - r(x) = O(x^{\partial r}). \tag{28}$$

The set of all rational functions $r = r_0/r_1$ with given numerator and denominator degree at most $\partial r_0, \partial r_1$, respectively, will be denoted by

$$[\partial r_0/\partial r_1].$$

A function $r \in [\partial r_0/\partial r_1]$ in this way associated to f is called **Padé approximation** of f. Such a Padé approximation may not exist, but there are never two different Padé approximations. In many cases the Padé approximation has a much better convergence behavior than the Taylor series of f. Details and examples can be found in books on Padé approximation, like the book by BAKER [1975] or BAKER & GRAVES-MORRIS [1981]. A very detailed history on Padé approximations is given by BREZINSKI [1991]. One example from BAKER [1975, p. 3/4] is

$$f(x) = \sqrt{\frac{1+2x}{1+x}} = 1 + \frac{1}{2}x - \frac{5}{8}x^2 + \frac{13}{16}x^3 - \frac{141}{128}x^4 + \cdots$$

where the Taylor series is not converging for $x > \frac{1}{2}$, though $\lim_{x\to\infty} f(x) = \sqrt{2}$. In this case the Padé approximation $r \in [1/1]$ has the form

$$r(x) = \frac{1 + \frac{7}{4}x}{1 + \frac{5}{4}x} = 1 + \frac{1}{2}x - \frac{5}{8}x^2 + O(x^3)$$

and $\lim_{x\to\infty} r(x) = \frac{7}{5}$ which agrees with $\sqrt{2}$ already for two digits. Let $r \in [\partial r_0/\partial r_1]$ with prescribed $\partial r_0, \partial r_1$ and let f be given with

$$f(x) = t(x) + O(x^{\partial r})$$

where t is the Taylor polynomial

$$t(x) := \sum_{k=0}^{\partial r - 1} \frac{f_k}{k!}\, x^k$$

of f. It may be regarded as a one point Hermite-Lagrange polynomial and the condition (28) is equivalent to the rational one point interpolation problem

$$r^{(k)}(0) = f_k, \quad k = 0, 1, \ldots, \partial r - 1, \quad r \in [\partial p/\partial q],$$

where ∂r is defined in (27). Let r have the form

$$r(x) := \frac{p(x)}{q(x)} := \frac{\sum_{j=0}^{\partial p} p_j x^j}{\sum_{k=0}^{\partial q} q_k x^k}.$$

If we multiply equation (28) by q and neglect all terms of order ∂r and higher we obtain a system of linear equations for the $\partial r + 1$ unknown coefficients p_j, $j = 0, 1, \ldots, \partial p$, q_k, $k = 0, 1, \ldots, \partial q$. Since p/q does not change if we multiply numerator and denominator by any non vanishing constant, we may assume that $q_0 = 1$. However, tacitly by this setting we assume that $q_0 \neq 0$. If we follow Baker & Graves-Morris [1981, p. 2/3] we obtain a linear $(\partial r \times \partial r)$ system which splits into a $(\partial q \times \partial q)$ system for the denominator coefficients q_k alone and one $(\partial p + 1 \times \partial p + 1)$ system for all coefficients. These systems have a special structure which allows a simplified solution technique.

Let us end this part with a well known example (Abramowitz & Stegun [1964, p. 81]), namely

$$\arctan x = \sum_{j=0}^{\infty} (-1)^j \frac{z^{2j+1}}{2j+1} = \frac{z}{1+} \frac{z^2}{3+} \frac{4z^2}{5+} \frac{9z^2}{7+} \cdots \frac{j^2 z^2}{(2j+1)+} \cdots (j \geq 1).$$

The Taylor series is valid for $|z| \leq 1, z \neq \pm\mathbf{i}$, the continued fraction is valid for all complex z with the exception of $z = \pm\mathbf{i}s$ and $s \geq 1$. For $x = 1023/1024 \approx 0.9990$ we have $\arctan(x) \approx 0.78491$. The Taylor expansion with six terms and using 26 flops gives 0.74401 (error$=$ 0.04) and the continued fraction with six terms using 11 flops gives 0.78510 (error$=$ 0.0002, which is 200 times smaller).

We will treat the same problem as before, but applied to numbers. For rational numbers $r = r_0/r_1$ Euclid's division algorithm (20) just mentioned will work for this case as well. The numbers ∂r_j have to be replaced by r_j directly. Let $r_0 > r_1 > 0$. The last number is then $r_{k+1} = \gcd(r_0, r_1)$, the greatest common divisor of r_0, r_1. A simple example with $r_0 = 75, r_1 = 21$ is

$$\begin{aligned} 75 &= 3 \cdot 21 + 12, \\ 21 &= 1 \cdot 12 + 9, \\ 12 &= 1 \cdot 9 + 3, \\ 9 &= 3 \cdot \mathbf{3} + 0. \end{aligned}$$

So we have $\gcd(75,21)=3$. In the same manner as in (21) we can write

$$r = \frac{75}{21} = 3 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{3}$$

and we notice that the parts $3, 3+\frac{1}{1}=4, 3+\frac{1}{1+}\,\frac{1}{1}=\frac{7}{2}$ are approximations of $75/21$ with strictly decreasing error.

The remaining question is how to approximate an irrational number. As a starting point we again look at Euclid's division algorithm (20) for integers, define

$$\rho_j := \frac{r_j}{r_{j+1}}, \quad j = 0, 1, \ldots, k$$

and observe that

$$\rho_j := q_j + \frac{1}{\rho_{j+1}},\ j = 0, 1, \ldots, k-1, \quad \rho_k := q_k \tag{29}$$

which results in the same form as (21) with $q_k > 1$. Now, we may write the foregoing sequence (29) and (20) equivalently by

$$q_j := \lfloor \rho_j \rfloor, \quad \frac{1}{\rho_{j+1}} = \rho_j - \lfloor \rho_j \rfloor, \quad j = 0, 1, \ldots, \tag{30}$$

where $\lfloor \xi \rfloor$ for any real ξ defines the greatest integer not exceeding ξ ($\lfloor\ \rfloor$ is also called floor). This is the key for finding a continued fraction for an irrational number ξ. Let $\xi > 0$ and define according to (30)

$$\begin{aligned} &\rho_0 := \xi, \\ &q_j := \lfloor \rho_j \rfloor, \quad \rho_{j+1} := \frac{1}{\rho_j - q_j}, \quad j = 0, 1, \ldots \end{aligned} \tag{31}$$

This process will not terminate and produce infinitely many integers $q_j, j \geq 0$ and defines the infinite continued fraction

$$\xi = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_j+}\cdots$$

And one can indeed show that the sequence of finite subfractions converges to ξ, Henrici [1977, p. 492]. The algorithm (31) is easy to implement. However, there are some numerical difficulties, in particular, in forming $q_j := \lfloor \rho_j \rfloor$ when the computed ρ_j is a little less than an integer. In this case, q_j may differ by one from the correct value. We have already seen, that such a continued fraction should be evaluated with the Euler-Wallis formula (25) which gives the subfractions $\frac{A_j}{B_j}$ defined in (24), but the algorithm (31) also gives the tail of the continued fraction, namely

$$\rho_j := q_j + \frac{1}{q_{j+1}+} \; \frac{1}{q_{j+2}+} \cdots, \quad j = 0, 1, \ldots \tag{32}$$

There is the following formula (Henrici [1977, p. 491]) which relates the subfractions $\frac{A_j}{B_j}$ and the tails ρ_j in the form

$$\xi = \frac{A_{j-1} + A_j \rho_{j+1}}{B_{j-1} + B_j \rho_{j+1}}, \quad j = 1, 2, \ldots \tag{33}$$

The following theorem is straightforward.

Theorem 15. *A real number is rational if and only if the corresponding continued fraction terminates.*

It turns out that the square roots have surprising continued fractions. Any real zero of a quadratic polynomial with integer coefficients will be called an algebraic number of degree two. For the proof (not so easy) of the following theorem we refer to Henrici [1977, p. 495/496].

Theorem 16. *(Lagrange) An irrational number is an algebraic number of degree two if and only if its continued fraction is periodic.*

Example 17.

$$\begin{aligned}
\frac{1+\sqrt{5}}{2} &= 1 + \frac{1}{1+} \; \frac{1}{1+} \cdots, \\
\sqrt{2} &= 1 + \frac{1}{2+} \; \frac{1}{2+} \cdots, \\
\sqrt{3} &= 1 + \frac{1}{1+} \; \frac{1}{2+} \; \frac{1}{1+} \; \frac{1}{2+} \; \frac{1}{1+} \cdots, \\
2 + \sqrt{7} &= 4 + \frac{1}{1+} \; \frac{1}{1+} \; \frac{1}{1+} \; \frac{1}{4+} \; \frac{1}{1+} \; \frac{1}{1+} \; \frac{1}{1+} \cdots
\end{aligned}$$

If we look at the examples, we see little differences. In the first and last example the period starts immediately in the beginning of the expansion, whereas in the other two examples the period starts at a later stage. We call a periodic infinite continued fraction purely periodic if the period starts already with the first term $q_0 > 0$. Let p be a quadratic polynomial with integer coefficients. If the two zeros ξ, ξ' of p are real then they are called algebraically conjugate to each other. The following characterization of irrationals with purely periodic continued fractions is far from being trivial.

Theorem 18. *Let ξ be an irrational, algebraic number of degree two. The continued fraction of ξ is purely periodic if and only if $\xi > 1$ and the algebraic conjugate satisfies $-1 < \xi' < 0$. Let ξ be purely periodic and η be defined by the purely periodic continued fraction where the period of ξ is reversed. Then, $\eta = -1/\xi'$.*

Example 19. Let $\xi := 2 + \sqrt{7}$ whose continued fraction is given in the last example. Its period is $4, 1, 1, 1, \ldots$ Then $\xi' = 2 - \sqrt{7} \approx -0.65$ and the above Theorem 18 implies

$$\eta = -1/\xi' = \frac{1}{\sqrt{7}-2} = \frac{2+\sqrt{7}}{3} = 1 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4+}\cdots$$

§4. The solutions of Pell's equation by continued fractions

The only book giving a connection between Pell's equation and continued fractions is (apparently[3)]) the book by Henrici [1977]. We start with a simpler equation, namely the linear equation

$$lx - my = 1, \quad l, m \in \mathbb{N} \tag{34}$$

to be solved in integers $x, y \in \mathbb{Z}$ by means of continued fractions. We assume that $\gcd(l, m) = 1$. Let

$$\frac{l}{m} = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\,\cdots\,\frac{1}{q_k}. \tag{35}$$

[3)] see the Addendum in the end

Assume, we know two distinct solutions $(x_0, y_0), (x_1, y_1)$ of (34), then $l(x_1 - x_0) - m(y_1 - y_0) = 0$, and

$$\frac{l}{m} = \frac{y_1 - y_0}{x_1 - x_0}.$$

Since $\gcd(l, m) = 1$, we have for some integer j

$$y_1 = y_0 + jl; \quad x_1 = x_0 + jm.$$

Conversely, any such (x_1, y_1) is a solution and hence the general solution is

$$(x, y) := (x_0, y_0) + j(m, l), \quad j \in \mathbb{Z}.$$

The remaining question is, how to find an initial solution (x_0, y_0). Let us denote by

$$\frac{q_0}{1} =: \frac{A_0}{B_0}, \frac{A_1}{B_1}, \ldots, \frac{A_k}{B_k} := \frac{l}{m}$$

the sequence of fractions defined by (35) and to be computed by (25). From (26) we have $A_j B_{j-1} - A_{j-1} B_j = (-1)^{j+1}, j = 0, 1, \ldots, k$ since all $c_j = 1$. If k happens to be odd, then $A_k = l, B_k = m$ and $lB_{k-1} - A_{k-1} m = 1$ and

$$(x_0, y_0) := (B_{k-1}, A_{k-1})$$

is a solution. If k is even, then one defines

$$(x_0, y_0) := (m - B_{k-1}, l - A_{k-1}).$$

Since $lx_0 - my_0 = l(m - B_{k-1}) - m(l - A_{k-1}) = -lB_{k-1} + mA_{k-1} = 1$, (x_0, y_0) is again a solution.

Example 20. Let us treat

$$75x - 58y = 1.$$

The corresponding continued fraction is

$$\frac{75}{58} = 1 + \frac{1}{3+}\,\frac{1}{2+}\,\frac{1}{2+}\,\frac{1}{3}$$

and the subfractions are

j	0	1	2	3	4
A_j	1	4	9	22	75
B_j	1	3	7	17	58

Since $k = 4$ is even, the general solution is

$$(x, y) = (41, 53) + j(58, 75), \quad j \in \mathbb{Z},$$

where $41 = 58 - 17,\ 53 = 75 - 22$.

Let us finally turn to Pell's equation. If we assume that D in (16), (17) is negative and a multiple of four, then the two types of Pell's equation can be written as

$$\text{(36)} \qquad \text{(a)} \quad y^2 - lx^2 = 1, \quad \text{(b)} \quad y^2 - lx^2 = -1, \quad l \in \mathbb{N}, \quad \sqrt{l} \notin \mathbb{N}.$$

The irrational number $\xi := \sqrt{l}$ will not have a purely periodic continued fraction, since $\xi' := -\sqrt{l} < -1$ does not satisfy the conditions mentioned in Theorem 18. However,

$$\xi := \lfloor\sqrt{l}\rfloor + \sqrt{l} > 1$$

has a purely periodic continued fraction for all natural l which are not squares since $-1 < \lfloor\sqrt{l}\rfloor - \sqrt{l} < 0$. Now let $l > 1$ be an integer, but not a square and let

$$\text{(37)} \quad \tilde{\xi} := \lfloor\sqrt{l}\rfloor + \sqrt{l} = 2q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_k+}\quad\frac{1}{2q_0+}\,\frac{1}{q_1+}\cdots\frac{1}{q_k+}\quad\frac{1}{2q_0+}\cdots$$

The integer part of $\tilde{\xi}$ is always even, therefore, the continued fraction of $\tilde{\xi}$ starts with $2q_0$. Since $q_0 = \lfloor\sqrt{l}\rfloor$, we obtain an expansion for $\xi := \sqrt{l}$ by subtracting q_0 from both sides of (37):

$$\text{(38)} \qquad \xi := \sqrt{l} = q_0 + \frac{1}{q_1+}\,\frac{1}{q_2+}\cdots\frac{1}{q_k+}\quad\frac{1}{2q_0+}\,\frac{1}{q_1+}\cdots\frac{1}{q_k+}\quad\frac{1}{2q_0+}\cdots$$

The period of $\xi = \sqrt{l}$ is $q_1, q_2, \ldots, q_k, 2q_0$. Its length is $k+1$. Now let the subfractions of the expansion for $\xi = \sqrt{l}$ ending with q_k be

$$\frac{A_k}{B_k}, \frac{A_{2k+1}}{B_{2k+1}}, \frac{A_{3k+2}}{B_{3k+2}}, \ldots$$

For all tails of ξ starting with $2q_0$ we have

$$\rho_{s(k+1)} = \lfloor\sqrt{l}\rfloor + \sqrt{l}, \quad s = 1, 2, \ldots.$$

If we apply the formula (33) for $j = sk + s - 1$, $s = 1, 2\ldots$ we obtain

$$\xi = \sqrt{l} = \frac{A_{j-1} + A_j(\lfloor\sqrt{l}\rfloor + \sqrt{l})}{B_{j-1} + B_j(\lfloor\sqrt{l}\rfloor + \sqrt{l})}, \quad j = sk + s - 1,\ s = 1, 2\ldots$$

If we multiply this equation with the denominator we obtain after some rearrangement

(39) $\sqrt{l}\{B_{j-1}+B_j q_0-A_j\} = \{A_{j-1}+A_j q_0-lB_j\}, \quad j = sk+s-1, s = 1,2\ldots$

Since the numbers enclosed in $\{\ \ \}$ are integers, both sides of this equation must be zero. Hence, $A_{j-1} = lB_j - A_j q_0$, $B_{j-1} = A_j - B_j q_0$. Now, we use the former result (26) related to the Euler-Wallis formula and obtain

(40)
$$(-1)^{j+1} = A_j B_{j-1} - B_j A_{j-1} = A_j(A_j - B_j q_0) - B_j(lB_j - A_j q_0) = A_j^2 - lB_j^2.$$

Since j is subjected to (39) we obtain finally the following theorem.

Theorem 21. *Let Pell's equation (36) be given and let $\sqrt{l}$ have the continued fraction given in (38). (a) Let k be even. Then $(x,y) := (B_j, A_j)$ solves $y^2 - lx^2 = -1$ for $j = sk+s-1, s = 1,3,5,\ldots$ and it solves $y^2 - lx^2 = 1$ for $j = sk+s-1, s = 2,4,6,\ldots$ (b) Let k be odd. Then $y^2 - lx^2 = -1$ has no solution and (B_j, A_j) solves $y^2 - lx^2 = 1$ for $j = sk+s-1, s = 1,2,3,\ldots$*

Proof: Subject to $j = sk+s-1$, $s = 1,2\ldots$ one has to distinguish between even and odd j in equation (40). If k is odd, then all possible j are odd and $(-1)^{j+1} = 1$. $\square$

Example 22. 1. Let $l := 2$ in Pell's equation. According to Example 17 we have

$$\sqrt{2} = q_0 + \frac{1}{2q_0+}\,\frac{1}{2q_0+}\,\cdots, \quad q_0 = 1.$$

Thus, the relevant $k = 0$ is even and according to (a) of Theorem 21 $(x,y) := (B_{2j}, A_{2j})$ solve $y^2 - lx^2 = -1$ and (B_{2j+1}, A_{2j+1}) solve $y^2 - lx^2 = 1, j = 0,1,\ldots$ The first subfractions of $\sqrt{2}$ are given in Table 23.

Table 23. Solutions of Pell's equation $y^2 - 2x^2 = -1$, marked in boldface and of $y^2 - 2x^2 = 1$

j	A_j	B_j
0	**1**	**1**
1	3	2
2	**7**	**5**
3	17	12
4	**41**	**29**
5	99	70

j	A_j	B_j
6	**239**	**169**
7	577	408
8	**1 393**	**985**
9	3 363	2 378
10	**8 119**	**5 741**
11	19 601	13 860

2. Let $l := 11$ in Pell's equation. We find by applying algorithm (31)

$$\sqrt{11} = q_0 + \frac{1}{q_1+} \quad \frac{1}{2q_0+} \frac{1}{q_1+} \cdots, \qquad q_0 = q_1 = 3.$$

Thus, the relevant $k = 1$ is odd and according to (b) of Theorem 21 $(x, y) := (B_{2j+1}, A_{2j+1})$, $j = 0, 1, \ldots$ solve $y^2 - lx^2 = 1$ and $y^2 - lx^2 = -1$ has no solution. The first subfractions of $\sqrt{11}$ are given in Table 24.

Table 24. Solutions of Pell's equation $y^2 - 11x^2 = 1$, marked in boldface

j	A_j	B_j
0	3	1
1	**10**	**3**
2	63	19
3	**199**	**60**
4	1 257	379
5	**3 970**	**1 197**
6	25 077	7 561
7	**79 201**	**23 880**
8	500 283	150 841
9	**1 580 050**	**476 403**

Both types (36), (a) and (b) of Pell's equation can be solved by means of continued fractions only if the length $k + 1$ of the period is odd. This happens for $\sqrt{2}, \sqrt{5}, \sqrt{10}, \sqrt{13}, \sqrt{17}, \ldots$ For the cases $\sqrt{3}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{11}, \sqrt{12}, \sqrt{14}, \sqrt{15}, \ldots$ we can only solve type (a) of Pell's equation (36) by means of continued fractions. Type (b) has no solution. In particular, the starting equation (1) with $l = 2$ is included in this list given in Table 23. The algebraic Lemma 8 is void, if $y^2 - lx^2 = -1$ has no positive solutions. In this case the algebraic theory does not furnish solutions for $y^2 - lx^2 = 1$, whereas the continued fraction of $\sqrt{l}$ also finds the solutions in this case.

It should be pointed out, that Henrici [1977, p. 499] only looks for one solution of $y^2 - lx^2 = 1$. The equation $y^2 - lx^2 = -1$ is not treated.

§5. A calendarian peculiarity of the number 50

The length of the year is based on the length of the so-called tropical year which has the length of 365.2422 days. Years which are divisible by 100 are called secular years. In order to make the years having almost the right length Pope Gregor XIII introduced in 1582 the new rule (Gregorian calendar) that the leap years introduced already by Julius Cäsar (46 B.C.) (Julian calendar) were abandoned in the secular years with the exception of those secular years which are divisible by 400. This gives the year an average length of 365.2425 days. In addition, in order to make up for the errors in the Julian calendar the 10 days from the 5th to the 14th of October 1582 were skipped when introducing the Gregorian calendar. Many more details can be found in encyclopedias, e. g. in dtv-Lexikon [1999, vol. 9] or in `http://www.salesianer.de/util/kalender.html` where the latter web page also allows calculations.

The above rules make it difficult to find the exact length of a longer period, whose endpoints are given by calendar dates. For this reason the astronomers have developed a program where all days of a rather long period are just numbered by natural numbers.

In many cases a person who turns 50, observes that the weekday of his/her 50th birthday is the same as the weekday of his/her birth. Thus, we compute the length of 50 years in days in order to see how probable the above observation is. If we make only a rough calculation, 50 years consist of $50 \cdot 365$ days plus a number l of leap days in the period from the birth to the 50th birthday.

Definition 25. By the period of one year we understand a time period starting with any calendar date and ending with the date one day prior to the same date the next year. Correspondingly, a period of $n \in \mathbb{N}$ years is defined.

Some examples: If a one year period starts with March 1, then it ends either with February 28 or February 29 the next year if this day exists. If the one year period starts with February 29, it ends with February 28 the next year. If it starts with January 1 it ends with December 31 the same year.

Lemma 26. *The number l of leap days in any period of 50 years is $l = 11$, $l = 12$, or $l = 13$.*

Proof: There are two cases:

(a) The period of 50 years covers no year divisible by 4 which is not a leap year,

(b) The period of 50 years covers exactly one year divisible by 4 which is not a leap year (e. g. 1900).

We partition the period of 50 years into 12 groups of four consecutive years and in one group of the last two years. In case (a) we have $l = 12$ or $l = 13$. The case $l = 13$ occurs only if in the group of the last two years there is one additional leap day. In case (b) there is one leap year less, so we have $l = 11$ or $l = 12$. □

From the lemma it follows that the number of days in any period of 50 years varies from 18261 to 18263 and the remainder modulo seven is $5, 6, 0$, respectively. So, in the case of $l = 13$, the weekdays at the birth and at the 50th birthday are the same. In the case of $l = 12$ the weekday of the birth is one day later than the weekday on the 50th birthday.

Example 27. Let us compute the number of leap days of a period of 50 years which starts at October 22, 1954 and ends at October 21, 2004. According to the above lemma (and its proof) this period belongs to case (a) since the year 2000 is a leap year. Therefore, the first 48 years cover 12 leap days and in the period of October 22, 2002 to October 21, 2004 there is one additional leap day, namely February 29, 2004. Thus, the total number of leap days is $l = 13$ and October 22, 1954 and October 22, 2004 have the same weekday (Friday). If we start the 50 year period with February 28, 1954, then the number of leap days is $l = 12$, since in the period of the last two years, February 28, 2002 to February 27, 2004, we miss the leap day in 2004. And the weekday on February 28, 1954 is one day later than that on February 28, 2004 (Saturday).

The remaining question is, what is the probability for the three numbers 11, 12, 13 occurring in Lemma 26. The answer depends on the time period in which one puts the 50 year periods. For two time periods, we have made a simple count. If we count over long periods (the 50 year period starts in year 1 to year 10000 on January 1) then our count results in the three probabilities 0.180, 0.515, 0.305, for $l = 11$, $l = 12$, or $l = 13$ leap days, respectiveley. This is also the asymptotic value for longer periods[4)]. For 50 year periods starting in the 200 years 1910 to 2109 the corresponding probabilities for $l = 11$, $l = 12$, $l = 13$ are 0.12, 0.51, 0.37.

Acknowledgments. The author thanks Gerhard Tischel, Schriftleitung of the Mitteilungen der Mathematischen Gesellschaft in Hamburg for his TEXnical support. The author also thanks Professor Ron Guenther, Oregon State University, Corvallis, Oregon, USA, for reading this text resulting in many improvements.

4) In all cases we have assumed the validity of the Gregorian calendar. However, for very long astronomical periods this is still not good enough. The tropical year and the year set by the Gregorian calendar will differ by one day in $1/(365.2425 - 365.2422) = 3333$ years. A remedy would be to cancel the leap days in the years 4916, 8248, etc.

Addendum

In the beginning of §4 we wrote that the quoted book by HENRICI is (apparently) the only one solving Pell's equation with continued fractions. This is of course not true. Henrici himself mentioned two sources: HARDY & WRIGHT [3rd ed. 1954] and DAVENPORT [1st ed. 1952]. The book by DAVENPORT is in print now for over 50 years. It exists in its 7th edition, 1999, and it provides numerical examples to almost all topics treated. It also contains a very readable overview on Pell' equation and even contains a list of all continued fractions for $\sqrt{l}$ with $l \leq 50$. It is not so difficult to recompute these fractions with `matlab`. However, one will run into difficulties if one uses `matlab` for larger l, say $l > 100$. Problems arise if the length of the period of the continued fraction for $\sqrt{l}$ is long, say 15 or larger. The longest period for all $l \leq 99$ appears for $l = 94$ where the length of the period is 16. For $l = 166$ the period has length 22 which is the longest for all $l \leq 200$. Solutions of type (a) of Pell's equation for $l \leq 102$ can be found in WEISSTEIN [1999]. Sources for tables for continued fractions and for solutions of Pell's equations are given by PERRON [1954, p. 90 & 95]. In PERRON [1954, p. 91] one also finds a table with all continued fractions for $\sqrt{l}$ for $2 \leq l \leq 99$. In LEGENDRE [1893, p. 430], there is a table for all smallest solutions of the two equations $y^2 - lx^2 = \pm 1$ for $2 \leq l \leq 1003$.

Pell's equation is related to the so-called *cattle problem* which is described in a poem by Archimedes (ca. 285 – ca. 212 BC). More information and an English translation (by Ivor Thomas, Cambridge, MA, 1941) can be found under `https://www.cs.drexel.edu/~crorres/Archimedes/Cattle/Statement.html`. More details in the quoted web page. The English version reads:

If thou art diligent and wise, O stranger, compute the number of cattle of the Sun, who once upon a time grazed on the fields of the Thrinacian isle of Sicily, divided into four herds of different colours, one milk white, another a glossy black, a third yellow and the last dappled. In each herd were bulls, mighty in number according to these proportions: Understand, stranger, that the white bulls were equal to a half and a third of the black together with the whole of the yellow, while the black were equal to the fourth part of the dappled and a fifth, together with, once more, the whole of the yellow. Observe further that the remaining bulls, the dappled, were equal to a sixth part of the white and a seventh, together with all of the yellow. These were the proportions of the cows: The white were precisely equal to the third part and a fourth of the whole herd of the black; while the black were equal to the fourth part once *more of the dappled and with it a fifth part, when all, including the bulls, went to pasture together. Now the dappled in four parts were equal in number to a fifth part and a sixth of the yellow herd. Finally the yellow were in number equal to a sixth part and a seventh of the white herd. If thou canst accurately tell, O stranger, the number of cattle of the Sun, giving separately the number of well-fed bulls and again the number of females according to each colour, thou wouldst not be called unskilled or ignorant of numbers, but not yet shalt thou be numbered among the wise.*

But come, understand also all these conditions regarding the cattle of the Sun. When the white bulls mingled their number with the black, they stood firm, equal in depth and breadth, and the plains of Thrinacia, stretching far in all ways, were filled with their multitude. Again, when the yellow and the dappled bulls were gathered into one herd they stood in such a manner that their number, beginning from one, grew slowly greater till it completed a triangular figure, there being no bulls of other colours in their midst nor none of them lacking. If thou art able, O stranger, to find out all these things and gather them together in your mind, giving all the relations, thou shalt depart crowned with glory and knowing that thou hast been adjudged perfect in this species of wisdom.

In these pages, quoted above, one finds the solution of step 1, the linear part, very detailed. The total number T of all cattle is $T := t \cdot k$ for any $k \in \mathbb{N}$, where $t := 50\,389\,082$. However, the second part lacks some details. It stops with the mathematical description of the line in the second part starting with *Again, when the yellow and the dappled bulls ... till it completed a triangular figure,...* which is mathematically modelled as

$$ar^2 = \frac{m(m+1)}{2} \tag{41}$$

where the reported value of $2a$ is $2a := 4\,729\,494 \cdot 4\,657^2$. The final problem is to find r, m which satisfy (41). No indication is given on that web page on how to do that. However, only school mathematics is necessary, to see that this equation is equivalent to Pell's equation of the form

$$y^2 - 2aX^2 = 1, \tag{42}$$

where $y := 2m + 1$ and $X := 2r$. Of interest for the solution is eventually the number $k := \tau \cdot r^2$ where $\tau := 4\,456\,749$ since all wanted eight numbers (of white bulls, white cows, etc.) are known multiples of k. From this number we deduce the total number of cattle as $T = t \cdot \tau \cdot r^2 = t \cdot \tau \cdot (\frac{X}{2})^2$, where X solves (42).

We will make a short excursion to the question on how to reduce Pell's equation with a large L to Pell's equation with a smaller l. This will always work if the large L contains a square factor, λ^2, $\lambda \in \mathbb{N}$. Hence, assume that $L = \lambda^2 l$ for some $\lambda, l \in \mathbb{N}, \lambda, l \geq 2$. In this case we write $y^2 - LX^2 = y^2 - \lambda^2 l X^2 = y^2 - lx^2$, where $x := \lambda X$. So we have two problems: The original one:
(i) $y^2 - LX^2 = 1$, and the new one (ii) $y^2 - lx^2 = 1$. Both have infinitely many solutions. If $\{(X, y)\}$ denotes the set of all solutions of (i), then $\{(\lambda X, y)\}$ will be contained in the set of all solutions $\{(x, y)\}$ of (ii). If, on the other hand, (x, y) is any solution of (ii) such that x is a multiple of λ, then $(X, y) := (x/\lambda, y)$ is a solution of (i). Thus, solving (ii), is sufficient to solve (i). Let us treat a little example with $L := 50 = 5^2 l$ and $l = 2$. Solutions (x, y) of $y^2 - 2x^2 = 1$ are listed in Table 23. The first solution of (ii) where x is a multiple of $\lambda = 5$ is $(x, y) = (70, 99)$, thus, $(X, y) = (14, 99)$ is a solution of equation (i). The second such solution of (ii) where x is a multiple of $\lambda = 5$ is $(x, y) = (13860, 19601)$ implying that $(X, y) := (x/5, y) = (2772, y)$ is another solution of (i). Since this can be done with any l and any λ the following lemma must be true.

Lemma 28. *Let l, λ be positive integers, where l is not a square and $\lambda \geq 2$. Denote by $\{(x_j, y_j)\}$, $j = 0, 1, \ldots$ the sequence of all solutions of $y^2 - lx^2 = 1$. Then, there is a first j_0 such that x_{j_0} is a multiple of λ and (X_{j_0}, y_{j_0}) solves $y^2 - LX^2 = 1$, where $L = \lambda^2 l$ and $X_{j_0} := x_{j_0}/\lambda$.*

According to the previous investigation applied to the cattle problem, it is sufficient to solve

$$y^2 - 4\,729\,494 x^2 = 1, \tag{43}$$

where this equation is mentioned by Davenport [1992, p. 107]. Even with a conventional home computer of nowadays problems of this size can be solved in a few seconds. The smallest solution of (43) is $(x, y) := (5.055...340 \cdot 10^{40}, 1.099...049 \cdot 10^{44})$ and the length of the period of the continued fraction of $\sqrt{4\,729\,494}$ is 92. In order to solve the original problem one has to find a solution (x, y) of (43) such that $X := x/4\,657 \in \mathbb{N}$. This is also within the scope of home computers though the computing time for this search may take several hours. Solution no. 2329 is the smallest solution (x, y) of (43) such that x is divisible by $4\,657$. And we find $x = 1731 \ldots 5860$ where x has altogether

103 270 decimal places and $X := x/4657 = 3717\ldots6980$ which has 103 266 decimal places. The resulting k is $k = 1540\ldots4900$ with altogether 206 538 decimal places. And the total number T of cattle is $T = 7760\ldots1800$ which has 206 545 decimal places. We recomputed this solution with a `bc` (*basic computer*) program, which is available for free at all unix and linux stations including macs with operating system OS X.

According to the given web page, the Greek text of Archimedes was edited for the first time in modern times by Gotthold Ephraim Lessing (1773). It can be found on the quoted web page. A complete German translation seems to be lacking. This was confirmed independently by Dr. Helmut Berthold, Wolfenbüttel, and Dr. Christos Fakas, Hamburg.

References

M. Abramowitz & I. A. Stegun (eds.), Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, National Bureau of Standards, Applied Mathematical Series, 55, U.S. Government Printing Office, Washington, D.C. 1964, Seventh Printing 1968.

G. A. Baker, Jr., Essentials of Padé Approximants, Academic Press, New York, 1975, 306 p.

G. A. Baker, Jr., P. Graves-Morris, Padé Approximants, Vol. I: Basic Theory, Addison Wesley, Reading, Mass., 1981, 325 p.

P. Bethge, Tanz der Variablen, Der Spiegel, 27/1.7.2002, p.134–136.

C. Brezinski, History of Continued Fractions and Padé Approximants, Springer, Berlin, 1991, 551 p.

E. Catalan, Note extraite d'une lettre adressé à l'éditeur, J. reine angew. Math. **27** (1844), p. 192.

H. Davenport, The Higher Arithmetic, 1st ed. Hutchinson, 1952, 6th ed. Cambridge University Press, 1992, 217 p., 7th ed. Cambridge University Press, 1999.

dtv-Lexikon in 20 Bänden, Deutscher Taschenbuch Verlag, München, 1999.

S. Gottwald, H.-J. Ilgauds, & K.-H. Schlote (eds.), Lexikon bedeutender Mathematiker, Harri Deutsch, Thun, Frankfurt (M.), 1990, 504 p.

G. H. Hardy & E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., Oxford University Press, 1960, 421 p.

P. Henrici, Applied and Computaional Complex Analysis, Vol. 2, Special Functions - Integral Transforms - Asymptotics - Continued fractions, Wiley, New York, 1977, 662 p.

A.-M. Legendre, Zahlentheorie, 1. Band, nach der dritten Auflage übersetzt von H. Maser, Teubner, Stuttgart, 1893, 442 p.

M. S. Mahoney, The Mathematical Career of Pierre de Fermat 1601–65, Princeton University Press, Princeton, N. J., 1973, 419 p.

T. Metsänkylä, Catalan's Conjecture: Another old diophantine problem solved, Bull. Amer. Math. Soc. (N. S.), **41** (2004), p. 43–57.

P. Mihăilescu, Primary Cyclotomic Units and a Proof of Catalan's Conjecture, J. reine angew. Math. **572** (2004), 167–195.

L. J. Mordell, Diophantine Equations, Academic Press, London, New York, 1969, 312 p.

G. Opfer, Numerische Mathematik für Anfänger, 4. Aufl., Vieweg, Braunschweig, 2002, 357 p.

G. Opfer & W. Ripken, Complex Version of Catalan's Problem, Mitt. Math. Ges. Hamburg, **17** (1998), p. 101–112.

O. Perron, Die Lehre von den Kettenbrüchen, Band I, 3. Aufl., Teubner, Stuttgart, 1954, 194 p.

A. Scholz & B. Schoeneberg, Einführung in die Zahlentheorie. Sammlung Göschen, Band 1131, Walter de Gruyter, Berlin 1961, 126 p.

Schülke (bearbeitet von W. Dreetz), Schülkes Tafeln vierstelliger Logarithmen, Funktions- und Zahlenwerte, 45. Aufl., Teubner, Stuttgart, 1959, 44 S., first published 1895.

S. Singh, Fermat's Last Theorem, Fourth Estate, London, 1997, 362 p.

S. Singh, Fermats letzter Satz, die abenteuerliche Geschichte eines mathematischen Rätsels, Carl Hanser Verlag, München-Wien, 1998, 364 p.

E. W. Weisstein, Pell Equation. From *MathWorld*–A Wolfram Web Resource. `http://mathworld.wolfram.com/PellEquation.html`, 1999.

Author's address:

Gerhard Opfer
University of Hamburg
MIN Faculty, Section of Mathematics
Center of Optimization and Approximation
Bundesstr. 55
20146 Hamburg, Germany
e-mail: `opfer@math.uni-hamburg.de`