Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 56 (2001)

Artikel: Characterization of regular Diophantine quadruples
Autor: Assaf, Eran / Gueron, Shay
DOI: https://doi.org/10.5169/seals-6673

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 01.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Elem. Math. 56 (2001) 71 – 81
0013-6018/01/020071-11 $ 1.50+0.20/0

© Birkhäuser Verlag, Basel, 2001

Elemente der Mathematik

Characterization of regular Diophantine quadruples

Eran Assaf and Shay Gueron

Shay Gueron is a faculty member of the department of mathematics at the University of Haifa, Israel. His research interests are in applied mathematics (mathematical biology, and computations). He is also interested in problem solving and mathematical competitions, and has been the Israeli Team Leader for the International Mathematical Olympiad since 1994.

Eran Assaf, a student of Shay Gueron, studies in a special gifted students' enrichment program. He was a member of the Israeli team for the International Mathematical Olympiad, in the year 2000.

1 Introduction

A set S of positive integers is said to have a Diophantine property, and called a *Diophantine set*, if $xy+1$ is a perfect square for any $x \neq y \in S$. The task of finding integer Diophantine quadruples $\{a,b,c,d\}$, where $a<b<c<d$, involves several open problems.

An integer Diophantine quadruple $\{a,b,c,d\}$ is called *regular* if $(a+b-c-d)^2 = 4(ab+1)(cd+1)$. No non-regular Diophantine quadruple has been found, and it has been conjectured that all Diophantine quadruples are regular.

In this paper we solve the following problem:

Problem. Characterize the regular Diophantine quadruples of the form $\{1,b,c,d\}$, with positive integers $1<b<c<d$, and give an algorithm for constructing them.

Das Lösen diophantischer Probleme stellt immer eine besondere Herausforderung dar. So verhält es sich zum Beipsiel auch mit der Frage nach dem Auffinden sogenannter diophantischer Mengen. Dies sind Mengen S natürlicher Zahlen mit der Eigenschaft, dass $x \cdot y + 1$ für alle $x, y \in S$, $x \neq y$, eine Quadratzahl ist. Soll S jeweils nur zwei natürliche Zahlen enthalten, so erkennen wir beispielsweise sofort die Paare $\{n-1, n+1\}$, wobei n eine positive natürliche Zahl ist, als zweielementige diophantische Mengen. Im nachfolgenden Beitrag erhalten wir nun Auskunft über das Auffinden diophantischer Mengen, welche jeweils aus vier Elementen bestehen sollen. *jk*

2 A brief historical account

The Diophantine problem was originally posed by Diophantus (3rd century [3]) and reads: find four *rational* numbers $\{r_1, r_2, r_3, r_4\}$ such that $r_i r_j + 1$ is the square of a rational number for any $1 \le i \ne j \le 4$. Diophantus provided the example $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$.

Fermat (17th century) dealt with integer Diophantine quadruples. He asked whether a fifth integer can be added to the Diophantine quadruple $\{1, 3, 8, 120\}$ and make it a Diophantine 5-tuple. The answer to this problem is still unknown. Furthermore, no Diophantine 5-tuple has ever been found, and nobody has proved that such 5-tuples do not exist. On the other hand, it is known that there are infinitely many Diophantine quadruples, and it was probably Euler (18th century) who first demonstrated this by looking at the family of quadruples

$$\{a,\ b,\ a+b+2\sqrt{ab+1},\ 4(a+\sqrt{ab+1})(b+\sqrt{ab+1})\sqrt{ab+1}\} \tag{1}$$

for a and b such that $ab+1$ is a perfect square. Special cases of Euler's solution yield several interesting infinite sub-families of Diophantine quadruples. Two examples are

$$\{F_{2n}, F_{2n+2}, F_{2n+4}, 4F_{2n+1}F_{2n+2}F_{2n+3}\} \tag{2}$$

where F_n ($F_1 = F_2 = 1$) denotes the n-th Fibonacci number (see [5]), and the infinite family $\{n, n+2, 4n+4, 4(n+1)(2n+1)(2n+3)\}$.

It is interesting to point out that although there are infinitely many Diophantine quadruples, no algorithm for *generating all of them* has been found. For more details see [13, 4].

Upgrading a Diophantine triplet

The problem of upgrading a Diophantine triplet deals with searching (all the) integers d that can be added to a given Diophantine triplet $\{a, b, c\}$ ($a < b < c$) and make it a Diophantine quadruple with $a < b < c < d$. This problem is still unsolved, and only a few partial results, on which we report here, have been established.

Upgrading a triplet is always possible. Upgrading a given Diophantine triplet $\{a, b, c\}$ is always possible. One way, proposed by Montgomery (see [4]), is to choose

$$d = d_+ = a + b + c + 2abc + 2\sqrt{(ab+1)(ac+1)(bc+1)} > c\,. \tag{3}$$

Note that the value $d_- = a + b + c + 2abc - 2\sqrt{(ab+1)(ac+1)(bc+1)}$ also gives a Diophantine quadruple but $d_- < c$. Although it has not been proved that d_+ is the only upgrading possibility, nobody has found a quadruple for which $a < b < c < d$ and $d \ne d_+$.

Unique upgrading. There are only few examples where a certain value of d can be shown to be the only possible upgrading value.

Davenport and Baker (1969, [2]) proved that 120 is the only integer that upgrades the triplet $\{1, 3, 8\}$. The proof of this result is not elementary. The problem can be reduced

to finding a solution to the system of Pell equations $3x^2 - 2 = y^2$, and $8x^2 - 7 = z^2$. Using Baker's theorem on linear forms in the logarithms of algebraic numbers, it can be shown that this system has only finitely many solutions, an upper bound can be fixed, and numerical verification shows that 120 is the only one greater than 8.

Analogously, Veluppillai (1980, [11]) showed that 420 is the only fourth integer that upgrades the Diophantine triplet $\{2, 4, 12\}$. This was done by reducing the problem to that of solving the system of Pell equations $z^2 - 3y^2 = -2$, $z^2 - 6x^2 = -5$.

The problem of regular Diophantine quadruples

A quadruple of integers $\{a, b, c, d\}$ is called *regular* if it satisfies the quadratic relation $(a + b - c - d)^2 = 4(ab + 1)(cd + 1)$. Such quadruples turn out to have various special properties (see [13, 4]).

Gibbs [4] proved that the value d_+ in (3) is the *only* fourth integer that upgrades the Diophantine triplet $\{a, b, c\}$ to a *regular* Diophantine quadruple.

A non-regular quadruple has never been found and Gibbs, Arkin, Hoggatt and Strauss conjectured that all the Diophantine quadruples are regular (see [4]). This conjecture is still open.

In this paper we solve the problem of finding all regular Diophantine quadruples of the form $\{1, b, c, d\}$, where $1 < b < c < d$. We characterize quadruples and provide two algorithms for generating all of them.

We shall use hereafter some well-known facts about Pell equations. To make the paper self contained, we provide a brief summary of facts, concerning the unit Pell equation, in the Appendix. We also include a paragraph describing how the general case can be treated when solutions exist.

3 An infinite family of regular Diophantine quadruples

We start with constructing one infinite family of regular Diophantine quadruples of the form $\{1, b, c, d\}$, where $1 < b < c < d$.

We write $b = m^2 - 1$ for some $2 \leq m \in N$. To generate the next number, c, we observe that c must be of the form $c = t^2 - 1$ for some $t = t_m = t(m)$ such that $3 \leq t_m \in N$ ($t \geq 3$ because for $t = 2$ we have $b > c$). Further, we must have

$$(m^2 - 1)(t^2 - 1) = s^2 - 1 \tag{4}$$

for some $s = s_m = s(m)$ such that $5 \leq s \in N$. Rearranging (4), we obtain the following Pell equation for the unknowns t and s

$$s^2 - (m^2 - 1)t^2 = 2 - m^2 . \tag{5}$$

For any choice of m, Equation (5) has infinitely many positive integer solutions, and our goal is to find all of them. We start with finding one family of positive integer solutions,

which we denote by $t_{m,n}$ and $s_{m,n}$, $n = 0, 1, 2, \ldots$ where the smallest one in the chain is $s_{m,0} = t_{m,0} = 1$. To find $t_{m,n}$ and $s_{m,n}$, we first solve the related unit Pell equation

$$u^2 - (m^2 - 1)v^2 = 1\,. \tag{6}$$

The smallest positive integer solution of (6) is $u = m$, $v = 1$. Therefore, all of its positive integer solutions are obtained as the rational and irrational coefficients of the expansion $(m + \sqrt{m^2 - 1})^n$, for $n = 1, 2, \ldots$ Consequently, an infinite family of solutions to (5) is generated by the rational and irrational coefficients of the expansion

$$s_{m,n} + \sqrt{m^2 - 1}t_{m,n} = (1 + \sqrt{m^2 - 1})(m + \sqrt{m^2 - 1})^n, \quad n = 1, 2, \ldots \tag{7}$$

To compute this family explicitly, we write the recurrence relations

$$\begin{aligned} s_{m,n} + \sqrt{m^2-1}t_{m,n} &= (m + \sqrt{m^2-1})(s_{m,n-1} + \sqrt{m^2-1}t_{m,n-1}) \\ &= ms_{m,n-1} + (m^2-1)t_{m,n-1} + (s_{m,n-1} + mt_{m,n-1})\sqrt{m^2-1} \end{aligned} \tag{8}$$

which lead to

$$t_{m,n} = s_{m,n-1} + mt_{m,n-1}, \quad s_{m,n} = ms_{m,n-1} + (m^2 - 1)t_{m,n-1}\,. \tag{9}$$

After some algebraic manipulations this reduces to

$$\begin{aligned} t_{m,0} &= 1, \quad t_{m,1} = m + 1, & t_{m,n} &= 2mt_{m,n-1} - t_{m,n-2}\,, \\ s_{m,0} &= 1, \quad s_{m,1} = m^2 + m - 1, & s_{m,n} &= 2ms_{m,n-1} - s_{m,n-2}\,. \end{aligned} \tag{10}$$

The second order linear recurrence relation (10) yields the following explicit form of $t_{m,n}$

$$t_{m,n} = \frac{1}{2\sqrt{m^2-1}}\left((\sqrt{m^2-1}+1)(m + \sqrt{m^2-1})^n + (\sqrt{m^2-1}-1)(m - \sqrt{m^2-1})^n\right). \tag{11}$$

From the latter result, we conclude that an infinite family of Diophantine quadruples of the form $\{1, b, c, d\}$, sorted in ascending lexicographic order, can be generated by

$$\begin{aligned} \{1, b, c, d\} &= \{1, m^2-1, {t_{m,n}}^2-1, m^2 + {t_{m,n}}^2 + 2{s_{m,n}}^2 + 2mt_{m,n}s_{m,n} - 3\} \\ &= \{1, m^2-1, {t_{m,n}}^2-1, (s_{m,n}+mt_{m,n})^2+{s_{m,n}}^2-(m^2-1){t_{m_n}}^2+m^2-3\}. \end{aligned} \tag{12}$$

Using (5), and (9), this solution can be summarized by

Result. A family of regular Diophantine quadruples of the form $\{1, b, c, d\}$ is given by

$$\{a, b, c, d\} = \{1, m^2 - 1, {t_{m,n}}^2 - 1, {t_{m,n+1}}^2 - 1\} \tag{13}$$

where $m \geq 2$ and $n \geq 1$, and the values of $t_{m,n}$ are determined by (11).

Remarks

A. Non Eulerian Diophantine quadruples. The infinite family (13) is not generated by Euler's solution (1). In fact, Euler's solution is obtained if we substitute $n = 1$ in (13).

B. Other possible families emanating from 1. The family (13) is not the *only* infinite family of regular Diophantine quadruples emanating from 1. The reason is that the Pell equation (5) has other positive integer solutions in addition to the set $(s_{m,n}, t_{m,n})$ defined above. For example, consider the case $m = 3$. We have $a = 1$, $b = m^2 - 1 = 8$ and the resulting Pell equation is

$$s^2 - 8t^2 = -7\,. \tag{14}$$

Equation (14) has two *fundamental solutions*, $(1,1)$ and $(5,2)$, and each of them generates a different infinite family of positive integer solutions, namely:

$$t_{3,n} = \frac{\sqrt{2}}{8}\left((1+\sqrt{8})(3+\sqrt{8})^n + (-1+\sqrt{8})(3-\sqrt{8})^n\right) \tag{15}$$

which yields $(1,8,15,528)$, $(1,8,528,17955),\ldots$, and

$$u_{3,n} = \frac{1}{8}\left((8+5\sqrt{2})(3+\sqrt{8})^n + (8-5\sqrt{2})(3-\sqrt{8})^n\right) \tag{16}$$

which yields $(1,8,120,4095)$, $(1,8,4095,139128),\ldots$

In the next section we find all the positive solutions of (5).

4 Generating all the regular Diophantine quadruples emanating from 1

In order to generate all regular Diophantine quadruples emanating from 1, i.e., $\{1,b,c,d\}$, where $1 < b < c < d$, we need to solve some non-unit Pell equations which, in our case, have several infinite families of solutions. Lemma 1 shows how this general case can be treated.

Lemma 1 *Let L be an integer and d be a positive integer which is not a perfect square. Consider the Pell equation*

$$x^2 - dy^2 = L \tag{17}$$

and the related unit Pell equation

$$x^2 - dy^2 = 1\,. \tag{18}$$

Suppose that (α_1,β_1) is the minimal positive integer solution of (17)*, and define $P_1 = \alpha_1 + \sqrt{d}\beta_1$. Let (μ_1,ν_1) be the minimal positive integer solution of* (18) *and define $S_1 = \mu_1 + \sqrt{d}\nu_1$. Suppose that (α_2,β_2) is another integer solution of* (17) *such that $P_2 = \alpha_2 + \sqrt{d}\beta_2$ is not of the form $P_1S_1^k$. Then, Equation* (17) *has an integer solution (α_*,β_*) with $S_* = \alpha_* + \sqrt{d}\beta_*$, generating P_2 and satisfying*

$$P_1 < S_* < P_1S_1\,. \tag{19}$$

The proof of Lemma 1 is given in the Appendix. Lemma 1 provides an algorithm for generating all the regular Diophantine quadruples of the form $\{1, b, c, d\}$, in a lexicographic order, as detailed below.

Algorithm 1

Step 1: Using the solution (13), obtain an infinite family emanating from the fundamental solution $(1, 1)$ of the Pell equation (5). This gives $P_1 = 1 + \sqrt{m^2 - 1}$. Denote $S_1 = m + \sqrt{m^2 - 1}$, and the resulting infinite family of solutions is therefore $S_1 P_1^n$, $n = 0, 1, 2, \ldots$

Step 2: Use Lemma 1 to search for other solutions. Any other family of solutions must have one member, S_2, that satisfies the inequality $P_1 < S_2 < P_1 S_1$. This gives

$$1 + \sqrt{m^2 - 1} < \alpha + \beta\sqrt{m^2 - 1} < m^2 + m - 1 + (m + 1)\sqrt{m^2 - 1} \tag{20}$$

where α, and β are positive integers. Therefore, all the solutions of (5) can be tracked down by going over at most $m - 1$ cases, namely $\beta = 2, 3, \ldots, m$, and checking if α is a positive integer. Each additional solution of (5) that emerges in this search yields a new infinite family of solutions $t_{m,n}$ of (5), which provides a new set of Diophantine quadruples defined by (13).

Example. In the above example where $m = 3$, we have $P_1 = 1 + \sqrt{8}$ and $S_1 = 3 + \sqrt{8}$. To find other solutions, we need only to check the two cases $\beta = 2, 3$. Verification shows that the only additional solution is generated by $(5, 2)$, as explained in (16). Therefore the solutions for $m = 3$ emanate only from the above two families.

Additional solutions

It is easy to verify that for any value of $m \geq 3$, there are at least two fundamental solutions, namely $(1, 1)$, and $(m - 1, m^2 + m - 1)$. These give at least two infinite families of solutions.

There exist values of $m > 3$ for which additional families appear. If $m = k^2 + (k+1)^2 - 2$ for some k, there are at least four fundamental solutions $(1, 1)$, $(m - 1, m^2 - m - 1)$, $(k, 2k^3 + 2k^2 - 2k - 1)$, $(k+1, 2k^3 + 4k^2 - 1)$. The first such value is $m = 11 = 2^2 + 3^2 - 2$, which has the fundamental solutions $(1, 1)$, $(2, 19)$, $(3, 31)$, $(10, 109)$. Further, there are values of m which are not of the form $m = k^2 + (k + 1)^2 - 2$ but give four fundamental solutions. The smallest such example is obtained for $m = 41$.

We point out that using Algorithm 1 for $1 \leq m \leq 20,000$ did not reveal any value of m for which there are six or more fundamental solutions.

5 Characterizing the regular Diophantine quadruples emanating from 1

The solution proposed in the previous section is an $O(m)$ complexity algorithm, but the result depends on a number of numerical tests. Here, we provide a closed form characterization. We start with the following lemma:

Lemma 2 *Let $\{1, t^2 - 1, m^2 - 1\}$ be a Diophantine triplet with $1 < t < m$, and denote $(m^2 - 1)(t^2 - 1) = s^2 - 1$. Then, the following triplets are also Diophantine triplets:*

$$\begin{aligned} &\{1, t^2 - 1, (mt - s)^2 - 1\}, \quad \{1, m^2 - 1, (mt - s)^2 - 1\}, \\ &\{1, t^2 - 1, (mt + s)^2 - 1\}, \quad \{1, m^2 - 1, (mt + s)^2 - 1\}. \end{aligned} \tag{21}$$

Further, we have $mt - s < m < mt + s$.

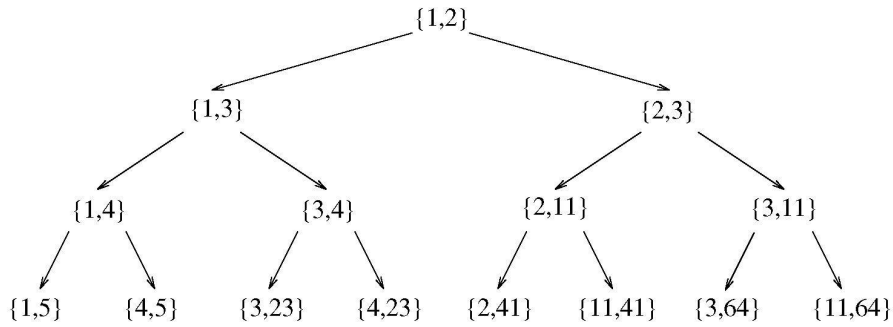

Fig. 1 Applying Algorithm 2.
Each couple generates two new couples $(m,t) \longrightarrow (m, mt+s)$ and $(t, mt+s)$.
Each couple (t,m) corresponds to the Diophantine triplet $(1, t^2-1, m^2-1)$.

Proof. We only need to verify that if we multiply the second and third elements of the above triplets, and add 1, we obtain a perfect square. Indeed,

$$\begin{aligned}
(t^2-1)((mt-s)^2-1)+1 &= \left(ts-m(t^2-1)\right)^2,\\
(m^2-1)((mt-s)^2-1)+1 &= \left(ms-t(m^2-1)\right)^2,\\
(t^2-1)((mt+s)^2-1)+1 &= \left(ts+m(t^2-1)\right)^2,\\
(m^2-1)((mt+s)^2-1)+1 &= \left(ms+t(m^2-1)\right)^2.
\end{aligned} \tag{22}$$

Verifying that $mt-s<m<mt+s$ is straightforward. This completes the proof of the lemma. □

We now define a recursive algorithm for generating all Diophantine triplets of the form $\{1,b,c\}$.

Algorithm 2 First, seek a method that gives all the generating couples $\{t,m\}$ for which $\{1,t^2-1,m^2-1\}$ is a Diophantine triplet. The first couple (in lexicographic order) is $\{1,1\}$ and the related Diophantine triplet is $\{1,0,0\}$. Using Lemma 2, obtain another couple $\{1,2\}$ (note that we require $m,t>0$). The triplet generated by $\{1,2\}$ is $\{1,0,3\}$. The value of s in the couple is $s=1$, and it follows from Lemma 2 that $\{1,3\}$ and $\{2,3\}$ are also Diophantine couples. These generate the Diophantine triplets $\{1,0,8\}$ and $\{1,3,8\}$. Continue this recursive procedure to obtain two new couples $(m, mt+s)$ and $(t, mt+s)$ from each couple (m,t). Upgrade each triplet to a regular Diophantine quadruple using the value of d_+ in (3).

Figure 1 illustrates the procedure of Algorithm 2.

We now prove the following theorem.

Theorem 1 *Algorithm* 2 *generates all Diophantine triplets of the form* $\{1,b,c\}$.

Proof. Suppose that this is not the case, and consider the minimal positive integer m for which the Diophantine triplet $\{1,t^2-1,m^2-1\}$, with $t<m$, is not obtained by the algorithm. From Lemma 2, it follows that $\{1,t^2-1,(mt-s)^2-1\}$

is also a Diophantine triplet. Since $mt - s < m$, it follows from the definition of m that the latter triplet is obtained by our algorithm. We now write $m' = mt - s$, and $s' = \sqrt{(m'^2 - 1)(t^2 - 1) + 1} = ts - m(t^2 - 1)$, and use our algorithm to produce the triplet $\{1, t^2 - 1, (m't - s')^2 - 1\}$. But since we have

$$m't - s' = (mt - s)t - (ts - m(t^2 - 1)) = m \tag{23}$$

we obtain a contradiction. Consequently, the algorithm described above generates all the diophantine triplets of the form $\{1, b, c\}$. □

6 Concluding remarks

Comparison between Algorithms 1 and 2. Although both Algorithms 1 and 2 give all the regular Diophantine quadruples of the form $\{1, b, c, d\}$, they differ in two important aspects: Algorithm 1 is a practical mean for generating a lexicographically sorted list of the regular Diophantine quadruples, but depends on several manual verifications per step. On the other hand, Algorithm 2 gives a recursive construction of all regular Diophantine quadruples, and thus a closed form mathematical characterization. However, it yields an unsorted list of results.

A note on general Diophantine quadruples. The technique we used for quadruples of the form $\{1, b, c, d\}$ does not apply to the general case, at least not directly. For general quadruples $\{a, b, c, d\}$, we have $b = \frac{m^2-1}{a}$, and $c = \frac{t^2-1}{a}$ for some positive integers m, t with $a \mid m^2 - 1$ and $a \mid t^2 - 1$. Since $bc + 1 = s^2$ for some s, we write $(m^2 - 1)(t^2 - 1) + a^2 = a^2 s^2$. This yields

$$a^2 s^2 - (m^2 - 1)t^2 = a^2 + 1 - m^2, \qquad \text{s.t. } a \mid l\,. \tag{24}$$

It is easy to see that $(s, t) = (1, 1)$ is a solution to (24). Unfortunately, the idea of generating all the solutions of (24) by solving the related unit Pell does not work. Since $a \mid a^2 s^2 - (m^2 - 1)t^2 = 1$, the related unit Pell equation $a^2 s^2 - (m^2 - 1)t^2 = 1$ has no integer solutions if $a \neq 1$.

Appendix: a quick review on Pell equations

We summarize here a few standard results concerning Pell equations. Additional information can be found, for example, in the references [1, 3, 6, 8, 9, 10, 12].

The quadratic Diophantine equation in the unknowns x, y,

$$x^2 - dy^2 = L, \tag{A.1}$$

where the positive integer d has no square factors, and L is an integer, is called *Pell's equation*. When $L = 1$, (A.1) is called a *unit Pell equation* (sometimes the unit Pell equation is identified as Pell equation).

The unit Pell equation

The unit Pell equation

$$x^2 - dy^2 = 1 \tag{A.2}$$

has the trivial solution $x = 1$, $y = 0$, which we ignore hereafter. The case where $d = \mu^2$ (ruled out above) is a square admits no nontrivial solutions since it leads to $x^2 - (\mu y)^2 = 1$ and the difference between two nonzero squares is greater than 1. Further, without loss of generality, one can assume that d is square free because any square factor of d can be absorbed into the unknown y.

We now associate each solution (p, q) of the unit Pell equation (A.2) with the number $p + \sqrt{d}q$ of the ring $\mathbb{Z} + \sqrt{d}\,\mathbb{Z}$, and treat these two representations interchangeably.

Since $1 = p^2 - dq^2 = (p + \sqrt{d}q)(p - \sqrt{d}q)$, it follows that the product and quotient of two solutions of (A.2) is also a solution. Therefore, each solution (p, q) produces an infinite family of solutions. This family can be found by observing that for any positive integer n, $(p^2 - dq^2)^n = 1$, and by factoring

$$(x + \sqrt{d}y)(x - \sqrt{d}y) = (p + \sqrt{d}q)^n (p - \sqrt{d}q)^n . \tag{A.3}$$

This leads to the solutions

$$x + \sqrt{d}y = (p + \sqrt{d}q)^n, \quad x - \sqrt{d}y = (p - \sqrt{d}q)^n, \tag{A.4}$$

in the $\mathbb{Z} + \sqrt{d}\,\mathbb{Z}$ ring representation, or in explicit notations

$$x = \frac{1}{2}\left((p + q\sqrt{d})^n + (p - q\sqrt{d})^n\right) \quad y = \frac{1}{2\sqrt{d}}\left((p + q\sqrt{d})^n - (p - q\sqrt{d})^n\right) . \tag{A.5}$$

Note that if the solution (p, q) is positive, then $p + \sqrt{d}q > 1$ and also $0 < p - \sqrt{d}q < 1$. We show now that if $p_0 + \sqrt{d}q_0$ is the smallest positive solution of the unit Pell equation (A.2), then all of the solutions are given by $x + \sqrt{d}y = (p_0 + \sqrt{d}q_0)^n$ and $x - \sqrt{d}y = (p_0 - \sqrt{d}q_0)^n$ where $n = 1, 2, \ldots$ To prove this claim, suppose that the number $g + \sqrt{d}h > 1$ is a solution of (A.2), and that it is not a power of $(p_0 + \sqrt{d}q_0)$. We can therefore bound it between two consecutive such powers, i.e.,

$$(p_0 + \sqrt{d}q_0)^m < g + \sqrt{d}h < (p_0 + \sqrt{d}q_0)^{m+1} \tag{A.6}$$

for some positive integer m. After multiplying (A.6) by $(p_0 - \sqrt{d}q_0)^{-m}$, we get

$$1 < (p_0 - \sqrt{d}q_0)^m (g + \sqrt{d}h) < (p_0 + \sqrt{d}q_0) . \tag{A.7}$$

Since the product of two solutions of the unit Pell equation is also a solution, and from (A.7) we have $(p_0 - \sqrt{d}q_0)^m (g + \sqrt{d}h) > 1$, we obtained another positive solution which is smaller than the presumably smallest positive solution $p_0 + \sqrt{d}q_0$. This is a contradiction.

From the above discussion we see that in order to solve the unit Pell equation completely, one needs only to find the smallest positive solution. One can either guess this solution by a trial and error process, or find it by computing the continued fraction $[a_0, a_1, \ldots]$ of $\sqrt{d}$. We briefly describe the continued fraction method (which works also for the minus-unit equation, i.e., $L = -1$ in (A.1)). Suppose that p_n/q_n is the n-th convergent $[a_0, a_1, \ldots, a_n]$ of the continued fraction of $\sqrt{d}$. We seek a convergent satisfying $p_n^2 - dq_n^2 = (-1)^{n+1}$. This is possible since $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_r, 2a_0}]$ for some r, that is, the continued fraction is periodic with $a_{r+1} = 2a_0$. Suppose that p_r/q_r is the r-th convergent. If r is odd, then $(-1)^{r-1} > 0$ and the smallest integer solution is $x = p_r$ and $y = q_r$. If r is even, then $(-1)^{r-1} < 0$ and $p_{2r+1}^2 - dq_{2r+1}^2 = 1$. Thus, the smallest integer solution is $x = p_{2r+1}$, $y = q_{2r+1}$.

The general Pell equation

The general Pell equation (A.1) with $L \neq 1$, may have several infinite families of solutions or have no solution at all (e.g., $x^2 - 3y^2 = 11$ which is impossible modulo 4). Lemma 1 shows how the general case can be treated when solutions do exist.

Lemma 1 *Let L be an integer and d be a positive integer which is not a perfect square. Consider the Pell equation*

$$x^2 - dy^2 = L \tag{A.8}$$

and the related unit Pell equation

$$x^2 - dy^2 = 1\,. \tag{A.9}$$

Suppose that (α_1, β_1) is the minimal positive integer solution of (A.8)*, and define $P_1 = \alpha_1 + \sqrt{d}\beta_1$. Let (μ_1, ν_1) be the minimal positive integer solution of* (A.9) *and define $S_1 = \mu_1 + \sqrt{d}\nu_1$. Suppose that (α_2, β_2) is another integer solution of* (A.8) *such that $P_2 = \alpha_2 + \sqrt{d}\beta_2$ is not of the form $P_1 S_1^k$. Then, Equation* (A.8) *has an integer solution (α_*, β_*) with $S_* = \alpha_* + \sqrt{d}\beta_*$, generating P_2 and satisfying*

$$P_1 < S_* < P_1 S_1\,. \tag{A.10}$$

Proof. As P_2 is not generated by the sequence $P_1 S_1^k$, $k = 0, 1, \ldots$, there exists some positive integer n such that

$$P_1 S_1^n < P_2 < P_1 S_1^{n+1}\,. \tag{A.11}$$

If we multiply (A.11) by $\bar{S}_1^n$, where $\bar{S}_1 = \mu_1 - \sqrt{d}\nu_1$, we get

$$P_1 < P_2 \bar{S}_1^n < P_1 S_1\,. \tag{A.12}$$

Since $\bar{S}_1^n$ corresponds to a solution of (A.9), it follows that $P_2 \bar{S}_1^n$ corresponds to a solution of (A.8), and this completes the proof. □

Acknowledgements
We thank Oran Lang and Ran Tessler for helpful suggestions and discussions.

References

[1] Beiler, A.H.: The Pellian. In: Recreations in the Theory of Numbers: The Queen of Mathematics Entertains (Ch. 22). Dover, New York 1966, 248–268.

[2] Davenport, H., and Baker, A.: The Equations $[3x^2 - 2 = y^2]$ and $[8x^2 - 7 = z^2]$. *Quart. J. Math. (Oxford) Ser.* 2, 20 (1969), 129–137.

[3] Dickson, L.E.: *History of the Theory of Numbers*. Chelsea, New York 1952.

[4] Gibbs, P.: www.weburbia.demon.co.uk/pg/diophant.htm

[5] Hoggatt, V.E., and Bergum, G.E.: A Problem of Fermat and the Fibonacci Sequence. *Fib. Quart.* 15 (1977), 323–330.

[6] Hua, C.: *Introduction to Number Theory*. Springer-Verlag, New York 1982.

[7] Jones, L.: A polynomial approach to a Diophantine problem. *Math. Mag.* 72 (1999), 52–55.

[8] Lagarias, J.C.: On the Computational Complexity of Determining the Solvability or Unsolvability of the Equation $X^2 - DY^2 = -1$. *Trans. Amer. Math. Soc.* 260 (1980), 458–508.

[9] Sierpinski, W.: *Elementary Theory of Numbers*. North Holland, Amsterdam 1988.

[10] Stillwell, J.C.: *Mathematics and Its History*. Springer-Verlag, New York 1989.

[11] Veluppillai, M.: The equations $z^2 - 3y^2 = -2$ and $z^2 - 6x^2 = -5$. In: A collection of manuscripts related to the Fibonacci sequence. (Hoggatt, V.E., and Bicknell-Johnson, M., eds.), Fibonacci Association 1980, 71–75.

[12] Whiford, E.E.: *Pell Equation*. Columbia University Press, New York 1912.

[13] www.seanet.com/ksbrown/number.htm/kmath289.htm

Eran Assaf
Bar Ilan University
Ramat Gan, Israel

Shay Gueron
Department of Mathematics
University of Haifa
Haifa, 31905, Israel
e-mail: `shay@math.haifa.ac.il`