BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 52, Number 2, April 2015, Pages 345–351
S 0273-0979(2014)01483-1
Article electronically published on December 19, 2014

Solving the Pell equation, by Michael J. Jacobson, Jr. and Hugh C. Williams, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, Springer, New York, 2009, xx+495 pp., ISBN 978-0-387-84922-5, US $59.95

> *The men of Harold stood well together, as their wont was, and formed sixty and one squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter their redoubts; for a single blow of a Saxon war-hatchet would break his lance and cut through his coat of mail. ... When Harold threw himself into the fray the Saxons were one mighty square of men, shouting the battle-cries, "Ut!" "Olicrosse!" "Godemitè!"*

The little-known account of the battle of Hastings (October 14, 1066) just quoted, formulates the equation $x^2 = 61y^2+1$, to be solved in positive integers x, y. It is an instance of the *Pell equation* $x^2 = d{\cdot}y^2 + 1$, where d is a given positive integer; one excludes values of d that are perfect squares, since for $d = e^2$ the two consecutive positive integers $dy^2 = (ey)^2$ and $dy^2 + 1$ cannot both be squares.

The Pell equation is like a raindrop in which all of number theory is reflected. Indeed, one of the stated objectives of the book under review is to introduce the reader to "the delights of algebraic number theory" by means of the Pell equation, and in its 500 pages the analytic, algorithmic, and applied aspects of the subject all receive ample attention. In addition, one learns about the rich history of the equation, which, as Weil's book [11] illustrates, is not very different from the history of number theory itself. A second stated objective of the book by Jacobson and Williams is "to detail the enormous progress" that has in recent decades been made on developing efficient solution methods for the Pell equation. Such methods are both practically and theoretically of interest: practically because of their uses in cryptography, and theoretically because they are manifestations of novel concepts that are nowadays viewed as belonging to *Arakelov theory*.

There are three results on the Pell equation that everybody should know. They concern the *existence* of a solution, the *structure* of the set of solutions, and an *algorithm* for finding them.

First, for any nonsquare positive integer d, the Pell equation $x^2 = dy^2 + 1$ does have a solution in positive integers x, y. Most likely, Fermat (1601–1665) was already in possession of a proof of this nontrivial fact (cf. [11]), but the first published proof was given in 1768 by Lagrange (1736–1813) [1]. An admirably brief

2010 *Mathematics Subject Classification.* Primary 11D09, 11A55.

proof, much in the spirit of the nineteenth century, is contained in the very first chapter of the book under review.

Second, there is the structure of the set of solutions. It is best understood if one rewrites the equation as $(x+y\sqrt{d})\cdot(x-y\sqrt{d})=1$: the product of a "quadratic integer" and its conjugate equals 1. This property is preserved under taking powers, so starting from any solution x_1, y_1 in positive integers, one obtains, for each positive integer n, a solution x_n, y_n by expanding $(x_1+y_1\sqrt{d})^n$ in the form $x_n+y_n\sqrt{d}$. One readily checks $x_1<x_2<x_3<\cdots$ and $y_1<y_2<y_3<\cdots$, so a single solution gives rise to infinitely many. In fact, if one chooses x_1, y_1 to be the *least* positive solution, then one obtains *all* positive solutions in this manner. These results are perfectly elementary, and in one form or another they must have been known long before Lagrange.

Third, one considers algorithms: given d, how does one "efficiently" find the least positive integers $x(d)$, $y(d)$ satisfying the Pell equation? This has from the very beginning been the most investigated question in the subject. It is important to realize that a simple search will in practice not suffice, since it is an experimental fact, backed up by a fairly solid conjecture, that $x(d)$ and $y(d)$ are usually gigantic. An example is provided by Archimedes's *Cattle problem*, duly treated in the book, which is equivalent to the Pell equation for $d = 410\,286423\,278424$; in this case, $x(d)$ and $y(d)$ have 103273 and 103265 decimal digits, respectively.

There is a proven upper bound: for all d one has

$$\log y(d) < \log x(d) < d^{1/2}(\log(4d)+2),$$

where $d^{1/2}$ denotes the positive real square root of d. It is a folklore conjecture, related to the Cohen–Lenstra heuristics, that this upper bound is typically of the correct order of magnitude, in the sense that for each $\epsilon>0$ asymptotically 100% of all nonsquares d satisfy $\log x(d) > \log y(d) > d^{1/2-\epsilon}$. Providing a proof is the major open problem in the theory of the Pell equation. It is not even known whether there is a positive constant c such that infinitely many square-free values of d satisfy $\log x(d) > d^c$.

Given the conjectured typical size of $x(d)$, it is not reasonable to ask for a polynomial-time algorithm that given d computes $x(d)$. Nevertheless, there does exist a fairly quick method for calculating $x(d)$, $y(d)$ from d, and it has, in different guises, been frequently discovered throughout history. In its currently most fashionable formulation, it makes use of *continued fractions*. The existence of this method is the third fact about the Pell equation that should be common knowledge. The algorithm can be made to run in time no more than $\log x(d)$ multiplied by a constant power of $1+\log d$; in other words, *computing* the numbers $x(d)$ and $y(d)$ can be done almost as quickly as *writing them down*.

To describe the fundamental idea, we can hardly do better than quote the particularly lucid explanation that Euler (1706–1783) provides in his famous *Algebra* (1770) [3]. It uses no more than the traditional Euclidean algorithm. Euler's attribution of the method to John Pell (1611–1685), who has apparently nothing to do with the equation, has given rise to much heated debate, but the name has stuck. Here is how Euler deals with the case $d=7$, in the oldest English translation of his textbook [4, Part II, Chapter VII, Article 102]:

> Let us proceed farther, and let $a = 7$, and $7nn+1 = mm$; we see that $m > 2n$; let us therefore make $m = 2n+p$, and we shall

have $7nn + 1 = 4nn + 4np + pp$, or $3nn = 4np + pp - 1$; which gives $n = \frac{2p+\sqrt{7pp-3}}{3}$. At present, since $n > \frac{4}{3}p$, and, consequently, greater than p, let us make $n = p + q$, and we shall have $p + 3q = \sqrt{7pp - 3}$; then, squaring both sides, $pp + 6pq + 9qq = 7pp - 3$, so that $6pp = 6pq + 9qq + 3$, or $2pp = 2pq + 3qq + 1$, whence we get $p = \frac{q+\sqrt{7qq+2}}{2}$. Now, we have here $p > \frac{3q}{2}$; and, consequently, $p > q$; so that making $p = q + r$, we shall have $q + 2r = \sqrt{7qq + 2}$; the squares of which are $qq+4qr+4rr = 7qq+2$; then $6qq = 4qr+4rr-2$, or $3qq = 2qr + 2rr - 1$; and, lastly, $q = \frac{r+\sqrt{7rr-3}}{3}$. Since now $q > r$, let us suppose $q = r + s$, and we shall have $2r + 3s = \sqrt{7rr - 3}$; then $4rr + 12rs + 9ss = 7rr - 3$, or $3rr = 12rs + 9ss + 3$, or $rr = 4rs + 3ss + 1$, and $r = 2s + \sqrt{7ss + 1}$. Now, this formula is like the first; so that making $s = 0$, we shall obtain $r = 1$, $q = 1$, $p = 2$ and $n = 3$, or $m = 8$.

Euler treats seven values of d in this manner and, not surprisingly, he finds a solution in each case. However, his claim [3, Part II, Chapter VII, Article 104] that the method always leads to a solution, is, other than he apparently thought, not backed up by a proof. It will surely find a solution if one exists; but this is also the case for the *negative Pell equation* $x^2 - dy^2 = -1$, which already for $d = 3$ is unsolvable in integers.

Can one directly prove that the method explained by Euler does lead to a solution? Weil [11, Chapter II, §XIII] remarked that the sequence of equations

$$\begin{aligned} 3nn &= 4np + pp - 1 \\ 2pp &= 2pq + 3qq + 1 \\ 3qq &= 2qr + 2rr - 1 \\ rr &= 4rs + 3ss + 1 \end{aligned}$$

that Euler derived from $mm = 7nn+1$ displays a symmetry that can hardly escape notice, and he used it to construct a solvability proof that, as he plausibly argued, may have been the one that Fermat had in mind. In 1944, Hofmann [5] presented a completely different reconstruction of Fermat's proof, but since it is based on several erroneous theorems, it cannot be taken seriously.

We sketch an alternative argument that uses Euler's chain of equations to prove that Pell's equation has a positive solution. Instead of $x^2 = dy^2 + 1$, one considers more general equations of the type $ax^2 = 2bxy + cy^2 \pm 1$, where a, b, $c \in \mathbf{Z}$ satisfy $a > 0$, $b \geq 0$, $c > 0$, and where $b^2 + ac$ equals our given nonsquare positive integer d; we also require $2b > a - c$ or, equivalently, that the positive zero of $at^2 - 2bt - c$ is greater than 1. Writing k for the integer part of that zero, we see that the procedure explained by Euler is equivalent to putting $x = kx^* + y^*$, $y = x^*$, which transforms the given equation into an equation $a^*x^{*2} = 2b^*x^*y^* + c^*y^{*2} \mp 1$, where a^*, b^*, $c^* \in \mathbf{Z}$ are certain expressions in a, b, c, k that satisfy the same conditions as a, b, c.

We could now continue to formalize Euler's argument, and show that a positive integer solution (x, y) of our equation corresponds to a smaller and still nonnegative solution (x^*, y^*) of the next; thus, the equation one starts from has a positive integer solution if and only if one eventually runs into an equation that has the trivial

solution $(1,0)$. But why this actually happens if one starts from the equation $x^2 = dy^2 + 1$ remains unclear.

Instead, we do not *wait* for the trivial solution $(1,0)$ to appear, but *start* from it, noting that it does solve the Pell equation $x^2 = dy^2 + 1$, which we use as the initial equation in Euler's reduction process. It gives rise to the solution $(x^*, y^*) = (0,1)$ of the next equation, next to (x^{**}, y^{**}) with $x^{**}y^{**} < 0$, and in general one will have $0 = x^*y^* > x^{**}y^{**} > x^{***}y^{***} > \cdots$. Each time we pass from one equation to the next, the $*$-operation is a bijection between their sets of solutions, so that any two equations in the chain thus constructed have equally many solutions. Since there are only finitely many triples of nonnegative integers a, b, c satisfying $b^2 + ac = d$, at least one equation occurs infinitely often in this chain, and the process produces infinitely many integer solutions to that equation. Then the initial equation $x^2 = dy^2 + 1$ has infinitely many integer solutions as well, and passing to absolute values we also find infinitely many solutions that are positive.

Whether the argument just given, in its reliance on negative numbers and infinities, is likely to have occurred to Fermat, we leave to the reader to decide.

To sketch later developments, we consider the set of equations $ax^2 = 2bxy + cy^2 \pm 1$ that satisfy $\gcd(a, 2b, c) = 1$ in addition to the conditions listed above. For each d, this set of equations is finite, and it is mapped to itself by Euler's reduction operation. Iterating the operation on a given equation, one ultimately runs into a cycle, and we shall write C_d for the set of distinct cycles obtained in this way. Gauss (1777–1855) proved in 1801 that C_d has a natural abelian *group* structure, derived from *composition* of quadratic forms; the neutral element of C_d is the cycle that the Pell equation $x^2 = dy^2+1$ eventually runs into. (Gauss's formulation is not the same as ours, but the difference need not bother the reader.) Composition of quadratic forms is a mysterious operation, which, as Dirichlet (1805–1859) pointed out, is best understood through the arithmetic of the quadratic ring $\mathbf{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x,\ y \in \mathbf{Z}\}$. Dirichlet showed that C_d may be identified with a suitably defined *ideal class group* of $\mathbf{Z}[\sqrt{d}]$, composition of quadratic forms then taking the form of multiplication of ideals.

The book under review owes its existence to an observation of Daniel Shanks (1917–1996) from 1972 [10]. He restricted composition to the cycle that corresponds to the neutral element of C_d, and he observed phenomena reminiscent of the group operation in a circle group. Since this is happening "inside" the unit element of C_d, he used the word *infrastructure* for his discovery. It was soon realized that Shanks had indeed run into a group that is closely related to the class group [6]. Later, the same group arose in the context of *Arakelov theory*, which is a branch of arithmetic algebraic geometry that emerged a few years after Shanks's work. Nowadays, the group is often referred to as the *Arakelov class group*.

To explain what the Arakelov class group is, we digress for a moment from the Pell equation. By a *lattice* in the field $\mathbf{C}$ of complex numbers we mean a noncyclic additive subgroup L of $\mathbf{C}$ that is discrete in the usual topology on $\mathbf{C}$; equivalently; it is a subset of the form $\mathbf{Z}z_1 + \mathbf{Z}z_2$, where $z_1,\ z_2 \in \mathbf{C}$ are linearly independent over the field $\mathbf{R}$ of real numbers. Two lattices L and M in $\mathbf{C}$ are called *similar* if for some z in the multiplicative group $\mathbf{C}^*$ of nonzero complex numbers one has $L = z \cdot M$. Intuitively, one may say that two lattices are similar if and only if they "look the same", modulo zooming in or zooming out or turning one's head left or right; but a mirror is not allowed. Here zooming in or out corresponds to taking

$z \in \mathbf{R}_{>0}$, and turning one's head to taking z in the circle group $\mathbf{T}$, which is the largest compact subgroup of $\mathbf{C}^*$; note that $\mathbf{C}^*$ is the direct product of its subgroups $\mathbf{R}_{>0}$ and $\mathbf{T}$. We shall consider lattices in $\mathbf{C}$ only up to similarity.

By the *product* $L{\cdot}M$ of two lattices in $\mathbf{C}$ we mean the additive subgroup of $\mathbf{C}$ generated by $\{x{\cdot}y : x \in L,\ y \in M\}$. Usually, $L \cdot M$ is not a lattice, and one may wonder under which conditions it is. To answer this question in the case $L = M$, one defines the *multiplier ring* $R_L = \{z \in \mathbf{C} : z{\cdot}L \subset L\}$ of L, which is a discrete subring of $\mathbf{C}$ that depends only on the similarity class of L. It is not hard to show that either $R_L = \mathbf{Z}$, or R_L is itself a lattice. It is precisely in the latter case that $L{\cdot}L$ is a lattice; such lattices are said to admit *complex multiplication*, and they are of interest in the theory of elliptic curves.

The multiplier rings R_L that one encounters for lattices L with complex multiplication are *imaginary quadratic*, in the sense that they are of the form $\mathbf{Z}+\mathbf{Z}\alpha$, where α is a complex zero of a quadratic polynomial with integer coefficients, leading coefficient 1, and negative discriminant. Examples are the ring $\mathbf{Z}[\mathrm{i}] = \{x + y\mathrm{i} : x,\ y \in \mathbf{Z}\}$ of Gaussian integers, and its subring $\mathbf{Z}[3\mathrm{i}]$. The *class group* of such a ring R is the set of similarity classes of lattices L in $\mathbf{C}$ with $R_L = R$. Multiplication of lattices makes the class group into an abelian group, the neutral element being the similarity class of R itself and the inverse being obtained by complex conjugation. A classical theorem, in substance due to Gauss, asserts that this group is *finite*. For the ring $\mathbf{Z}[\mathrm{i}]$ the group is trivial, and for $\mathbf{Z}[3\mathrm{i}]$ it is of order 2. For imaginary quadratic orders, the Arakelov class group coincides with the class group.

The situation is different for the *real* quadratic rings $\mathbf{Z}[\sqrt{d}]$ that are relevant for the Pell equation. In order to be able to view such rings as lattices, we replace the field $\mathbf{C}$ by $\mathbf{R}\times\mathbf{R}$, which is a commutative ring with componentwise ring operations: addition is vector addition, and multiplication is defined by $(r, s){\cdot}(t, u) = (rt, su)$. We write 1 for the unit element $(1, 1)$, and view $\mathbf{R} = \mathbf{R}{\cdot}1$ as a subring of $\mathbf{R} \times \mathbf{R}$. For a positive integer d that is not a square, we denote the element $(d^{1/2}, -d^{1/2})$ of $\mathbf{R} \times \mathbf{R}$ by $\sqrt{d}$; it does satisfy $(\sqrt{d})^2 = d$. We can now view $\mathbf{Z}[\sqrt{d}] = \mathbf{Z}{\cdot}1 + \mathbf{Z}{\cdot}\sqrt{d}$ as a subring of $\mathbf{R} \times \mathbf{R}$.

Other than $\mathbf{C}$, the ring $\mathbf{R} \times \mathbf{R}$ has nonzero elements that have no multiplicative inverse, namely the elements that have exactly one of their coordinates equal to 0. The rings $\mathbf{Z}[\sqrt{d}]$ just defined contain none of those "undesirable" elements. Generally, we may define a *lattice in* $\mathbf{R} \times \mathbf{R}$ to be a noncyclic discrete additive subgroup L of $\mathbf{R} \times \mathbf{R}$ such that every nonzero element of L has a multiplicative inverse in $\mathbf{R} \times \mathbf{R}$. Thus, our rings $\mathbf{Z}[\sqrt{d}]$ are lattices in $\mathbf{R} \times \mathbf{R}$. It is in the definition of similarity that the greatest difference with the case of lattices in $\mathbf{C}$ is to be found: two lattices L and M in $\mathbf{R}\times\mathbf{R}$ are called *similar* if there exists $z \in \mathbf{R}_{>0}{\cdot}\{(\pm1, \pm1)\}$ with $L = z{\cdot}M$; here the *finite* group $\{(\pm1, \pm1)\}$, which is the maximal compact subgroup of the group $\mathbf{R}^* \times \mathbf{R}^*$ of invertible elements of $\mathbf{R} \times \mathbf{R}$, plays the role that $\mathbf{T}$ played earlier. One should note that $\mathbf{R}_{>0}{\cdot}\{(\pm1, \pm1)\}$ is quite a bit smaller than $\mathbf{R}^* \times \mathbf{R}^*$. In fact, if we write $\mathbf{H} = \{(x, x^{-1}) : x \in \mathbf{R}_{>0}\} = \{(\mathrm{e}^t, \mathrm{e}^{-t}) : t \in \mathbf{R}\}$, then $\mathbf{R}^* \times \mathbf{R}^*$ is the direct product of its three subgroups $\mathbf{R}_{>0}$, $\{(\pm1, \pm1)\}$, and $\mathbf{H}$; the group $\mathbf{H}$ is half a hyperbola, and it is isomorphic to the additive group $\mathbf{R}$. The reason for restricting to $z \in \mathbf{R}_{>0}{\cdot}\{(\pm1, \pm1)\}$ is that it enables us, just as for lattices in $\mathbf{C}$, to decide whether two lattices are similar just by "looking" at them. By contrast, for a large element $z \in \mathbf{H}$ a typical lattice L will not bear a recognizable resemblance to $z{\cdot}L$.

Again, let d be a positive integer that is not a square. The *Arakelov class group* A_d of $\mathbf{Z}[\sqrt{d}]$ is defined to be the set of similarity classes of lattices L in $\mathbf{R}\times\mathbf{R}$ for which the multiplier ring $\{z\in\mathbf{R}\times\mathbf{R} : z\cdot L\subset L\}$ equals $\mathbf{Z}[\sqrt{d}]$. It is an abelian group, the multiplication being defined as in the case of lattices in $\mathbf{C}$. The Arakelov class group A_d of $\mathbf{Z}[\sqrt{d}]$ is not finite, but it is compact in a naturally defined topology, in which the similarity classes of two lattices are "close" to each other if and only if they "look almost the same". The best way to understand this, is by considering the group homomorphism $\mathbf{R}\to A_d$ that sends t to the similarity class of $(\mathrm{e}^t,\mathrm{e}^{-t})\cdot\mathbf{Z}[\sqrt{d}]$. Its kernel is $\mathrm{reg}_d\cdot\mathbf{Z}$, where the *regulator* reg_d equals $\frac{1}{2}\log(x(d)+y(d)d^{1/2})$ or $\log(x(d)+y(d)d^{1/2})$, depending on whether the negative Pell equation $x^2-dy^2=-1$ does or does not have a solution in integers. The cokernel of the map $\mathbf{R}\to A_d$ is essentially equal to the class group C_d mentioned earlier. In particular, A_d has a copy of the *circle group* $\mathbf{R}/\mathrm{reg}_d\cdot\mathbf{Z}$ as a subgroup of finite index, so that A_d is indeed in a natural way a compact topological group. Shanks's infrastructure is nothing but the group structure in the circle group $\mathbf{R}/\mathrm{reg}_d\cdot\mathbf{Z}$, which in the book under review is referred to as an "infinite cyclic group" (p. 176). For each equation $ax^2=2bxy+cy^2\pm1$ as we saw in the definition of C_d, the set $\mathbf{Z}\cdot a+\mathbf{Z}\cdot(b-\sqrt{d})$ is a lattice in $\mathbf{R}\times\mathbf{R}$ with multiplier ring $\mathbf{Z}[\sqrt{d}]$, so that its similarity class belongs to A_d. There is a sense in which the similarity classes obtained in this way are to be found "everywhere" in A_d, and they form a convenient vehicle for doing computations in A_d.

The Arakelov class group can in fact be defined for any ring of algebraic integers in any algebraic number field. It contains information about both the class group and the unit group of the ring. Since the 1920s, number theorists have observed an analogy between algebraic number fields on the one hand and function fields of curves over finite fields on the other. Seen from this perspective, the Arakelov class group is the analogue of the group of rational points on the Jacobian of a curve over a finite field. The Jacobian is an algebraic group, and while no such thing can be asserted for the Arakelov class group, the latter is in several theoretical and computational respects far more manageable than the traditional class group and unit group of a ring of algebraic integers. For a discussion of the Arakelov class group and its algorithmic merits, we refer the reader to Schoof's tutorial [9].

The continued fraction method for solving the Pell equation, Euler's reduction operation, and Shanks's infrastructure all admit natural interpretations in terms of the Arakelov class group. Combining them, one can develop a much faster method for solving the Pell equation than is possible with the continued fraction method alone. The resulting technique is explained in considerable detail in the book by Jacobson and Williams. Given that the entire method effectively operates in the Arakelov class group, it is somewhat surprising that the authors have chosen a presentation in which they mention that group only in passing (p. 176), while admitting that its practical impact is "currently unclear" to them. In general, their text is computationally and analytically much stronger than conceptually and algebraically, their novel definition of the notion of a *prime ideal* (p. 93) providing a further illustration.

As the authors are justified in emphasizing (p. ix), their book "is not intended to be used as a textbook". The early chapters, which treat the history of Pell's equation, are especially valuable. Regrettably, the thoroughness of the discourse is not matched by an adequate listing of original sources: the 28-page bibliography

invariably replaces the latter by more recent reprints, so that the historically naive reader may think of the contributions by Euler and Lagrange as belonging to the nineteenth century. The technical material that forms the core of the book can be profitably consulted by the many mathematicians who share the authors' belief that nothing can match the clarity of a formula when it comes to conveying a mathematical truth.

Clarity is of course in the eyes of the observer, and there are also mathematicians who see a difference between the medium and the message. David Mumford [7], drawing a parallel between art and mathematics, once compared the way of thinking that Galois (1811–1832) introduced into mathematics with the "light and air" of the English painter William Turner (1775–1851). It is this "light and air" that the present-day follower of Galois will vainly look for in the book. One does not encounter the battle of Hastings either, since, other than Neukirch and Geyer [8, Kap. I, §7, Aufgabe 3] would have us believe, the chronicle that we quoted is entirely apocryphal, having been invented by the English puzzle king Henry Dudeney (1857–1930) [2, nr. 129].

References

[1] J.-L. de la Grange, *Solution d'un problème d'arithmétique*, Mélanges de philosophie et de mathématique de la Société Royale de Turin **4** (1766–1769), 44–97 (this paper was written and submitted for publication in 1768, and it appeared in 1773; see [12, Chapter IV, §II]); *Œuvres*, vol. I, Gauthier-Villars, Paris, 1867, 669–731.

[2] H. E. Dudeney, *Amusements in mathematics*, Thomas Nelson and Sons, London, 1917.

[3] L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg, 1770. A Russian translation had already appeared in 1768/69. Edition used: *Opera omnia*, series prima, volumen primum, H. Weber (ed.), B. G. Teubner, Leipzig and Berlin, 1911.

[4] L. Euler, *Elements of algebra*, translated from the French [by J. Hewlett and F. Horner], two volumes, J. Johnson, London, 1797.

[5] J. E. Hofmann, *Studien zur Zahlentheorie Fermats (Über die Gleichung $x^2 = py^2 + 1$)*, Abh. Preuss. Akad. Wiss. Math.-Nat. Kl. 1944 (1944), no. 7, 19 pp.

[6] H. W. Lenstra, *On the calculation of regulators and class numbers of quadratic fields*, J. Armitage (ed.), Journées Arithmétiques, 1980, London Math. Soc. Lecture Note Ser. **56**, Cambridge University Press, Cambridge, 1982, 123–150.

[7] D. Mumford, *The lure of the abstract: tracing the parallel influences of the Zeitgeist on art and mathematics in the last 200 years*, unpublished lecture.

[8] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992. The English translation *Algebraic number theory* (1999) corrects the error, but the 2002 reprint of the German original doesn't; one senses the influence of the GCHQ.

[9] René Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 447–495. MR2467554 (2009k:11212)

[10] Daniel Shanks, *The infrastructure of a real quadratic field and its applications*, Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972), Univ. Colorado, Boulder, Colo., 1972, pp. 217–224. MR0389842 (52 #10672)

[11] A. Weil, *Number theory, an approach through history*, Birkhäuser, Boston, 1984.

Hendrik Lenstra
Universiteit Leiden
E-mail address: hwl@math.leidenuniv.nl

Peter Stevenhagen
Universiteit Leiden
E-mail address: psh@math.leidenuniv.nl