HIGHER DESCENT ON PELL CONICS. I. FROM LEGENDRE TO SELMER

FRANZ LEMMERMEYER

Introduction

The theory of Pell's equation has a long history, as can be seen from the huge amount of references collected in Dickson [Dic1920], from the two books on its history by Konen [Kon1901] and Whitford [Whi1912], or from the books by Weber [Web1939], Walfisz [Wal1952], Faisant [Fai1991], and Barbeau [Bar2003]. For the better part of the last few centuries, the continued fractions method was the undisputed method for solving a given Pell equation, and only recently faster methods have been developed (see the surveys by Lenstra [Len2002] and H.C. Williams [Wil2002]).

This is the first in a series of articles which have the goal of developing a theory of the Pell equation that is as close as possible to the theory of elliptic curves: we will discuss 2-descent on Pell conics, introduce Selmer and Tate-Shafarevich groups, and prove an analogue of the Birch–Swinnerton-Dyer conjecture.

In this article, we will review the history of results that are related to this new interpretation. We will briefly discuss the construction of explicit units in quadratic number fields, and then deal with Legendre's equations and the results of Rédei, Reichardt and Scholz on the solvability of the negative Pell equation.

The second article [Lem2003a] is devoted to instances of a "second 2-descent" in the mathematical literature from Euler to our times, and in [Lem2003b] we will discuss the first 2-descent and the associated Selmer and Tate-Shafarevich groups from the modern point of view.

1. Explicit Units

Since finding families of explicit units in number fields is only indirectly related to our topic, we will be rather brief here. The most famous families of explicitly given units live in fields of Richaud-Degert type: if $d = b^2 + m$ and $b \mid 4m$, then $\alpha = b + \sqrt{d}$ has norm $-m$, hence is a unit if $m \in \{\pm 1, \pm 4\}$; if α is not a unit, then $\frac{1}{m}\alpha^2$ is.

Brahmagupta observed in 628 AD that if $a^2 - nb^2 = k$, then $x = \frac{2ab}{k}$, $y = \frac{a^2+nb^2}{k}$ satisfy the Pell equation $x^2 - ny^2 = 1$. If $k = \pm 1, \pm 2$, these solutions are integral; if $k = \pm 4$, Brahmagupta showed how to construct an integral solution. Note that x and y are necessarily integral if k divides the squarefree integer n.

According to C. Henry (see [Mab1879] and Dickson [Dic1920, v. II, p. 353]), Malebranche (1638–1715) claimed that the Pell equation $Ax^2 + 1 = y^2$ can be solved easily if $A = b^2 + m$ with $m|2b$.

Euler mentioned in [Eul1765, p. 99] and later again in [Eul1773] that if $d = b^2c^2 \pm 2b$ or $d = b^2c^2 \pm b$, then the Pell equation $x^2 - dy^2 = 1$ can be solved explicitly. This result was rediscovered often, for example by M. Stern [Ste1834], Richaud [Ric1865b], Hart [Har1878b], Speckman [Spe1895] and Degert [Deg1958]. Special cases are due to Moreau [Mor1873], de Jonquières [Jon1898],Ricalde [Ri1901], Boutin [Bou1902], Malo [Mal1906], and von Thielmann [vTh1926]. The quadratic fields $\mathbb{Q}(\sqrt{d}\,)$ with $d = a^2 \pm r$ and $r \mid 2a$ were called fields of Richaud-Degert type by Hasse [Has1965]. Over time, the problems treated in these articles changed from simply writing down a solution (e.g. $(x, y) = (m, 1)$ for $x^2 - (m-1)y^2 = 1$) to showing that such a solution is fundamental (i.e., minimal) except for at most finitely many, explicitly given values of m: see e.g. Nagell [Nag1925], Schepel [Sch1932], and Degert [Deg1958]. Degert's results were generalized by Yokoi [Yok1968, Yok1970], Kutsuna [Kut1974], Katayama [Kat1991, Kat1992], Nordhoff [Nor1974], Takaku & Yoshimoto [TY1993], Ramasamy [Ram1994], and Mollin [Mol1997].

The results about units in "fields of Richaud-Degert type" had actually been generalized long before Degert. Observe that the computation of the fundamental solution of $X^2 - dY^2 = 1$ for $d = m^2 + 1$ with the method of continued fractions is trivial because the development of $\sqrt{d}$ has period 1. Similarly, the development of $\sqrt{d}$ for d of Richaud-Degert type have small periods; here are some examples:

- $d = k^2 + k$: $\sqrt{d} = [k, \overline{2, 2k}]$;
- $d = k^2 + 2k$: $\sqrt{d} = [k, \overline{1, 2k}]$;
- $d = a^2k^2 + a$: $\sqrt{d} = [ak, \overline{2k, 2ak}]$;
- $d = a^2k^2 + 2a$: $\sqrt{d} = [ak, \overline{k, 2ak}]$.

Actually, already Euler [Eul1765] gave the continued fraction expansions for $d = n^2+1$, n^2+2, n^2+n, $9n^2+3$ and a few other values of d; he did, however, not show that the units he obtained were fundamental.

Perron [Per1913] gave examples of polynomials $f(x)$ for which the continued fraction expansion of $\sqrt{f(x)}$ can be given explicitly; the period lengths of his examples were ≤ 6. More examples were given by Yamamoto [Yam1971] and Bernstein [Ber1976, Ber1976] (who produced units whose continued fraction expansions have arbitrarily long period), as well as by Azuhata [Azu1984, Azu1987], Tomita [Tom1995, Tom1997], Levesque & Rhin [Lev1988], Levesque [Lev1988], Madden [Mad2001], Mollin [Mol2001], H.C. Williams [Wil2002], van der Poorten & H.C. Williams [PW1999], J. McLaughlin [McL2003, McL2003], and probably many others.

Nathanson [Nat1976] proved that $X^2 - DY^2 = 1$, where $D = x^2 + d$, has nontrivial solutions $X, Y \in \mathbb{Z}[x]$ if and only if $d = \pm 1, \pm 2$. This result was generalized by Hazama [Haz1997] and by Webb & Yokota [WY2003]. For connections with elliptic curves, see Berry [Ber1990] and Avanzi & Zannier [AZ2001]. In a recent article, Yu [Yu2001] explains connections between the solvability of the Pell equation over function fields $K(X)$ and the arithmetic of hyperelliptic curves; the main problem is whether there is a divisor of the form $n(\infty_+ - \infty_-)$ in the quadratic function field associated to the Pell equation $x^2 - Dy^2 = 1$, where D is a squarefree polynomial with even degree and whose leading coefficient is a square. This problem actually goes back to Abel [Abe1826].

2. Legendre

2.1. **Legendre's Théorie des Nombres.**

§ VII of Legendre's book [Leg1830] on number theory had the title

> Théorèmes sur la possibilité des équations de la forme $Mx^2 - Ny^2 = \pm 1$ ou ± 2.[1]

Legendre starts his investigation by assuming that A is prime, and that p and q are the smallest positive solutions of the equation

$$p^2 - Aq^2 = 1. \tag{1}$$

Writing this equation as $(p-1)(p+1) = Aq^2$ he deduces that $q = fgh$ with $f \in \{1, 2\}$ and

$$\left.\begin{array}{rcl} p+1 &=& fg^2A \\ p-1 &=& fh^2 \end{array}\right\} \quad \text{or} \quad \left.\begin{array}{rcl} p+1 &=& fg^2 \\ p-1 &=& fh^2A \end{array}\right\}$$

Subtracting these equations from each other he gets equations of the form $\pm\frac{2}{f} = x^2 - Ay^2$. The case $f = \pm 1$ leads to contradictions modulo

[1] Theorems on the solvability of the equations of the form $Mx^2 - Ny^2 = \pm 1$ or ± 2.

4, the case $f = 2$ contradicts the minimality of p and q, thus we must have $f = -2$ and therefore $-1 = x^2 - Ay^2$ (see [Leg1830, p. 55]).

Similar arguments easily yield

Proposition 2.1. *Let p be a prime.*

1. *If $p \equiv 1 \bmod 4$, then $X^2 - pY^2 = -1$ has integral solutions.*
2. *If $p \equiv 3 \bmod 8$, then $X^2 - pY^2 = -2$ has integral solutions.*
3. *If $p \equiv 7 \bmod 8$, then $X^2 - pY^2 = +2$ has integral solutions.*

Next Legendre considers composite values of A: if $A = MN$ is the product of two odd primes $\equiv 3 \bmod 4$, then he shows that $Mx^2 - Ny^2 = \pm 1$ is solvable;[2] if $M \equiv N \equiv 1 \bmod 4$, however, none of the equations $x^2 - MNy^2 = -1$ and $Mx^2 - Ny^2 = \pm 1$ can be excluded. He also states that for given A at most one of these equations can have a solution, but the argument he offers is not conclusive.

He then treats the general case and comes to the conclusion

> Étant donné un nombre quelquonque non quarré A, il est toujours possible de décomposer ce nombre en deux facteurs M et N tels que l'une des deux équations $Mx^2 - Ny^2 = \pm 1$, $Mx^2 - Ny^2 = \pm 2$ soit satisfaite, en prenant convenablement le signe du second membre.[3]

Again, Legendre adds the remark that among these equations there is exactly one which is solvable; he gives a different argument this time, which again is not conclusive since he is only working with the minimal solution of the Pell equation.

2.2. **Dirichlet's Exposition.** Dirichlet [Dir1834] gave an exposition of Legendre's technique, which we will quote now; his § 1 begins

> Wir beginnen mit einer kurzen Darstellung der Legendre'schen Methode. Es bezeichne A eine gegebene positive Zahl ohne quadratischen Factor, d.h. deren Primfactoren alle von einander verschieden sind, und es seien p und q die kleinsten Werthe ($p = 1$ und $q = 0$ ausgenommen), welche der bekanntlich immer lösbaren Gleichung:
>
> $$p^2 - Aq^2 = 1 \qquad (1)$$

[2]Using the solvability of $Mx^2 - Ny^2 = 1$ for primes $M \equiv N \equiv 3 \bmod 4$, Legendre later proved a special case of the quadratic reciprocity law, namely that $(\frac{p}{q}) = -(\frac{q}{p})$ for such primes.

[3]Given an arbitrary nonsquare number A it is always possible to decompose this number into two factors M and N such that one of the two equations $Mx^2 - Ny^2 = \pm 1$, $Mx^2 - Ny^2 = \pm 2$ is satisfied, the sign of the second number being conveniently taken.

> Bringt man dieselbe in die Form $(p+1)(p-1) = Aq^2$, und bemerkt man, dass $p+1$ und $p-1$ relative Primzahlen sind oder bloss den gemeinsamen Factor 2 haben, je nachdem p gerade oder ungerade ist, so sieht man, dass die Gleichung (1) im ersten Falle die folgenden nach sich zieht:
>
> $$p+1 = Mr^2, \quad p-1 = Ns^2, \quad A = MN, \ q = rs,$$
>
> und ebenso im zweiten:
>
> $$p+1 = 2Mr^2, \quad p-1 = 2Ns^2, \quad A = MN, \ q = 2rs,$$
>
> wo M, N und mithin r, s durch p völlig bestimmt sind. Es sind nämlich M, N im ersten Fall respective die grössten gemeinschaftlichen Theiler von A, $p+1$ und A, $p-1$, im andern dagegen von A, $\frac{p+1}{2}$ und A, $\frac{p-1}{2}$. Aus diesen Gleichung folgt
>
> $$Mr^2 - Ns^2 = 2, \quad Mr^2 - Ns^2 = 1. \tag{2}$$
>
> Hat man die Gleichung (1) nicht wirklich aufgelöst, und ist also p nicht bekannt, so weiss man bloss, dass eine dieser Gleichungen stattfinden muss, und da unter dieser Voraussetzung M und N nicht einzeln gegeben sind, so enthält jede der Gleichungen (2) mehrere besondere Gleichungen, die man erhält, indem man successive für M alle Factoren von A (1 und A mit eingeschlossen) nimmt und $N = \frac{A}{M}$ setzt. [4]

Thus we have

[4]We start with a short presentation of Legendre's method. Let A denote a given positive number without quadratic factors, i.e., whose prime factors are all pairwise distinct, and let p and q be the smallest values (except $p = 1$ and $q = 0$) satisfying the equation (1), which is known to be always solvable. Writing (1) in the form $(p+1)(p-1) = Aq^2$ and observing that $p+1$ and $p-1$ are relatively prime or have the common factor 2 according as p is even or odd, it can be seen that the equation (1) in the first case implies the following:

$$p+1 = Mr^2, \quad p-1 = Ns^2, \quad A = MN, \ q = rs,$$

and similarly in the second case:

$$p+1 = 2Mr^2, \quad p-1 = 2Ns^2, \quad A = MN, \ q = 2rs,$$

where M, N and therefore r, s are completely determined by p. In fact, M, N are, in the first case, the greatest common divisors of A, $p+1$ and A, $p-1$, in the second case of A, $\frac{p+1}{2}$ and A, $\frac{p-1}{2}$. From these equations we deduce (2).

If we do not have a solution of (1), thus if p is not known, then we only know that one of these equations must have a solution, and since under this assumption M and N are not given explicitly, each of the equations (2) contains several equations

Proposition 2.2. *The solvability of the Pell equation $X^2 - AY^2 = 1$ implies the solvability of one of the equations $Mr^2 - Ns^2 = 1$ or $Mr^2 - Ns^2 = 2$, where $MN = A$.*

This set of auxiliary equations (2) was derived using continued fractions by Arndt [Arn1845, Arn1846], as well as by Richaud [Ric1865a, Ric1865b] and Roberts [Rob1879]. Catalan [Cat1867] also studied the equations (2).

Legendre's method, Dirichlet writes, consists in showing that all but one of the equations in Prop. 2.2 are unsolvable, thus demonstrating that the remaining equation must have integral solutions. Dirichlet then shows how to apply this technique by proving Legendre's Proposition 2.1 as well as the following result:

Proposition 2.3. *Let p denote a prime.*

(1) *If $p \equiv 3 \bmod 8$, then $pr^2 - 2s^2 = 1$ has integral solutions.*
(2) *If $p \equiv 5 \bmod 8$, then $2pr^2 - s^2 = 1$ has integral solutions.*
(3) *If $p \equiv 7 \bmod 8$, then $2r^2 - ps^2 = 1$ has integral solutions.*

If $p \equiv 1 \bmod 8$, either of the three equations may be solvable.

2.3. **Richaud.** These results were extended to d having many prime factors by Richaud. In [Ric1864], he states without proof some results of which the following are special cases (Richaud considered values of d that were not necessarily squarefree):

Proposition 2.4. (1) *If p and q are primes congruent to $5 \bmod 8$, then the equations $X^2 - 2pY^2 = -1$ and $X^2 - 2pqY^2 = -1$ are solvable in integers.*
(2) *If p, q and r are primes congruent to $5 \bmod 8$, and if $(2p/q) = (2p/r) = -1$, then the equation $X^2 - 2pqrY^2 = -1$ is solvable in integers.*
(3) *If $p \equiv 5 \bmod 8$ and $a \equiv b \equiv 1 \bmod 8$ are primes such that $(2p/a) = (2p/b) = -1$, then the equations $X^2 - 2apY^2 = -1$ and $X^2 - 2abpY^2 = -1$ are solvable in integers.*
(4) *If $p \equiv q \equiv 5 \bmod 8$ and $a \equiv 1 \bmod 8$ are primes such that $(pq/a) = -1$, then the equation $X^2 - 2apqY^2 = -1$ is solvable in integers.*

Here are some results from Richaud [Ric1865a, Ric1865b, Ric1866]:

Proposition 2.5. *Let p_i denote primes.*

---

which we get by letting M run through all factors of A (including 1 and A) and putting $N = \frac{A}{M}$.

(1) *If* $d = p_1p_2p_3p_4$, $p_i \equiv 5 \bmod 8$, *if* $X^2 - p_1p_2p_3Y^2 = -1$, *and if* $(p_4/p_1) = (p_4/p_2) = (p_4/p_3) = 1$, *then* $X^2 - dY^2 = -1$ *is solvable. This generalizes to arbitrary numbers of primes.*

(2) *If* $d = p_1p_2p_3p_4$, $p_i \equiv 5 \bmod 8$, *if* $X^2 - p_1p_2p_3Y^2 = -1$, *and if* $(p_1/p_3) = (p_2/p_3) = -1$, $(p_1/p_4) = (p_2/p_4) = (p_3/p_4) = -1$, *then* $X^2 - dY^2 = -1$ *is solvable. This generalizes to arbitrary numbers of primes.*

(3) *If* $d = p_1p_2p_3p_4$, *where* $p_1 \equiv \ldots \equiv p_4 \equiv 5 \bmod 8$, *then* $X^2 - dY^2 = -1$ *is solvable if* $(p_1p_2/p_3) = (p_1p_2/p_4) = (p_3p_4/p_1) = (p_3p_4/p_2)$.

The following result is due to Tano [Tan1889]; the special case $n = 3$ was already proved by Dirichlet.

Proposition 2.6. *Let* $p_1, \ldots, p_n$ *denote primes* $p_i \equiv 1 \bmod 4$, *where* $n \geq 3$ *is an odd number, and put* $d = p_1 \cdots p_n$. *Assume that* $(p_i/p_j) = +1$ *for at most one pair* (i, j). *Then* $X^2 - dY^2 = -1$ *has an integral solution.*

Proposition 2.6 was generalized by Trotter [Tro1969], who was motivated by the results of Pumplün [Pum1968]:

Proposition 2.7. *Let* $p_1, \ldots, p_n$, *where* n *is an odd integer, denote primes* $p_i \equiv 1 \bmod 4$. *If there is no triple* i, j, k *such that* $(p_i/p_j) = (p_j/p_k) = +1$, *then* $X^2 - dY^2 = -1$ *has an integral solution.*

Newman [New1977] rediscovered a weaker form of Proposition 2.6: he assumed that $(p_i/p_j) = -1$ for all $i \neq j$.

There are a lot more results of this kind concerning the solvability of the negative Pell equation $X^2 - dY^2 = -1$ in terms of Legendre symbols than we can (or may want to) mention here. We will see in [Lem2003b] that these results can be interpreted as computations of Selmer groups for certain types of discriminants.

In fact, as Dickson [Dic1930, §25] observed, Legendre's set of equations $Mr^2 - Ns^2 = 1, 2$ admit a group structure; in modern language, it is induced by identifying $Mr^2 - Ns^2 = 1$ and $Mr^2 - Ns^2 = 2$ with the elements $M\mathbb{Q}^{\times 2}$ and $2M\mathbb{Q}^{\times 2}$ of the multiplicative group $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. This group will be called the 2-Selmer group of the corresponding Pell equation (see [Lem2003b]).

3. Dirichlet

After having explained Legendre's technique, Dirichlet [Dir1834] refines this method by invoking the quadratic reciprocity law. His first result going beyond Legendre is the following (for information on quartic residue symbols see [Lem2000]):

Proposition 3.1. *For primes $p \equiv 9 \bmod 16$ such that $(2/p)_4 = -1$, the equation $2pr^2 - s^2 = 1$ has an integral solution.*

Proof. Consider the equation $2r^2 - ps^2 = 1$. We see that s is odd, and that $(2/s) = +1$. Thus $s \equiv \pm 1 \bmod 8$, therefore $s^2 \equiv 1 \bmod 16$, and then $2r^2 \equiv 2 \bmod 16$ and $p \equiv 9 \bmod 16$ yield a contradiction.

Next consider $pr^2 - 2s^2 = 1$. Here $1 = (2/p)_4(s/p)$, and $(s/p) = (p/s) = 1$. Thus solvability implies $(2/p)_4 = 1$, which is a contradiction. □

Dirichlet next considers other cases where d has two or three prime factors; we are content with mentioning

Proposition 3.2. *Let $p \equiv q \equiv 1 \bmod 4$ be distinct primes.*

(1) *If $(p/q) = -1$, then $s^2 - pqr^2 = -1$ has an integral solution.*
(2) *If $(p/q)_4 = (q/p)_4 = -1$, then $s^2 - pqr^2 = -1$ has an integral solution.*

Using similar as well as some other techniques, Dirichlet's results such as Propositions 3.1 and 3.2 were generalized by Tano [Tan1889].

Dirichlet was the first to give a complete proof for Legendre's claim that there is essentially only one among the equations derived by Legendre which has an integral solution:

Theorem 3.3. *Let A be a positive squarefree integer. Then there is exactly one pair of positive integers $(M, N) \neq (1, A)$ with $MN = d$ such that $Mr^2 - Ns^2 = 1$ or $Mr^2 - Ns^2 = 2$ is solvable.*

Proof (Dirichlet). We know that all solutions of the Pell equation $P^2 - AQ^2 = 1$ are given by $P + Q\sqrt{A} = \pm(p + q\sqrt{A})^m$, where $m \in \mathbb{Z}$ and where $p + q\sqrt{A}$ is the fundamental solution. Up to sign we thus have $P = \frac{1}{2}((p + q\sqrt{A})^m + (p - q\sqrt{A})^m)$. This shows that $P \equiv p^m \bmod A$.

Assume first that m is odd. Then $P \equiv p \bmod 2$. If p is even, then we have

$$p \equiv -1 \bmod M, \qquad p \equiv 1 \bmod N,$$

which implies that

$$P \equiv -1 \bmod M, \qquad P \equiv 1 \bmod N.$$

Thus $P + Q\sqrt{A}$ leads to the very same equation $Mr^2 - Ns^2 = 2$ as the fundamental solution $p + q\sqrt{A}$. If p is odd, then we find similarly that

$$p \equiv -1 \bmod 2M, \qquad p \equiv 1 \bmod 2N,$$

and again $P + Q\sqrt{A}$ leads to the same equation $Mr^2 - Ns^2 = 1$ as $p + q\sqrt{A}$.

Finally, if m is even, then it is easy to see that $P + Q\sqrt{A}$ leads to $r^2 - As^2 = 1$. This shows that there are exactly two equations with integral solutions. □

Proofs of results equivalent to Theorem 3.3, based on the theory of continued fractions, were given by Petr [Pet1926, Pet1927] and Halter-Koch [HaK1987]; different proofs are due to Nagell [Nag1954], Kaplan [Kap1983], and Mitkin [Mit1997]; Trotter [Tro1969] proved the special case where the fundamental unit has negative norm. Pall [Pal1969] showed that Theorem 3.3 follows easily from a result that Gauss proved in his Disquisitiones Arithmeticae. See also Walsh [Wal1988, Wal2002].

In the ideal-theoretic interpretation, Theorem 3.3 says that if $K = \mathbb{Q}(\sqrt{d}\,)$ has a fundamental unit of norm $+1$, then there is exactly one nontrivial relation in the strict class group among the ambiguous ideals, the trivial relation coming from the factorization of the principal ideal $(\sqrt{d}\,)$: in fact, $Mr^2 - Ns^2 = 1$ is solvable if and only if $(Mr)^2 - ds^2 = M$ is, which is true if and only if the unique ideal $(M, \sqrt{d}\,)$ of norm M (remember that M divides the discriminant, so the ideals above the primes dividing m are ambiguous) is principal in the strict sense. From this point of view, Theorem 3.3 is an important step in the proof of the ambiguous class number formula for quadratic number fields.

4. Rédei, Reichardt, Scholz

In 1932, Rédei started studying the 2-class group of the quadratic number field $k = \mathbb{Q}(\sqrt{d}\,)$, and applied his results in [Red1935a] to problems concerning the solvability of the negative Pell equation $X^2 - dY^2 = -4$. In the following, let e_2 and e_4 denote the 2-rank and the 4-rank of the class group $C = \mathrm{Cl}_2^+(k)$ of k in the strict sense, that is, put $e_2 = \dim_{\mathbb{F}_2} C/C^2$ and $e_4 = \dim_{\mathbb{F}_2} C^2/C^4$. A factorization of the discriminant $d = \operatorname{disc} k$ into discriminants $d = \Delta_1\Delta_2$ is called a splitting of the second kind (or C_4-decomposition) if $(\Delta_1/p_2) = (\Delta_2/p_1) = +1$ for all primes $p_i \mid \Delta_i$.

Rédei (see e.g. [Red1937]) introduced a group structure on the set of splittings of the second kind by taking the product of two such factorizations $d = \Delta_1\Delta_2$ and $d = \Delta_1'\Delta_2'$ to be the factorization $d = \Delta_1''\Delta_2''$, where

$$\Delta_1'' = \frac{\Delta_1\Delta_1'}{\gcd(\Delta_1, \Delta_1')^2}.$$

This product is well defined because of the relations

$$\frac{\Delta_1\Delta_1'}{\gcd(\Delta_1, \Delta_1')^2} = \frac{\Delta_2\Delta_2'}{\gcd(\Delta_2, \Delta_2')^2}, \quad \frac{\Delta_1\Delta_2'}{\gcd(\Delta_1, \Delta_2')^2} = \frac{\Delta_2\Delta_1'}{\gcd(\Delta_2, \Delta_1')^2}.$$

A simple calculation shows that if $\Delta_1\Delta_2$ and $\Delta_1'\Delta_2'$ are splittings of the second kind, then so is $\Delta_1''\Delta_2''$. This makes the splittings of the second kind into an elementary abelian 2-group; in particular, it has the structure of an $\mathbb{F}_2$-vector space, and we have the notion of independent splittings.

The main result of [Red1932] (see also [RR1933]) is

Proposition 4.1. *The 4-rank e_4 equals the number of independent splittings of the second kind of d.*

This result of Rédei turned out to be very attractive; new variants of proofs were given by Iyanaga [Iya1935], Bloom [Blo1976], Carroll [Car1976], and Kisilevsky [Kis1976]. Inaba [Ina1940], Fröhlich [Fro1954a] and G. Gras [Gra1973] investigated the ℓ-class group of cyclic extensions of prime degree ℓ; see Stevenhagen [Ste1993a] for a modern exposition. For generalization's of Rédei's technique to quadratic extensions of arbitrary number fields see G. Gras [Gra1992]. Morton [Mor1979] and Lagarias [Lag1980a] gave modern accounts of Rédei's method for computing the 2-part of the class groups of quadratic number fields.

Damey & Payan [DP1970] proved

Proposition 4.2. *Let $k^+ = \mathbb{Q}(\sqrt{m}\,)$ be a real quadratic number field, and put $k^- = \mathbb{Q}(\sqrt{-m}\,)$. Then the 4-ranks $r_4^+(k^+)$ and $r_4(k^-)$ of $\mathrm{Cl}^+(k^+)$ (the class group of k^+ in the strict sense) and $\mathrm{Cl}(k^-)$ satisfy the inequalities $r_4^+(k^+) \le r_4(k^-) \le r_4^+(k^+) + 1$.*

Other proofs are due to G. Gras [Gra1973], Halter-Koch [HK1984], Uehara [Ueh1989] and Sueyoshi [Sue1995]; see also Sueyoshi [Sue1997, Sue2000]. Bouvier [Bou1971a, Bou1971b] proved that the 4-ranks and 8-ranks of $\mathbb{Q}(\sqrt{2}, \sqrt{m}\,)$ and $\mathbb{Q}(\sqrt{2}, \sqrt{-m}\,)$ differ at most by 4. This was generalized considerably by Oriat [Ori1976, Ori1977a, Ori1977b]; the following proposition is a special case of his results:

Proposition 4.3. *Let k be a totally real number field with odd class number, let $2^m \ge 4$ be an integer with the property that k contains the maximal real subfield of the field of 2^m-th roots of unity, and let $d \in k^\times$ be a nonsquare. Then the 2^m-ranks $r_m(K)$ and $r_m(K')$ of the class groups in the strict sense of $K = k(\sqrt{d}\,)$ and $K' = k(\sqrt{-d}\,)$ satisfy*

$$r_m(K) - r_m(K') \le R^- - r,$$

where R^- and r denote the unit rank of K^- and k, respectively.

Rédei & Reichardt [RR1933, Red1953] and Iyanaga [Iya1935] observed the following

Proposition 4.4. *If* $\mathrm{Cl}_2^+(k)$ *is elementary abelian, then* $N\varepsilon = -1$.

Since $e_4 = 0$ is equivalent to the rank of $R(d)$ being maximal, this can be expressed by saying that if the Rédei matrix has maximal possible rank $n-1$, then $N\varepsilon = -1$.

Rédei introduced what is now called the Rédei matrix of the quadratic field with discriminant $d = d_1 \cdots d_n$. It is defined as the $n \times n$-matrix $R(d) = (a_{ij})$ over $\mathbb{F}_2$ with the $a_{ij} \in \mathbb{F}_2$ defined as follows. Write $(a/p) = (-1)^{[a,p]}$ with $[a,p] \in \{0,1\}$ and set $a_{ij} = [d_i, p_j]$ for $i \neq j$ and $a_{ii} = \sum_{i \neq j} a_{ij}$. Rédei proved that the 4-rank of $\mathrm{Cl}^+(k)$ is given by

$$e_4 = n - 1 - \operatorname{rank} R(d).$$

Rédei & Reichardt [RR1933] and Scholz [Sch1934] started applying class field theory to finding criteria for the solvability of the negative Pell equation $X^2 - dY^2 = -4$. The immediate connection is provided by the following simple observation: we have $N\varepsilon = -1$ if and only if $\mathrm{Cl}(K) \simeq \mathrm{Cl}^+(K)$, which in turn is equivalent to the fact that the Hilbert class fields in the strict (unramified outside ∞) and in the usual sense (unramified everywhere) coincide. This proves

Proposition 4.5. *The fundamental unit of the quadratic field K has negative norm if and only if the Hilbert class field in the strict sense is totally real.*

The following theorem summarizes the early results of Rédei and Scholz; observe that 'unramified' below means 'unramified outside ∞':

Theorem 4.6. *Let k be a quadratic number field with discriminant d. There is a bijection between unramified cyclic C_4-extensions and C_4-factorizations of d.*

If K/k is an unramified C_4-extension, then $K/\mathbb{Q}$ is normal with $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$. The quartic normal extension $F/\mathbb{Q}$ contained in K can be written in the form $F = \mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2}\,)$. A careful examination of the decomposition and inertia groups of the ramifying primes shows that $(\Delta_1, \Delta_2) = 1$ and that $d = \Delta_1 \cdot \Delta_2$ is a C_4-factorization.

Conversely, if $d = \Delta_1\Delta_2$ is a C_4-factorization of d, then the diophantine equation $X^2 - \Delta_1 Y^2 = \Delta_2 Z^2$ has a nontrivial solution (x, y, z), and the extension $K = k(\sqrt{\Delta_1}, \sqrt{\mu}\,)$, where $\mu = x + y\sqrt{\Delta_1}$, is a C_4-extension of k unramified outside 2∞. By choosing the signs of x, y, z suitably one can make K/k unramified outside ∞.

The question of whether the cyclic quartic extension K/k constructed in Theorem 13.1. is real or not was answered by Scholz [Sch1934]. Clearly this question is only interesting if both Δ_1 and Δ_2 are positive.

Moreover, if one of them, say Δ_1, is divisible by a prime $q \equiv 3 \bmod 4$, then there always exists a real cyclic quartic extension K/k: this is so because $\alpha = x + y\sqrt{\Delta_1}$ as constructed above is either totally positive or totally negative (since it has positive norm), hence either $\alpha \gg 0$ or $-q\alpha \gg 0$, so either $k(\sqrt{\alpha}\,)$ or $k(\sqrt{-q\alpha}\,)$ is the desired extension. We may therefore assume that d is not divisible by a prime $q \equiv 3 \bmod 4$, i.e. that d is the sum of two squares. Then Scholz [Sch1934] has shown

Proposition 4.7. *Let k be a real quadratic number field with discriminant d, and suppose that d is the sum of two squares. Assume moreover that $d = \Delta_1 \cdot \Delta_2$ is a C_4-factorization. Then the cyclic quartic C_4-extensions K/k containing $\mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2}\,)$ are real if and only if $(\Delta_1/\Delta_2)_4(\Delta_2/\Delta_1)_4 = +1$. Moreover, if there exists an octic cyclic unramified extension L/k containing K, then $(\Delta_1/\Delta_2)_4 = (\Delta_2/\Delta_1)_4$.*

If Δ_1 and Δ_2 are prime, we can say more ([Sch1934]):

Theorem 4.8. *Let $k = \mathbb{Q}(\sqrt{d}\,)$ be a real quadratic number field, and suppose that $d = \operatorname{disc} k = \Delta_1\Delta_2$ is the product of two positive prime discriminants Δ_1, Δ_2. Let $h(k)$, $h^+(k)$ and ε denote the class number, the class number in the strict sense, and the fundamental unit of $\mathcal{O}_k$, respectively; moreover, let ε_1 and ε_2 denote the fundamental units of $k_1 = \mathbb{Q}(\sqrt{\Delta_1}\,)$ and $k_2 = \mathbb{Q}(\sqrt{\Delta_1}\,)$. There are the following possibilities:*

(1) $(\Delta_1/\Delta_2) = -1$*: then* $h(k) = h^+(k) \equiv 2 \bmod 4$*, and* $N\varepsilon = -1$.
(2) $(\Delta_1/\Delta_2) = +1$*: then* $(\varepsilon_1/\Delta_2) = (\varepsilon_2/\Delta_1) = (\Delta_1/\Delta_2)_4(\Delta_2/\Delta_1)_4$*, and 4.6 shows that there is a cyclic quartic subfield* K *of* k^1 *containing* k_1k_2*;*
i) $(\Delta_1/\Delta_2)_4 = -(\Delta_2/\Delta_1)_4$*: then* $h^+(k) = 2 \cdot h(k) \equiv 4 \bmod 8$*,* $N\varepsilon = +1$*, and* K *is totally complex;*
ii) $(\Delta_1/\Delta_2)_4 = (\Delta_2/\Delta_1)_4 = -1$*: then* $h^+(k) = h(k) \equiv 4 \bmod 8$*,* $N\varepsilon = -1$*, and* K *is totally real.*
iii) $(\Delta_1/\Delta_2)_4 = (\Delta_2/\Delta_1)_4 = +1$*: then* $h^+(k) \equiv 0 \bmod 8$*, and* K *is totally real.*

Here $(\Delta_1/\Delta_2)_4$ denotes the rational biquadratic residue symbol; like Jacobi symbols, it is defined in such a way that it becomes multiplicative in both numerator and denominator. Observe that $(\Delta_1/8)_4 = +1$ if $\Delta_1 \equiv 1 \bmod 16$ and $(\Delta_1/8)_4 = -1$ if $\Delta_1 \equiv 9 \bmod 16$. Moreover, (ε_1/p_2) is the quadratic residue character of $\varepsilon_1 \bmod \mathfrak{p}$ (if $p_2 \equiv 1 \bmod 4$), where $\mathfrak{p}$ is a prime ideal in k_1 above p_2; for $\Delta_2 = 8$ and $\Delta_1 \equiv 1 \bmod 8$, the symbol $(\varepsilon_1/8)$ is defined by $(\varepsilon_1/8) = (-1)^{T/4}$, where $\varepsilon_1 = T + U\sqrt{\Delta_1}$.

Corollary 4.9. *Let $p = \Delta_1$ and $q = \Delta_2 \equiv 1 \bmod 4$ be positive prime discriminants, and assume that Δ_2 is fixed; then*

$$\begin{aligned} 4|h^+(k) &\iff (\Delta_1/\Delta_2) = 1 &&\iff p \in \mathrm{Spl}(\Omega_4^+(\Delta_2)/\mathbb{Q}) \\ 4|h(k) &\iff (\Delta_1/\Delta_2)_4 = (\Delta_2/\Delta_1)_4 &&\iff p \in \mathrm{Spl}(\Omega_4(\Delta_2)/\mathbb{Q}) \\ 8|h^+(k) &\iff (\Delta_1/\Delta_2)_4 = (\Delta_2/\Delta_1)_4 = 1 &&\iff p \in \mathrm{Spl}(\Omega_4^+(\Delta_2)/\mathbb{Q}) \end{aligned}$$

Here, the *governing fields* $\Omega_j(\Delta_2)$ are defined by

$$\begin{aligned} \Omega_4^+(\Delta_2) &= \mathbb{Q}(i, \sqrt{\Delta_2}\,), \\ \Omega_4(\Delta_2) &= \Omega_4^+(\sqrt{\varepsilon_2}\,) = \mathbb{Q}(i, \sqrt{\Delta_2}, \sqrt{\varepsilon_2}\,), \\ \Omega_8^+(\Delta_2) &= \Omega_4(\sqrt[4]{\Delta_2}\,) = \mathbb{Q}(i, \sqrt[4]{\Delta_2}, \sqrt{\varepsilon_2}\,). \end{aligned}$$

The reason for studying governing fields comes from the fact that sets of primes splitting in a normal extension have Dirichlet densities. The existence of fields governing the property $8|h^+(k)$ allows us to conclude that there are infinitely many such fields. Governing fields for the property $8|h(k)$ or $16|h^+(k)$ are not known and conjectured not to exist. Nevertheless the primes $\Delta_1 = p$ such that $8 \mid h(k)$ (or $16 \mid h(k)$ etc.) appear to have exactly the Dirichlet density one would expect if the corresponding governing fields existed. Governing fields were introduced by Cohn and Lagarias [CL1981, CL1983] (see also Cohn's book [Coh1985]) and studied by Morton [Mor1982a, Mor1982b, Mor1983, Mor1990b, Mor1990a] and Stevenhagen [Ste1988, Ste1989, Ste1993b]. A typical result is

Proposition 4.10. *Let $p \equiv 1 \bmod 4$ and $r \equiv 3 \bmod 4$ be primes and consider the quadratic number field $k = \mathbb{Q}(\sqrt{-rp}\,)$. Then $8 \mid h(k) \iff (-r/p)_4 = +1$.*

More discussions on unramified cyclic quartic extensions of quadratic number fields can be found in Herz [Her1957], Vaughan [Vau1985], and Williams & Liu [WL1994]. Another discussion of Rédei's construction was given in Zink's dissertation [Zin1974].

The class field theoretical approach was also used by Rédei [Red1943, Red1953] (see Gerasim [Ger1990]), as well as Furuta [Fur1959], Morton [Mor1990b] and Benjamin, Lemmermeyer & Snyder [BLS1998].

The problem for values of d divisible by squares was treated (along the lines of Dirichlet) by Perott [Per1887] and taken up again by Rédei [Red1935a] and, via class field theory, by Jensen [Jen1962a, Jen1962b, Jen1962c] and Bülow [Bue2002]. Brown [Bro1983] proved a very special case of Scholz's results using the theory of binary quadratic forms; see also Kaplan [Kap1976]. Buell [Bue1989] gave a list of known criteria.

Despujols [Des1945] showed that the norm of the fundamental unit is $(-1)^{t-r}$, where t is the number of ramified primes, and 2^r the number of ambiguous ideal classes containing an ambiguous ideal.

5. Graphs of Quadratic Discriminants

In this section we will explain the graph theoretical description of classical results on the 4-rank of class groups (in the strict sense) of real quadratic number fields, and of solvability criteria of the negative Pell equation. The connection with graph theory was first described by Lagarias [Lag1980b] and used later by Cremona & Odoni [CO1989]. Similar constructions were used by Vazzana [Vaz1997a, Vaz1997b] for studying K_2 of the ring of integers $\mathcal{O}_k$, as well as by Heath-Brown [HB1993] and later by Feng [Fen1996], Li & Tian [LT2000], and Zhao [Zha1997, Zha2001] for describing the 2-Selmer group of elliptic curves $Y^2 = X^3 - d^2X$.

The Language of Graphs. A (nondirected) graph consists of a set V of vertices and a subset $E \subseteq V \times V$ whose elements are called edges.

The degree of a vertex d_i of a graph is the number of edges $(d_i, d_j) \in V$ adjacent to d_i. A graph is called Eulerian if all vertices have even degree; graphs are Eulerian if and only if there is a path through the graph passing each edge exactly once.

A tree is a connected graph containing no cycles (closed paths involving at least three vertices inside a graph). A subgraph of a graph γ is called a spanning tree of γ if it is a tree and if it contains all vertices.

Graphs of Quadratic Fields. Let d be the discriminant of a quadratic number field. Then d can be factored uniquely into prime discriminants: $d = d_1 \cdots d_n$. Here the d_i are discriminants of quadratic fields in which only one prime p_i is ramified.

Let d be a discriminant of a real quadratic number field such that all the d_i are positive (equivalently, d is the sum of two integral squares). This implies, by quadratic reciprocity, that $(d_i/p_j) = (d_j/p_i)$ for all $1 \le i, j \le n$.

To any discriminant d as above we associate a graph $\gamma(d)$ as follows:

- $V = \{d_1, \ldots, d_n\}$;
- $E = \{(d_i, d_j) : (d_i/p_j) = (d_j/p_i) = -1\}$.

Every factorization $d = \Delta_1\Delta_2$ of d into two discriminants Δ_1, Δ_2 of quadratic fields corresponds to a bipartitioning $\{A_1, A_2\}$ of the vertices by putting $A_1 = \{d_i : d_i \mid \Delta_1$ and $A_2 = \{d_i : d_i \mid \Delta_2$. Clearly we have $A_1 \cup A_2 = V$ and $A_1 \cap A_2 = \varnothing$, and if the factorization is nontrivial, we also have $A_1, A_2 \neq \varnothing$.

To each such bipartition, we associate a subgraph $\gamma(\Delta_1, \Delta_2)$ of $\gamma(d)$ by deleting all edges between vertices in V_1, and all edges between vertices in V_2; thus $\gamma(\Delta_1, \Delta_2)$ has vertices $V = V_1 \cup V_2$ and edges $E_{1,2} = \{(d_i, d_j) \in E : i \in V_1, j \in V_2\}$.

Lemma 5.1. *The factorization $d = \Delta_1\Delta_2$ is a C_4-decomposition if and only if $\gamma(\Delta_1, \Delta_2)$ is Eulerian.*

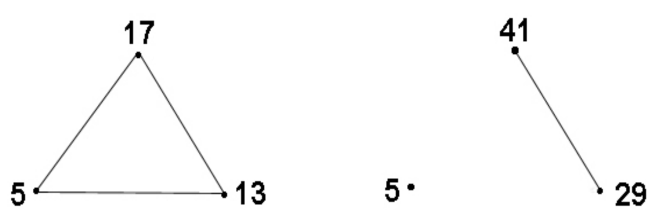
Proof. The graph $\gamma(\Delta_1, \Delta_2)$ is Eulerian if and only if for each $d_i \mid \Delta_1$ there is an even number of $d_j \mid \Delta_2$ such that $(d_j/p_i) = -1$. This is equivalent to $(\Delta_2/p_i) = +1$. The claim follows. $\square$

We call $\{A_1, A_2\}$ an Eulerian Vertex Decomposition (EVD) of $\gamma(d)$ if the subgraph $\gamma(\Delta_1, \Delta_2)$ is Eulerian. Since the number of C_4-decompositions equals the 4-rank e_2 of the class group in the strict class group of $k = \mathbb{Q}(\sqrt{d}\,)$, we see

Proposition 5.2. *The number of EVDs of $\gamma(d)$ is 2^{e_2}, where e_2 is the 4-rank of the class group of $k = \mathbb{Q}(\sqrt{d}\,)$ in the strict sense.*

The Rédei matrix can be interpreted as the adjacency matrix of a graph $\Gamma(d)$; if $V = V_1 \cup V_2$ and $V_1 \cap V_2 = \varnothing$, the graph with the same vertices as $\Gamma(d)$ and the edges within V_1 and V_2 deleted coincides with $\gamma(V_1, V_2)$.

The graph $\gamma(d)$ is said to be odd if it has the following property: for every bipartitioning of V, there is an $a_1 \in A_1$ that is joined to an odd number of $a_2 \in A_2$, or vice versa.



The graph $\gamma(5\cdot 13\cdot 17)$ is odd, the graph $\gamma(5\cdot 29\cdot 41)$ is not. Observe that the negative Pell equation is solvable in the first, but not in the second case.

Proposition 5.3. *Let the discriminant d of a quadratic number field be a sum of two squares. If $\gamma(d)$ is an odd graph, then $N\varepsilon = -1$.*

Proof. Let (x, y) be the solution of $X^2 - dY^2 = 1$ with minimal $y > 0$. Then x is odd, hence $x+1 = 2fr^2$, $x+1 = 2gs^2$, $fg = d$, $1 = fr^2 - gs^2$. If $g = 1$, then $N\varepsilon = -1$, and $f = 1$ contradicts the minimality of y. If

$f, g > 1$ then we claim that $1 = fr^2 - gs^2$ is not solvable in integers. Let $d = p_1 \cdots d_n$, $A = \{d_i : d_i \mid f\}$ and $B = \{d_i : d_i \mid g\}$. Then $A \cup B = V = \{d_1, \ldots, d_n\}$, $A \cap B = \varnothing$. Since $\gamma(d)$ is odd, we may assume that there is an $d_i \in A$ that is adjacent to an odd number of $d_j \in B$. This implies $(g/p_i) = -1$, contradicting the solvability of $1 = fr^2 - gs^2$. □

Lagarias observed that a congruence proved by Pumplün [Pum1968] could be interpreted as follows:

Proposition 5.4. *Let d be the discriminant of a quadratic number field. Then*

$$h^+(d) \equiv \sum_T \prod_{(d_i,d_j)\in T} \Big(1 - \Big(\frac{d_i}{p_j}\Big)\Big) \equiv 2^{n-1}\kappa_d \bmod 2^n,$$

where T runs over all spanning trees of the complete graph with n vertices, and where κ_d is the number of spanning trees of $\gamma(d)$.

This implies that Cl_2^+ is elementary abelian if and only if $\gamma(d)$ is an odd graph. This result is implicitly contained in Trotter [Tro1969].

Directed Graphs. If $d = p_1 \cdots p_n$ is a product of primes $p_i \equiv 3 \bmod 4$, then the graph with vertices $d_i = -p_i$ and adjacency matrix $A = (a_{ij})$ defined by

$$\Big(\frac{p_j}{p_i}\Big) = \begin{cases} (-1)^{a_{ij}} & \text{if } i \neq j \\ (-1)^{n+1}\big(\frac{d/p_i}{p_i}\big) & \text{if } i = j \end{cases}$$

is a directed graph (actually a tournament graph since each edge has a unique direction) studied by Kingan [Kin1995]. From Rédei's results, Kingan deduced the following facts (see also Sueyoshi [Sue2001]):

Proposition 5.5. *If n is even, then $r_4(d) = n - 1 - \operatorname{rank} A$ and $r_4(-d) = n - \operatorname{rank} A$ or $n - 1 - \operatorname{rank} A$.*

If n is odd, then $r_4(d) = n - 1 - \operatorname{rank} A$ or $r_4(d) = n - 2 - \operatorname{rank} A$, and $r_4(-d) = n - 2 - \operatorname{rank} A$.

Define c_i via $(-1)^{c_i} = (2/p_i)$ and put $v = (c_1, \ldots, c_n)^T$. Then in the cases where the rank formula is ambiguous, the greater value is attained if $v \in \operatorname{im}(A - I)$.

Kohno & Nakahara [KN1993] and Kohno, Kitamura, & Nakahara [KKN1992] used oriented graphs to describe Morton's results about governing fields and the computation of the 2-part of the class group of quadratic fields.

Parts of the theory of Rédei and Reichardt has been extended to function fields in one variable over finite fields; Ji [Ji1995] discussed decompositions of the second kind over function fields, and in [Ji1997] he proved results of Trotter [Tro1969] in this case, using the graph theoretic language discussed above.

Density Problems. In this section we will address the question for how many Δ the negative Pell equation $X^2 - \Delta Y^2 = -1$ is solvable. It was already noticed by Brahmagupta (see Whitford [Whi1912]) that the solvability implies that Δ must be a sum of two squares.

Consider therefore the set $\mathcal{D}$ of quadratic discriminants not divisible by any prime $\equiv 3 \bmod 4$, and let $\mathcal{D}(-1)$ denote the subset of all discriminants in $\mathcal{D}$ for which the negative Pell equation is solvable. The problem is then to determine whether the limit

$$\lim_{x\to\infty} \frac{\#\{\Delta \in \mathcal{D}(-1) : \Delta \leq x\}}{\#\{\Delta \in \mathcal{D} : \Delta \leq x\}} \tag{2}$$

exists, and if it does, to find it.

Such questions were first investigated by Nagell [Nag1933], and then by Rédei [Red1935b, Red1935c]; using criteria for the solvability of the negative Pell equation, Rédei could prove that

$$\liminf_{x\to\infty} \frac{\#\{\Delta \in \mathcal{D}(-1) : \Delta \leq x\}}{\#\{\Delta \in \mathcal{D} : \Delta \leq x\}} > \alpha := \prod_{j=1}^{\infty}(1 - 2^{1-2j}) = 0.419422\ldots,$$

a result later proved again by Cremona & Odoni [CO1989]. Stevenhagen [Ste1993c] gave heuristic reasons why the density in (2) should equal $1 - \alpha = 0.580577\ldots$.

Related questions concerning the density of quadratic fields whose class groups have given 4-rank were studied by Gerth [Ger1984, Ger1989] and Costa & Gerth [CG1995].

Observe that the negative Pell equation is just one among Legendre's equations; we might similarly ask for the density of discriminants $d \equiv 1 \bmod 8$ for which $2x^2 - dy^2 = 1$ is solvable, among all discriminants $d \equiv 1 \bmod 8$ whose prime factors are $\equiv \pm 1 \bmod 8$.

Selmer groups. The graph theoretic language introduced for studying the density of discriminants for which the negative Pell equation is solvable was also employed for computing the size of Selmer groups of elliptic curves with a rational point of order 2. See Heath-Brown [HB1993], Feng [Fen1996], Feng & Xiong [FX2004], Li & Tian [LT2000], and Zhao [Zha1997, Zha2001].

Acknowledgements

Ron Evans has read a preliminary draft of this article and corrected several misprints.

References

[Abe1826] N.H. Abel, *Über die Integration der Differential-Formel* $\frac{\sqrt{\rho}dx}{R}$*, wenn* R *und* ρ *ganze Functionen sind*, J. Reine Angew. Math. **1** (1826), 185–221 3

[Arn1845] F. Arndt, *Disquisitiones nonnullae de fractionibus continuis*, Diss. Sundia 1845, 32pp 5

[Arn1846] F. Arndt, *Bemerkungen über die Verwandlung der irrationalen Quadratwurzel in einen Kettenbruch*, J. Reine Angew. Math. **31** (1846), 343–358 5

[AZ2001] R.M. Avanzi, U.M. Zannier, *Genus one curves defined by separated variable polynomials and a polynomial Pell equation*, Acta Arith. **99** (2001), no. 3, 227–256 3

[Azu1984] T. Azuhata, *On the fundamental units and the class numbers of real quadratic fields* Nagoya Math. J. **95** (1984), 125–135 2

[Azu1987] T. Azuhata, *On the fundamental units and the class numbers of real quadratic fields. II*, Tokyo J. Math. **10** (1987), no. 2, 259–270 2

[Bar2003] E. Barbeau, *Pell's Equation*, Springer Verlag 2003 1

[BLS1998] E. Benjamin, F. Lemmermeyer, C. Snyder, *Real quadratic number fields with Abelian Gal(*k^2/k*)*, J. Number Theory **73** (1998), 182–194 13

[Ber1976] L. Bernstein, *Fundamental units and cycles in the period of real quadratic number fields. I*, Pacific J. Math. **63** (1976), 37–61 2

[Ber1976] L. Bernstein, *Fundamental units and cycles in the period of real quadratic number fields. II*, Pacific J. Math. **63** (1976), no. 1, 63–78 2

[Ber1990] T.G. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Arch. Math. (Basel) **55** (1990), no. 3, 259–266 3

[Blo1976] J. Bloom, *On the* 4*-rank of the strict class group of a quadratic number field*, Selected topics on ternary forms and norms (Sem. Number Theory, California Inst. Tech., Pasadena, Calif., 1974/75), Paper No. 8, 4 pp. California Inst. Tech., Pasadena, Calif., 1976 9

[Bou1902] A. Boutin, *Résolution complète de l'équation* $x^2-(Am^2+Bm+C)y^2=1$ *où* A, B, C *sont des entiers, par une infinité des polynômes en* m, L'Interméd. Math. **9** (1902), 60 2

[Bou1971a] L. Bouvier, *Sur le 2-groupe des classes de certains corps biquadratiques*, Thèse 3^e cycle, Grenoble 10

[Bou1971b] L. Bouvier, *Sur le 2-groupe des classes au sens restreint de certaines extensions biquadratiques de* $\mathbb{Q}$, C. R. Acad. Sci. Paris **272** (1971), 193–196 10

[Bro1983] E. Brown, *The class number and fundamental unit of* $Q(\sqrt{2p})$ *for* $p \equiv 1 \bmod 16$ *a prime*, J. Number Theory **16** (1983), no. 1, 95–99 13

[Bue1989] D. Buell, *Binary Quadratic Forms*, Springer Verlag 1989 13

[Bue2002] T. Bülow, *Power residue criteria for quadratic units and the negative Pell equation*, Canad. Math. Bull. **24** (2002), no. 2, 55–60 13

[Car1976] J. Carroll, *The Redei-Reichardt theorem*, Selected topics on ternary forms and norms (Sem. Number Theory, California Inst. Tech., Pasadena, Calif., 1974/75), Paper No. 7, 7 pp. California Inst. Tech., Pasadena, Calif., 1976 9

[Cat1867] E. Catalan, *Rectification et addition à la note sur un problème d'analyse indéterminée*, Atti dell'Accad. Pont. Nuovi Lincei **20** (1867), 1ff; 77ff 5

[Coh1985] H. Cohn, *Introduction to the Construction of Class Fields*, Cambridge 1985 13

[CL1981] H. Cohn, J. Lagarias, *Is there a density for the set of primes p such that the class number of $\mathbb{Q}(\sqrt{-p})$ is divisible by 16?*, Colloqu. Math. Soc. Bolyai **34** (1981), 257–280 13

[CL1983] H. Cohn, J. Lagarias, *On the existence of fields governing the 2-invariants of the class group of $\mathbb{Q}(\sqrt{dp})$ as p varies*, Math. Comp. **41** (1983), 711–730 13

[CG1995] A. Costa, F. Gerth, *Densities for 4-class ranks of totally complex quadratic extensions of real quadratic fields*, J. Number Theory **54** (1995), no. 2, 274–286 17

[CO1989] J.E. Cremona, R.W.K. Odoni, *Some density results for negative Pell equations; an application of graph theory*, J. Lond. Math. Soc. (2) **39** (1989), 16–28 13, 17

[DP1970] P. Damey, J.-J. Payan, *Existence et construction des extensions galoisiennes et non-abéliennes de degré 8 d'un corps de caractéristique differente de 2*, J. Reine Angew. Math. **244** (1970), 37–54 10

[Deg1958] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97 2

[Des1945] P. Despujols, *Norme de l'unité fondamentale du corps quadratique absolu*, C. R. Acad. Sci. Paris **221** (1945), 684–685 13

[Dic1920] L.E. Dickson, *History of the Theory of Numbers*, vol I (1920); vol II (1920); vol III (1923); Chelsea reprint 1952 1, 2

[Dic1930] L.E. Dickson, *Studies in the Theory of numbers*, Chicago 1930 7

[Dir1834] G.P.L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen*, Abh. Kön. Akad. Wiss. Berlin 1834, 649–664; Gesammelte Werke I, 221–236 4, 7

[Eul1765] L. Euler, *De usu novi algorithmi in problemate Pelliano solvendo*, Novi Acad. Sci. Petropol. **11** (1765) 1767, 28–66; Opera Omnia I-3, 73–111 2

[Eul1773] L. Euler, *Nova subsidia pro resolutione formulae $axx + 1 = yy$*, Sept. 23, 1773; Opusc. anal. **1** (1783), 310; Comm. Arith. Coll. **II**, 35–43; Opera Omnia I-4, 91–104 2

[Fai1991] A. Faisant, *L'équation diophantienne du second degré*, Hermann 1991 1

[Fen1996] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. **75** (1996), 71–83 13, 17

[FX2004] K. Feng, M. Xiong, *On elliptic curves $y^2 = x^3 - n^2x$ with rank zero*, J. Number Theory **109** (2004), 1–26 17

[Fro1954a] A. Fröhlich, *The generalization of a theorem of L. Rédei's*, Quart. J. Math. (2) **5** (1954), 130–140 9

[Fur1959] Y. Furuta, *Norm of units of quadratic fields*, J. Math. Soc. Japan **11** (1959), 139–145 13

[Ger1990] I.-Kh. I. Gerasim, *On the genesis of Rédei's theory of the equation $x^2 - Dy^2 = -1$* (Russian), Istor.-Mat. Issled. No. **32-33** (1990), 199–211 13

[Ger1984] F. Gerth, *The 4-class ranks of quadratic fields*, Invent. Math. **77** (1984), no. 3, 489–515 17

[Ger1989] F. Gerth, *The 4-class ranks of quadratic extensions of certain real quadratic fields*, J. Number Theory **33** (1989), no. 1, 18–31 17

[Gra1973] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l* I, II, Ann. Inst. Fourier **23** (1973), 1–48; ibid. **23** (1973), 1–44 9, 10

[Gra1992] G. Gras, *Sur la norme du groupe des unités d'extensions quadratiques relatives*, Acta Arith. **61** (1992), 307–317 10

[HK1984] F. Halter-Koch, *Über den 4-Rang der Klassengruppe quadratischer Zahlkörper*, J. Number Theory **19** (1984), 219–227 10

[HaK1987] F. Halter-Koch, *Über Pellsche Gleichungen und Kettenbrüche*, Arch. Math. **49** (1987), 29–37 8

[Har1878b] D.S. Hart, *A new method for solving equations of the form $x^2 - Ay^2 = 1$*, Educat. Times **28** (1878), 29 2

[Has1965] H. Hasse, *Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper*, Elem. Math. **20** (1965), 49–59 2

[Haz1997] F. Hazama, *Pell equations for polynomials*, Indag. Math. **8** (1997), 387–397 3

[HB1993] D.R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), 171–195 13, 17

[Her1957] C. S. Herz *Construction of Class Fields*, Seminar on complex multiplication (Chowla et al. eds.) (1957), Lecture Notes Math. 21, Springer Verlag 13

[Ina1940] E. Inaba, *Über die Struktur der l-Klassengruppe zyklischer Zahlkörper vom Primzahlgrad l*, J. Fac. Sci. Imp. Univ. Tokyo. Sect. I. **4** (1940), 61–115 9

[Iya1935] S. Iyanaga, *Sur les classes d'idéaux dans les corps quadratiques*, Actual. scient. et industr. 1935, Nr. 197 (Exposés math. VIII), 15 p. (1935) 9, 10

[Jen1962a] Ch. U. Jensen, *On the solvability of a certain class of non-Pellian equations*, Math. Scand. **10** (1962), 71–84 13

[Jen1962b] Ch. U. Jensen, *On the Diophantine equation $\xi^2 - 2m^2\eta^2 = -1$*, Math. Scand. **11** (1962), 58–62 13

[Jen1962c] Ch. U. Jensen, *Über eine Klasse nicht-Pellscher Gleichungen*, J. Reine Angew. Math. **209** (1962), 36–38 13

[Ji1995] C.G. Ji, *Norms of fundamental units in real quadratic function fields*, J. Nanjing Norm. Univ. Nat. Sci. Ed. **18** (1995), no. 4, 7–12 16

[Ji1997] C.G. Ji, *The norms of fundamental units in real quadratic function fields* J. Math. (Wuhan) **17** (1997), no. 2, 173–178 16

[Jon1898] E. de Jonquières, *Formules générales donnant des valeurs de D pour lesquelles l'équation $t^2 - Du^2 = -1$ est résoluble en nombres entiers*, C. R. Acad. Sci. Paris **126** (1898), 1837 2

[Kap1976] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. **283/284** (1976), 313–363 13

[Kap1983] P. Kaplan, *À propos des équations antipelliennes*, Enseign. Math. (2) **29** (1983), 323–327 8

[Kat1991] S. Katayama, *On fundamental units of real quadratic fields with norm -1*, Proc. Japan Acad. **67** (1991), 343–345 2

[Kat1992] S. Katayama, *On fundamental units of real quadratic fields with norm* +1, Proc. Japan Acad. **68** (1992), 18–20 2

[Kin1995] R.J. Kingan, *Tournaments and ideal class groups*, Canad. Math. Bull. **38** (1995), no. 3, 330–333 16

[Kis1976] H. Kisilevsky, *The Rédei-Reichardt theorem—a new proof*, Selected topics on ternary forms and norms (Sem. Number Theory, California Inst. Tech., Pasadena, Calif., 1974/75), Paper No. 6, 4 pp. California Inst. Tech., Pasadena, Calif., 1976 9

[KN1993] Y. Kohno, T. Nakahara, *Oriented graphs of* 2*-class group constructions of quadratic fields* (Japanese), Combinatorial structure in mathematical models (Kyoto, 1993), RIMS Kokyuroku **853**, (1993), 133–147 16

[KKN1992] Y. Kohno, S. Kitamura, T. Nakahara, 2*-rank component evaluation for class groups of quadratic fields using graphs* (Japanese), Optimal combinatorial structures on discrete mathematical models (Kyoto, 1992) Surikaisekikenkyusho Kokyuroku No. **820** (1993), 1–15 16

[Kon1901] H. Konen, *Geschichte der Gleichung* $t^2 - Du^2 = 1$, Leipzig (1901), 132 pp 1

[Kut1974] M. Kutsuna, *On the fundamental units of real quadratic fields*, Proc. Japan Acad. **50** (1974), 580–583 2

[Lag1980a] J.C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation* $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc. **260** (1980), no. 2, 485–508 10

[Lag1980b] J.C. Lagarias, *On determining the* 4*-rank of the ideal class group of a quadratic field* J. Number Theory **12** (1980), 191–196 13

[Leg1830] A.M. Legendre, *Théorie des Nombres*, third edition 1830 3

[Lem2000] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer Verlag 2000 7

[Lem2003a] F. Lemmermeyer, *Higher Descent on Pell Conics II. Two Centuries of Missed Opportunities*, preprint 2003 1

[Lem2003b] F. Lemmermeyer, *Higher Descent on Pell Conics III. The First* 2*-Descent*, preprint 2003 1, 7

[Len2002] H. Lenstra, *Solving the Pell equation*, Notices AMS **49** (2002), 182–192 1

[Lev1988] C. Levesque, *Continued fraction expansions and fundamental units*, J. Math. Phys. Sci. **22** (1988), no. 1, 11–44 2

[Lev1988] C. Levesque, G. Rhin, *A few classes of periodic continued fractions*, Utilitas Math. **30** (1986), 79–107 2

[LT2000] D. Li, Y. Tian, *On the Birch-Swinnerton-Dyer conjecture of elliptic curves* $E_D : y^2 = x^3 - D^2x$, Acta Math. Sin. **16** (2000), no. 2, 229–236 13, 17

[Mad2001] D.J. Madden, *Constructing families of long continued fractions* Pac. J. Math. **198** (2001), 123–147 2

[Mab1879] N. Malebranche, cf. C. Henry, Bull. Bibl. Storia Sc. Mat. Fis. **12** (1879), 696–698 2

[Mal1906] E. Malo, *Solution de l'équation* $x^2 - Dy^2 = -1$, L'Interméd. Math. **13** (1906), 246 2

[McL2003] J. Mc Laughlin, *Polynomial solutions of Pell's equation and fundamental units in real quadratic fields*, J. London Math. Soc. (2) **67** (2003), 16–28 2

[McL2003] J. Mc Laughlin, *Multi-variable polynomial solutions to Pell's equation and fundamental units in real quadratic fields*, Pacific J. Math. **210** (2003), 335–349 2

[Mit1997] D.A. Mitkin, *On some diophantine equations connected with Pellian equation*, Proc. Int. Conf. in honour of J. Kubilius; New Trends in Probab. Stat. **4** (1997), 27–32 8

[Mol1997] R.A. Mollin, *Polynomial solutions for Pell's equation revisited*, Indian J. Pure Appl. Math. **28** (1997), 429–438 2

[Mol2001] R. Mollin, *Polynomials of Pellian type and continued fractions*, Serdica Math. J. **27** (2001), 317–342 2

[Mor1873] C. Moreau, *Solution de la question 1055*, Nouv. Ann. (2) **12** (1873) 330–331 2

[Mor1979] P. Morton, *On Rédei's theory of the Pell equation*, J. Reine Angew. Math. **307/308** (1979), 373–398 10

[Mor1982a] P. Morton, *Density results for the* 2*-classgroups and fundamental units of real quadratic fields*, Studia Sci. Math. Hungar.**17** (1982), no. 1-4, 21–43 13

[Mor1982b] P. Morton, *Density result for the* 2*-classgroups of imaginary quadratic fields*, J. Reine Angew. Math. **332** (1982), 156–187 13

[Mor1983] P. Morton, *The quadratic number fields with cyclic* 2*-classgroups*, Pac. J. Math. **108** (1983), 165–175 13

[Mor1990a] P. Morton, *Governing fields for the* 2*-class group of* $\mathbb{Q}(\sqrt{-q_1q_2p}\,)$ *and a related reciprocity law*, Acta Arith. **55** (1990), 267–290 13

[Mor1990b] P. Morton, *On the nonexistence of abelian conditions governing solvability of the* -1 *Pell equation*, J. Reine Angew. Math. **405** (1990), 147–155 13

[Nag1925] T. Nagell, *Om den unbestemte ligning* $x^2-Dy^2=1$, Norsk. Mat. Tidskr. **7** (1925), 33–46 2

[Nag1933] T. Nagell, *Über die Lösbarkeit der Gleichung* $x^2-Dy^2=-1$, Ark. Mat. Astron. Fys. B **23**, No.6 (1933), 1–5 17

[Nag1954] T. Nagell, *On a special class of Diophantine equations of the second degree*, Ark. Mat. **3** (1954), 51–65 8

[Nat1976] M.B. Nathanson, *Polynomial Pell's equations*, Proc. Amer. Math. Soc. **56** (1976), 89–92 3

[New1977] M. Newman, *A note on an equation related to the Pell equation*, Amer. Math. Monthly (1977), 365–366 7

[Nor1974] H.-U. Nordhoff, *Explizite Darstellungen von Einheiten und ihre Anwendung auf Mehrklassigkeitsfragen bei reell-quadratischen Zahlkörpern. I*, J. Reine Angew. Math. **268/269** (1974), 131–149 2

[Ori1977a] B. Oriat, *Rélations entre les 2-groupes des classes d'idéaux des extensions quadratiques* $k(\sqrt{d}\,)$ *et* $k(\sqrt{-d}\,)$, Ann. Inst. Fourier **27** (1977), No.2, 37–59 10

[Ori1977b] B. Oriat, *Rélations entre les 2-groupes des classes d'ideaux de* $k(\sqrt{d}\,)$ *et* $k(\sqrt{-d}\,)$, Astérisque **41-42** (1977), 247–249 10

[Ori1976] B. Oriat, *Rélation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres*, Bull. Soc. Math. Fr. **104** (1976), 301–307 10

[Pal1969] G. Pall, *Discriminantal divisors of binary quadratic forms*, J. Number Theory **1** (1969), 525–533 8

[Per1913] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner 1913 2

[Pet1926] K. Petr, *Über die Pellsche Gleichung*, Rozpravy **35** (1926), 7pp 8

[Pet1927] K. Petr, *On Pell's equation* (Czech), Casopis **56** (1927), 57–66 8

[Per1887] J. Perott, *Sur l'équation* $t^2 - Du^2 = -1$*. Premier mémoire*, J. Reine Angew. Math. **102** (1887), 185–225 13

[PW1999] A. van der Poorten, H.C. Williams, *On certain continued fraction expansions of fixed period length*, Acta Arith. **89** (1999), no. 1, 23–35 2

[Pum1968] D. Pumplün, *Über die Klassenzahl und die Grundeinheit des reellquadratischen Zahlkörpers*, J. Reine Angew. Math. **230** (1968), 177–210 7, 15

[Ram1994] A.M.S. Ramasamy, *Polynomial solutions for the Pell's equation*, Indian J. Pure Appl. Math. **25** (1994), no. 6, 577–581 2

[Red1932] L. Rédei, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **49** (1932), 338–363 9

[Red1935a] L. Rédei, *Über die Pellsche Gleichung* $t^2 - du^2 = -1$, J. Reine Angew. Math. **173** (1935), 193–221; transl. from Mat. Termeszett. Ertes. **54** (1936), 1–44 9, 13

[Red1935b] L. Rédei, *Über einige Mittelwertfragen im quadratischen Zahlkörper*, Journ. Reine Angew. Math. **174** (1935), 15–55 17

[Red1935c] L. Rédei, *Ein asymptotisches Verhalten der absoluten Klassengruppe des quadratischen Zahlkörpers und die Pellsche Gleichung*, Jahresbericht D. M. V. **45** (1935), 78 kursiv 17

[Red1937] L. Rédei, *Über die D-Zerfällungen zweiter Art* (Hungarian; German summary), Math.-nat. Anz. Ungar. Akad. Wiss. **56** (1937), 89–125 9

[Red1943] L. Rédei, *Über den geraden Teil der Ringklassengruppe quadratischer Zahlkörper, die Pellsche Gleichung und die diophantische Gleichung* $rx^2 + sy^2 = z^{2^n}$ *I, II, III*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **62** (1943), 13–34, 35–47, 48–62 13

[Red1953] L. Rédei, *Die* 2*-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung*, Acta Math. Acad. Sci. Hungaricae **4** (1953), 31–87 10, 13

[RR1933] L. Rédei, H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1933), 69–74 9, 10

[Ri1901] G. Ricalde, Interméd. Math. **8** (1901), 256 2

[Ric1864] C. Richaud, *Énoncés de quelques théorèmes sur la possibilité de l'équation* $x^2 - Ny^2 = -1$ *en nombres entiers*, J. Math. Pures Appl. (2) **9** (1864), 384–388 6

[Ric1865a] C. Richaud, *Démonstrations de quelques théorèmes concernant la résolution en nombres entiers de l'équation* $x^2 - Ny^2 = -1$, J. Math. Pures Appl. (2) **10** (1865), 235–292 5, 6

[Ric1865b] C. Richaud, *Sur la résolution des équations* $x^2 - Ay^2 = \pm 1$, Atti Accad. Pont. Nuovi Lincei **19** (1865), 177–182 2, 5, 6

[Ric1866] C. Richaud, *Démonstrations de quelques théorèmes concernant la résolution en nombres entiers de l'équation* $x^2 - Ny^2 = -1$, J. Math. Pures Appl. (2) **11** (1866), 145–176 6

[Rob1879] S. Roberts, *On forms of numbers determined by continued fractions*, Proc. London Math. Soc. **10** (1878/79), 29–41 5

[Sch1932] D. Schepel, *Over de Vergelejking van Pell*, Ph. D. thesis Groningen, 1932 2

[Sch1934] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. **39** (1934), 95–111 10, 11

[Spe1895] G. Speckman, *Über die Auflösung der Pell'schen Gleichung*, Archiv Math. Phys. (2) **13** (1895), 330 2

[Ste1834] M.A. Stern, *Theorie der Kettenbrüche und ihre Anwendung*, J. Reine Angew. Math. **11** (1834), 311–350 2

[Ste1988] P. Stevenhagen, *Class groups and governing fields*, Ph. D. thesis, Berkeley 1988 13

[Ste1989] P. Stevenhagen, *Ray class groups and governing fields*, Théorie des nombres, Années 1988/89, Publ. Math. Fac. Sci. Besançon (1989) 13

[Ste1993a] P. Stevenhagen, *Rédei-matrices and applications*, Number theory (Paris, 1992–1993), 245–259, London Math. Soc. Lecture Note Ser., 215 10

[Ste1993b] P. Stevenhagen, *Divisibility by* 2*-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), 1–19 13

[Ste1993c] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Exp. Math. **2** (1993), 121–136 17

[Sue1995] Y. Sueyoshi, *Comparison of the* 4*-ranks of the narrow ideal class groups of the quadratic fields* $\mathbb{Q}(\sqrt{m}\,)$ *and* $\mathbb{Q}(\sqrt{-m}\,)$ (Japanese), Algebraic number theory and Fermat's problem (Kyoto, 1995), Surikaisekikenkyusho Kokyuroku No. **971** (1996), 134–144 10

[Sue1997] Y. Sueyoshi, *On a comparison of the* 4*-ranks of the narrow ideal class groups of* $\mathbb{Q}(\sqrt{m}\,)$ *and* $\mathbb{Q}(\sqrt{-m}\,)$, Kyushu J. Math. **51** (1997), 261–272 10

[Sue2000] Y. Sueyoshi, *Relations betwen the narrow* 4*-class ranks of quadratic number fields*, Adv. Stud. Contemp. Math. **2** (2000), 47–58 10

[Sue2001] Y. Sueyoshi, *On Rédei matrices with minimal rank*, Far East J. Math. Sci. (FJMS) **3** (2001), no. 1, 121–128 16

[TY1993] A. Takaku, S.-I. Yoshimoto, *Fundamental unit of the real quadratic field* $\mathbb{Q}(\sqrt{v(v^3+1)(v^6+3v^3+3)})$, Ryukyu Math. J. **6** (1993), 57–67 2

[Tan1889] F. Tano, *Sur quelques théorèmes de Dirichlet*, J. Reine Angew. Math. **105** (1889), 160–169 6, 8

[vTh1926] M. von Thielmann, *Zur Pellschen Gleichung*, Math. Ann. **95** (1926), 635–640 2

[Tom1995] K. Tomita, *Explicit representation of fundamental units of some real quadratic fields*, Proc. Japan Acad. **71** (1995), 41–43 2

[Tom1997] K. Tomita, *Explicit representation of fundamental units of some real quadratic fields. II*, J. Number Theory **63** (1997), no. 2, 275–285 2

[Tro1969] H. F. Trotter, *On the norms of units in quadratic fields*, Proc. Amer. Math. Soc. **22** (1969), 198–201 7, 8, 15, 16

[Ueh1989] T. Uehara, *On the* 4*-rank of the narrow ideal class group of a quadratic field*, J. Number Theory **31** (1989), 167–1731 10

[Vau1985] Th. P. Vaughan, *The construction of unramified cyclic quartic extensions of* $\mathbb{Q}(\sqrt{-m}\,)$, Math. Comp. **45** (1985), 233–242 13

[Vaz1997a] A. Vazzana, *On the* 2*-primary part of* K_2 *of rings of integers in certain quadratic number fields*, Acta Arith. **80** (1997), 225–235 13

[Vaz1997b] A. Vazzana, *Elementary abelian 2-primary parts of $K_2\mathcal{O}$ and related graphs in certain quadratic number fields*, Acta Arith. **81** (1997), No.3, 253–264 13

[Wal1952] A. Walfisz, *Pell's Equation* (Russian), Tbilisi 1952; 90 pp 1

[Wal1988] G. Walsh, *The Pell equation and powerful numbers*, M. Sc. thesis, Univ. Calgary 1988 8

[Wal2002] G. Walsh, *On a question of Kaplansky*, Amer. Math. Monthly **109** (2002), no. 7, 660–661 8

[WY2003] W.A. Webb, H. Yokota, *Polynomial Pell's equation*, Proc. Amer. Math. Soc. **131** (2003), 993–1006 3

[Web1939] W. Weber, *Die Pellsche Gleichung*, Deutsche Math., Beiheft 1 (1939), 151 pp. 1

[Whi1912] E.E. Whitford, *The Pell equation*, New York 1912, 193 pp 1, 16

[Wil2002] H.C. Williams, *Some generalizations of the S_n sequence of Shanks*, Acta Arith. **69** (1995), no. 3, 199–215 2

[Wil2002] H.C. Williams, *Solving the Pell equation*, Proc. Millenial Conference on Number Theory (Urbana 2000), Peters 2002, 397–435 1

[WL1994] K. S. Williams, D. Liu, *Representation of primes by the principal form of negative discriminant Δ when $h(\Delta)$ is* 4, Tamkang J. Math. **25** (1994), 321–334 13

[Yam1971] Y. Yamamoto, *Real quadratic number fields with large funamental units*, Osaka J. Math. **8** (1971), 261–270 2

[Yok1968] H. Yokoi, *On real quadratic fields containing units with norm* -1, Nagoya Math. J. **33** (1968), 139–152 2

[Yok1970] H. Yokoi, On the fundamental unit of real quadratic fields with norm 1. J. Number Theory **2** (1970), 106–115 2

[Yu2001] J. Yu, *On arithmetic of hyperelliptic curves*, Aspects of Mathematics, HKU 2001, 395–415 3

[Zha1997] Ch. Zhao, *A criterion for elliptic curves with lowest* 2*-power in* $L(1)$, Math. Proc. Cambridge Philos. Soc. **121** (1997), no. 3, 385–400 13, 17

[Zha2001] Ch. Zhao, *A criterion for elliptic curves with second lowest 2-power in* $L(1)$, Math. Proc. Cambridge Philos. Soc. **131** (2001), no. 3, 385–404 13, 17

[Zin1974] E. W. Zink, *Über die Klassengruppe einer absolut zyklischen Erweiterung*, Diss. Humboldt Univ. Berlin (1974) 13

Dept. Mathematics, Bilkent University, 06800 Bilkent, Ankara, Turkey

E-mail address: franz@fen.bilkent.edu.tr