Publ. Math. Debrecen
88/3-4 (2016), 319–343
DOI: 10.5486/PMD.2016.7337

Hilbert 2-class fields and 2-descent

By FRANZ LEMMERMEYER (Germany)

Abstract. We give a construction of unramified cyclic octic extensions of certain complex quadratic number fields. The binary quadratic form used in this construction also shows up in the theory of 2-descents on Pell conics and elliptic curves, as well as in the explicit description of cyclic quartic extensions.

Introduction

In this article we discuss several apparently unrelated problems involving integers of the form $m = a^2 + 4b^2 \equiv 1 \bmod 4$. A central role in the solution of these problems is played by the family of binary quadratic forms $Q_b = (b, a, -b)$ with discriminant m; here and below, $Q = (A, B, C)$ denotes the binary quadratic form $Q(X, Y) = AX^2 + BXY + CY^2$ with discriminant $\Delta = B^2 - 4AC$.

The first problem concerns the solvability of the negative Pell equation

$$T^2 - mU^2 = -4$$

and the computation of its fundamental solution. Results going back to Euler [17] show that such a solution can be computed from an integral solution of the equation $Q_b(r, s) = 1$.

The second problem is the explicit construction of octic cyclic unramified extensions L/k of the quadratic number field $k = \mathbb{Q}(\sqrt{-m})$. The construction of its quartic subextension $K = k(i, \sqrt{a + 2bi})$ is almost trivial, and we will see that explicit generators μ of the quadratic extension $L = K(\sqrt{\mu})$ can be written down explicitly using nontrivial solutions of the diophantine equation $Q_b(r, s) = 2x^2$.

Mathematics Subject Classification: 11R20, 11R29, 11G05.
Key words and phrases: Hilbert class field, binary quadratic form, descent, elliptic curves.

Afterwards we will briefly explain why the forms Q_b also play a role in performing 2-descent on certain families of elliptic curves, such as those of the form $E : y^2 = x(x^2 + p)$, where $p = a^2 + 4b^2$ is prime; here the existence of rational points on E is tied to the pair of equations $r^2 + s^2 = X^2$ and $Q_b(r, s) = Y^2$.

Finally we mention a few other problems in which these forms Q_b have shown up. It is clear that most of the problems discussed here may be generalized considerably. In particular, studying Pell descent or Hilbert 2-class fields should by no means be restricted to the special cases of the negative Pell equation or discriminants of the form $-4m$.

This article is written in the language of quadratic forms (although ideals show up occasionally). For understanding the results it is sufficient to know the most elementary basics; for readers who would like to read more about reduction and composition of forms, I strongly recommend the books by Flath [18] and Cox [15], as well as the recent contributions by Bhargava [10]. The first section of [32] gives a brief introduction to Bhargava's ideas, and a detailed elementary account can be found in Barker-Hoyt's thesis [8].

1. The quadratic space of binary quadratic forms

I expect that most of the results presented in this article may be generalized considerably. In this section I will therefore explain how the main actors in our play show up in a more general setting.

Let R be a domain with characteristic $\neq 2$, and consider the set $\mathcal{B} = \mathcal{B}_R$ of binary quadratic forms $Q(X, Y) = AX^2 + BXY + CY^2$, often abbreviated by $Q = (A, B, C)$, with $A, B, C \in R$. We define a bilinear map $\mathcal{B} \times \mathcal{B} \longrightarrow R$ via

$$\langle Q_1, Q_2 \rangle = B_1B_2 - 2A_1C_2 - 2A_2C_1,$$

where $Q_j = (A_j, B_j, C_j) \in \mathcal{B}$. Clearly $\langle Q_1, Q_2 \rangle = \langle Q_2, Q_1 \rangle$, and $\langle Q, Q \rangle = \operatorname{disc}(Q) = B^2 - 4AC$ is the discriminant of Q.

Matrices $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$ act on $\mathcal{B}$ via $Q|_S = Q'$, where

$$Q'(x, y) = Q\big((x, y)S'\big) = Q(rx + sy, tx + uy), \tag{1}$$

(here S' denotes the transpose of S). It is an easy exercise to show that

$$\langle Q_1|_S, Q_2 \rangle = \langle Q_1, Q_2|_{S'} \rangle \tag{2}$$

for $S \in \mathrm{SL}_2(\mathbb{Q})$. This identity is the essential content of the "Cantor diagrams" in [35, Theorem 2], [11, Proposition 3.3], and [12, Theorem 2].

From now on assume that $R = \mathbb{Z}$. If the form $Q_1 = (1, 0, -m)$ represents -1, say $r^2 - ms^2 = -1$, then $Q_2 = (ms, 2r, s)$ is a form with discriminant -4. Therefore Q_2 is equivalent to $(1, 0, 1)$, say $Q_2 = (1, 0, 1)|_S$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$. Write $Q_1|_{S'} = (a, 2B, c)$ for integers a, B, c; then equation (2) shows that $a + c = 0$, i.e., $Q_1|_{S'} = (a, 2B, -a)$. Since Q_1 and $Q_1|_{S'}$ both have discriminant $4m$, we must have $m = a^2 + B^2$. Observe that we have shown that if $(1, 0, -m)$ represents -1, then $m = a^2 + B^2$ is a sum of two squares.

Replacing the principal form $(1, 0, -a)$ with discriminant $4a$ by the principal form $Q_0 = \left(1, 1, \frac{1-a}{4}\right)$ with discriminant $\Delta = a^2 + 4b^2 \equiv 1 \bmod 4$ results in replacing $(a, 2B, -a)$ by $Q_b = (b, a, -b)$. This is the form that will play a central role in the problems described below: performing a second descent on Pell conics and elliptic curves, constructing Hilbert class fields of quadratic number fields with discriminant $-4m$, or in Hasse's description of the arithmetic of cyclic quartic number fields.

The pair of orthogonal forms $Q_1 = (1, 0, 1)$ and $Q_2 = (b, a, -b)$ will occur explicitly in our description of the second 2-descent on the elliptic curve $y^2 = x(x^2 - 4p)$ for primes $p = a^2 + 4b^2$. In fact we will see that finding a rational point on E is equivalent to finding a simultaneous representation $Q_1(r, s) = X^2$ and $Q_2(r, s) = Y^2$ of squares by these forms.

This problem can be reformulated as follows. Let $Q = (A, B, C) \in \mathcal{B}_R$ be a binary quadratic form over a domain R as above, and let F be the quotient field of R. We can evaluate Q on $\mathbb{P}^1F$ as follows: for each point $P = [x : y] \in \mathbb{P}^1F$ we set $P = Q(x, y)$ with values in $F^\times/F^{\times 2}$. Given a pair (Q_1, Q_2) of orthogonal forms, the pair of simultaneous equations $Q_1(r, s) = X^2$ and $Q_2(r, s) = Y^2$ is now equivalent to the existence of a point $P \in \mathbb{P}^1\mathbb{Q}$ with $Q_1(P) = Q_2(P) = 1$.

2. 2-descent on Pell conics

Let $m = 4n + 1$ be a squarefree integer, and consider the Pell equation

$$Q_0(T, U) = T^2 - TU - nU^2 = 1, \tag{3}$$

where $Q_0(X, Y) = X^2 - XY - nY^2$ is the principal binary quadratic form with discriminant $4n + 1 = m$.

Multiplying through by 4 and completing the square shows that this equation can also be written in the more familiar way

$$(2T - U)^2 - mU^2 = 4.$$

2.1. First 2-descent. In this section we will present methods for finding a nontrivial integral solution of (3) as well as criteria for the solvability of the negative Pell equation

$$Q_0(T,U) = -1. \tag{4}$$

To this end we write the Pell equation $(2T-U)^2 - mU^2 = 4$ in the form $mU^2 = (2T-U)^2 - 4 = (2T-U-2)(2T-U+2)$.

Now

$$\gcd(2T-U-2, 2T-U+2) = \begin{cases} 4 & \text{if } U \text{ is even,} \\ 1 & \text{if } U \text{ is odd;} \end{cases}$$

in both cases we find that there exist integers c, d, r, s with $cd = m$ and $2T - U + 2 = cr^2$ and $2T - U - 2 = ds^2$, and so $cr^2 - ds^2 = 4$.

The fact that $r \equiv s \bmod 2$ allows us to make the substitution $s = S$ and $r = 2R - S$, which transforms the equation $cr^2 - ds^2 = 4$ into

$$cR^2 - cRS + \frac{c-d}{4}S^2 = 1. \tag{5}$$

Observe that the quadratic form $cx^2 - dy^2$ has discriminant $4cd = 4m$, whereas the form on the left hand side of (5) has discriminant $c^2 - c(c-d) = cd = m$.

Thus each integral solution of the Pell equation comes from a solution of one of the equations (5) for some factorization $cd = m$ (see [31] for details). In fact, Legendre claimed and Dirichlet proved that exactly four among these equations[1] have solutions in integers:

Proposition 1. *First 2-descent on Pell conics: If $m = a^2 + 4b^2 = p_1 \cdots p_t$ is a product of t disctinct primes $p_j \equiv 1 \bmod 4$, then among the 2^{t+1} descendants (5) with $cd = m$ there are exactly four that have solutions in integers.*

In particular, apart from the trivial descendants $1 = x^2 - my^2$ and $1 = -mx^2 + y^2$ there is a unique nontrivial pair (c,d) with $cd = m$ such that $1 = cx^2 - dy^2$ and $1 = -dx^2 + cy^2$ have integral solutions.

Special cases. If $m = p$ is prime, all four factorizations of m must lead to solvable equations. In particular, $T^2 - pU^2 = -1$ is solvable in integers. This result is due to Legendre.

[1] If $m = 5$, for example, the solvable equations correspond to the factorizations $(c,d) = (1,5)$, $(5,1)$, $(-1,-5)$, and $(-5,-1)$. If $m = 34$, on the other hand, the solvable equations come from $(c,d) = (1,34)$, $(-34,-1)$, $(2,17)$ and $(-17,-2)$.

If $m = pq$ for primes $p \equiv q \equiv 1 \bmod 4$, we have the following essentially different descendants, written using forms with discriminant $4pq$:

$$x^2 - pqy^2 = 4, \quad pqx^2 - y^2 = 4, \quad px^2 - qy^2 = 4, \quad qx^2 - py^2 = 4.$$

If $\left(\frac{p}{q}\right) = -1$, it is immediately clear that the last two equations do not have rational (let alone integral) solutions; this implies

Corollary 2. *If $p \equiv q \equiv 1 \bmod 4$ are primes with $\left(\frac{p}{q}\right) = -1$, the negative Pell equation* (4) *is solvable in integers.*

If $\left(\frac{p}{q}\right) = 1$, on the other hand, further descents are necessary for deciding which of the equations (5) are solvable.

2.2. Second 2-descent. Let us show how to do such a second descent. We start with the equation $T^2 - mU^2 = -4$ and assume that it has an integral solution. Then $mU^2 = T^2 + 4 = (T + 2i)(T - 2i)$.

Now T is easily seen to be either odd or divisible by 4. Thus $\gcd(T + 2i, T - 2i) = 1$ in the first and $\gcd(T + 2i, T - 2i) = 2i = (1 + i)^2$ in the second case. This shows that we must have $\mu\rho^2 = j(T + 2i)$ for some unit $j = i^k$ and some $\mu, \rho \in \mathbb{Z}[i]$ with $\mu\overline{\mu} = m$ and $\rho\overline{\rho} = u$. Subsuming j into μ then gives $\mu\rho^2 = T + 2i$.

A simple calculation shows that $\mu \equiv 1 \bmod 2$; writing $\mu = a + 2bi$ (recall that $m = \mu\overline{\mu} = a^2 + 4b^2$) and $\rho = x + yi$, and comparing real and imaginary parts we find that

$$T = ax^2 - 4bxy - ay^2, \qquad 1 = bx^2 + axy - by^2.$$

Conversely, if x and y are integers with $bx^2 + axy - by^2 = 1$, then $T = ax^2 - 4bxy - ay^2$ and $U = x^2 + y^2$ is an integral solution of the equation $T^2 - mU^2 = -4$. We have proved the following

Proposition 3. *Let m be an odd squarefree natural number. The negative Pell equation* (4) *has an integral solution if and only if there exist integers $a, b \in \mathbb{N}$ with $m = a^2 + 4b^2$ such that the diophantine equation*

$$Q_b(x, y) = bx^2 + axy - by^2 = 1 \tag{6}$$

has an integral solution. In this case,

$$T = ax^2 - 4bxy - ay^2, \quad U = x^2 + y^2$$

is a solution of the original equation $Q_0(T, U) = -1$.

Example 1. Let $m = 41 = 5^2 + 4 \cdot 2^2$; for checking the solvability of $T^2 - TU - 10U^2 = -1$ we have to consider $Q(x,y) = 2x^2 + 5xy - 2y^2 = 1$. We find the solution $x = 3$, $y = -1$, hence $T = 5\cdot 3^2 + 8\cdot 3 - 5 = 64$ and $U = 3^2 + 1^2 = 10$. Thus $(T,U) = (64,10)$ is the fundamental solution of the negative Pell equation, and in fact we have $64^2 - 41\cdot 10^2 = -4$, or $32^2 - 41\cdot 5^2 = -1$ and $37^2 - 37\cdot 10 - 10\cdot 10^2 = -1$.

Example 2. Let $m = 221 = 13 \cdot 17$. Then $m = 5^2 + 4 \cdot 7^2 = 11^2 + 4 \cdot 5^2$, so we have to solve the equations

$$7x^2 + 5xy - 7y^2 = 1 \quad \text{or} \quad 5x^2 + 11xy - 5y^2 = 1.$$

These equations can be written in the form

$$(14x + 5y)^2 - my^2 = 28 \quad \text{and} \quad (10x + 11y)^2 - my^2 = 44.$$

Neither of these equations has a solution since $\left(\frac{7}{13}\right) = \left(\frac{11}{13}\right) = -1$; thus the negative Pell equation $T^2 - 221U^2 = -4$ is not solvable.

Example 3. If $m = 4777 = 17 \cdot 281 = 59^2 + 4 \cdot 18^2 = 69^2 + 4 \cdot 2^2$, then we have to check the solvability of the equations

$$18x^2 + 59xy - 18y^2 = 1, \quad \text{and} \quad 2x^2 + 69xy - 2y^2 = 1.$$

For solving the first equation, observe that $\xi = \frac{x}{y}$ is approximately equal to one of the roots of the equation $18\xi^2 + 59\xi - 18 = 0$, that is, to $\xi \approx 3.56$ or to $\xi \approx 0.28$. Using these approximations it is easy to solve the first equation by a brute force computation: we find $(x,y) = (587, 2089)$, hence $T = \frac{1}{2}(-59x^2 + 72xy + 59y^2) = 162715632$ and $U = \frac{1}{2}(x^2 + y^2) = 2354245$.

The second form $Q = (2, 69, -2)$ is not equivalent to the principal form and generates a class of order 2. In fact, we have $Q(587, -17) = 9$, so $Q \sim Q_1^2$ for some form $Q_1 = (3, *, *)$, which is not contained in the principal genus, hence cannot be equivalent to the principal form.

Rational solvability. A necessary condition for the solvability of a diophantine equation in integers is its solvability in rational numbers. Applied to the negative Pell equation (4), this gives us the classical observation that $\left(\frac{-1}{p}\right) = +1$ for all primes $p \mid m$, which is equivalent to m being a sum of two squares.

Although the solvability of (4) in integers is equivalent to the solvability of one of the equations (6) in integers, we get stronger conditions by applying the above observation to (6). In fact, the solvability of (6) in rational numbers is easy to check:

Lemma 4. *Equation* (6) *has a solution in rational numbers if and only if* $\left(\frac{a}{p}\right) = +1$ *(or, equivalently,* $\left(\frac{b}{p}\right) = +1$*) for all primes* $p \mid m$.

Proof. Multiplying (6) through by $4b$ and completing the square gives $(2bx + ay)^2 - my^2 = 4b$. The fact that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ follows immediately from the congruence $(a + 2b)^2 \equiv 4ab \bmod p$.

We have to check solvability in all completions of $\mathbb{Q}$. Solvability in the reals being clear, we have to verify local solvability in $\mathbb{Q}_p$ for all primes p. This is equivalent to the triviality of the Hilbert symbol $\left(\frac{b,m}{p}\right) = 1$ for all primes p. By the product formula $\prod_p \left(\frac{b,m}{p}\right) = 1$, it is enough to check solvability for all primes except one. We will therefore show that the equation above has solutions in the completions $\mathbb{Q}_p$ for all odd primes p. By Hensel's Lemma it is sufficient to check solvability modulo p. Now we distinguish two cases:

$p \nmid m$: Then $X^2 - mY^2$ represents at least one nonsquare mod p, hence all of them; thus $X^2 - mY^2 \equiv 4b \bmod p$ is solvable, and since $\gcd(a, 2b) = 1$, we can write $Y = y$ and $X = 2bx + ay$.

$p \mid m$: Then $(2bx + ay)^2 - my^2 \equiv 4b \bmod p$ implies $\left(\frac{b}{p}\right) = +1$. If conversely $\left(\frac{b}{p}\right) = +1$, we can show solvability modulo p and in $\mathbb{Z}_p$ exactly as above. □

By Gauss's genus theory, the conditions $\left(\frac{b}{p}\right) = +1$ for all primes $p \mid m$ is equivalent to Q_b being in the principal genus. Such forms are known to represent 1 rationally. Solvability criteria for the negative Pell equation following from this criterion are due to Dirichlet, Scholz, Epstein and others (see [31] for detailed references).

Special cases. Assume that $m = pq$ is the product of two primes $p \equiv q \equiv 1 \bmod 4$. We have already seen that (4) is solvable in integers if $\left(\frac{p}{q}\right) = -1$. Suppose therefore that $\left(\frac{p}{q}\right) = -1$, and write $p = A^2 + 4B^2$ and $q = C^2 + 4D^2$. Then $m = a^2 + 4b^2$ for $(a, b) = (AC - 4BD, AD + BC)$ and $(a, b) = (AC + 4BD, AD - BC)$. By Burde's reciprocity law (see [30]) we have

$$\left(\frac{AC \pm 4BD}{p}\right) = \left(\frac{AC \pm 4BD}{q}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 .$$

Thus if $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$, the second descendants $Q_b(x, y) = 1$ are not solvable, hence neither is the negative Pell equation (4).

If $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$, on the other hand, the first descendants $px^2 - qy^2 = \pm 1$ do not have solutions. In fact from $px^2 - qy^2 = 1$ we get $\left(\frac{q}{p}\right)_4 = \left(\frac{y}{p}\right)\left(\frac{-1}{p}\right)_4$, and with $y = 2^j u$ for some $j \geq 1$ we find $\left(\frac{y}{p}\right) = \left(\frac{2}{p}\right)^j \left(\frac{p}{u}\right) = \left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)_4$. Thus the

solvability of $px^2 - qy^2 = 1$ implies $\left(\frac{q}{p}\right)_4 = 1$. Similarly, $qx^2 - py^2 = 1$ can only be solvable if $\left(\frac{p}{q}\right)_4 = 1$. Thus if $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$, neither of the equations $px^2 - qy^2 = \pm 1$ is solvable; but then one of the equations $Q_b(x, y) = 1$ must have a solution. We have proved

Corollary 5. *Let $m = pq$ be a product of two primes $p \equiv q \equiv 1 \bmod 4$. Then we have the following possibilities:*

(1) $\left(\frac{p}{q}\right) = -1$*: then (4) is solvable.*

(2) $\left(\frac{p}{q}\right) = +1$*: If $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$, then (4) is not solvable.*
If $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$, then (4) is solvable.

These results go back to Dirichlet and Scholz. It is not very hard to produce numerous similar results for products of three and more primes.

Classes represented by the forms Q_b. The propositions above show that if the negative Pell equation $x^2 - my^2 = -1$ is solvable, then one of the forms Q_b (where b runs through all integers with $m = a^2 + 4b^2$) represents 1, hence lies in the principal class of the primitive binary quadratic forms with discriminant m. Our next result tells us exactly how the remaining forms Q_b are distributed among the equivalence classes of order dividing 2, and that the form Q_b representing 1 is unique:

Theorem 6. *Let $m = p_1 \cdots p_t$ be a product of primes $p_j \equiv 1 \bmod 4$, and let $m = a_j^2 + 4b_j^2$ $(1 \le j \le t,\ a_j, b_j > 0)$ be the different representations of m as a sum of two squares. Then the binary quadratic forms $Q_j = (b_j, a_j, -b_j)$ have discriminant m, and there are two cases:*

(1) *The negative Pell equation is solvable: then the forms Q_b represent the 2^{t-1} classes of order dividing 2 in $\mathrm{Cl}(m)$, the class group of binary quadratic forms with discriminant m. In particular, the form representing 1 is unique.*

(2) *The negative Pell equation is not solvable: then there exists a subgroup C of index 2 in $\mathrm{Cl}(m)[2]$ such that each form Q_b represents one class in $\mathrm{Cl}(m)[2] \setminus C$. Each such class is represented by exactly two forms.*

Under the standard correspondence between classes of binary quadratic forms and ideal classes, the class of the form $Q_b = (b, a, -b)$ with discriminant $a^2 + 4b^2 = m$ corresponds to the ideal class represented by the ideal $\left(\frac{a+\sqrt{m}}{2}, b\right)$.

If $m = p_1 \cdots p_t$ is the product of t prime factors $p_j \equiv 1 \bmod 4$, then $m = a_j^2 + 4b_j^2$ can be written in 2^{t-1} ways as a sum of two squares of positive integers. To each such sum we attach an ideal

$$\mathfrak{a}_j = (2b_j + \sqrt{m}, a_j),$$

which has the properties

$$N\mathfrak{a}_j = a_j, \qquad \mathfrak{a}_j^2 = (2b + \sqrt{m}\,).$$

In [33] (see also [9] for additional results in this direction) we have proved the following theorem, which is the ideal theoretic version of Theorem 6:

Theorem 7. *Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field, where $m = p_1 \cdots p_t$ is a product of primes $p_j \equiv 1 \bmod 4$. Let ε denote the fundamental unit of K.*

- *If $N\varepsilon = -1$, then the ideal classes $[\mathfrak{a}_j]$ are pairwise distinct and represent the 2^{t-1} classes of order dividing 2 in $\mathrm{Cl}(K)$. Each ideal $\mathfrak{a}_j$ is equivalent to a unique ramified ideal $\mathfrak{b}_e$. In particular, exactly one of the $\mathfrak{a}_j$ is principal; if $\mathfrak{a}_j = (\alpha)$, then*
$$\eta = \frac{2b_j + \sqrt{m}}{\alpha^2}$$
is a unit with norm -1 (equal to ε if α is chosen suitably).
- *If $N\varepsilon = +1$, then there is a subgroup C with index 2 in the group $\mathrm{Cl}(K)[2]$ of ideal classes of order dividing 2 such that each class in C is represented by two ramified ideals $\mathfrak{b}_e$ (thus C is the group of strongly ambiguous ideal classes in K). Each class in $\mathrm{Cl}(K)[2] \setminus C$ is represented by two ideals $\mathfrak{a}_j$.*

The unique pair (a, b) for which $Q_b(x, y) = 1$ is solvable in integers can be recovered as follows: the extension $\mathbb{Q}\big(\sqrt{\pm\varepsilon\sqrt{m}}\,\big)$, with $\varepsilon > 1$ the fundamental unit of $\mathbb{Q}(\sqrt{m}\,)$ and the sign chosen as $(-1)^{(m-1)/4} = \big(\frac{2}{m}\big)$, is a cyclic quartic extension with discriminant m^3, hence equal to one of the extensions $\mathbb{Q}\big(\sqrt{m + 2b\sqrt{m}}\,\big)$ for $m = a^2 + 4b^2$, which we have studied in [33].

Remarks. First traces of Proposition 3 can be found in Euler's work. In [17, Prob. 2] he proved that if $ap^2 - 1 = q^2$, then there exist integers b, c, f, g such that

$$a = f^2 + g^2, \quad p^2 = b^2 + c^2, \quad q = bf + cg \quad \text{and} \quad \pm 1 = bg - cf,$$

and we have $ax^2 + 1 = y^2$ for $x = 2pq$ and $y = 2q^2 + 1$.

Euler's observation is related to our results as follows: since (b, c, p) is a Pythagorean triple, there exist integers (switch b and c if necessary to make c even) m, n such that $p = m^2 + n^2$, $b = m^2 - n^2$ and $c = 2mn$; then $\pm 1 = bg - cf = gm^2 - 2mnf - gn^2$, i.e. ± 1 is represented by the binary quadratic form $(g, 2f, -g)$.

Euler's results were rediscovered and complemented by HART [23], A. GÉRARDIN [19], SANSONE [40], [41], EPSTEIN [16] (see also RÉDEI [37, Satz 3]), K. HARDY and K. WILLIAMS [22] (they first proved the uniqueness of the pair (a,b)), ARTEHA [2]. The connection with Pythagorean triples was also observed by GRYTCZUK, LUCA, and WOJTOWICZ [20].

Generalizations to other Pell equations are due to SYLVESTER [43], GÜNTHER [21], and BAPOUNGUÉ [3], [4], [5], [6], [7]. For details, see [31, Part II].

3. Hilbert class fields

Every number field K has a maximal unramified abelian extension L/K; the field L is called the Hilbert class field of K. Class field theory predicts that the Galois group $\mathrm{Gal}(L/K)$ of this extension is isomorphic to the class group $\mathrm{Cl}(K)$. The maximal 2-extension contained in L/K is called the Hilbert 2-class field, and is isomorphic to the 2-class group $\mathrm{Cl}_2(K)$, the 2-Sylow subgroup of $\mathrm{Cl}(K)$.

In this section we will present a very simple construction of unramified cyclic octic extensions of complex quadratic number fields. Such constructions are known (see e.g. [13], [14], [27], as well as the classical presentations [36], [38], [39]) for discriminants $m=-4p$ for primes $p\equiv 1 \bmod 8$, but even in this case we have managed to drastically simplify the construction.

Let $m\equiv 1 \bmod 4$ be a squarefree integer and a sum of two squares, say $m=a^2+4b^2$. Let $k=\mathbb{Q}(\sqrt{-m})$ denote the quadratic number field with discriminant $\Delta=-4m$. The quadratic extension $k_2=\mathbb{Q}(i,\sqrt{m})$ is unramified and abelian over $\mathbb{Q}$, and is a subfield of the genus class field of k, which is given by $k_{\mathrm{gen}}=\mathbb{Q}(i,\sqrt{p_1},\ldots,\sqrt{p_t})$, where $m=p_1\cdots p_t$ is the prime factorization of m.

The quadratic unramified extensions of k have the form $K=\mathbb{Q}(\sqrt{c},\sqrt{-d})$, where $m=cd$ is a factorization of m with $c\equiv -d\equiv 1 \bmod 4$. These factorizations already occurred in (5), where the factorizations $m=cd$ with $c\equiv 3 \bmod 4$ lead to equations that do not even have solutions modulo 4.

Unramified cyclic quartic extensions of k containing $k(\sqrt{d_1})$ correspond bijectively to factorizations $\Delta=d_1d_2$ into two discriminants d_1,d_2 with $(d_1/p_2)=(d_2/p_1)=+1$ for all primes $p_1\mid d_1$ and $p_2\mid d_2$. Such factorizations are called C_4-decompositions of $\Delta=-4m$. In this article we deal with unramified cyclic quartic extensions containing $k_2=\mathbb{Q}(i,\sqrt{m})$; such extensions exist if and only if $\Delta=-4\cdot m$ is a C_4-decomposition, that is, if and only if the primes dividing m are all $\equiv 1 \bmod 8$.

The ambiguous prime ideals $\neq(\sqrt{m})$ all generate ideal classes of order 2;

thus their inertia degree in the full Hilbert 2-class field is equal to 2. This means that if K/k is an unramified abelian 2-extension, then K is the full Hilbert 2-class field if and only if all primes dividing Δ have inertia degree 2 in K/k.

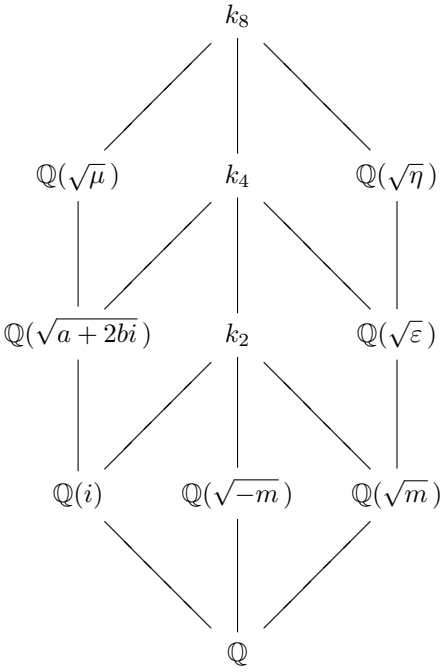

Figure 1. A piece of the 2-class field tower of $\mathbb{Q}(\sqrt{-m})$.

The construction of a cyclic unramified extension k_4/k containing $k(i) = k(\sqrt{m})$ is classical (see [26]): we have to solve the equation

$$A^2 + B^2 - mC^2 = 0. \tag{7}$$

This equation has solutions with $C = 1$, namely $A = a$ and $B = 2b$, where $m = a^2 + 4b^2$. The extension $k(\sqrt{a+2bi})/k$ is a cyclic quartic extension unramified outside of 2; this extension is unramified above 2 (and thus unramified everywhere) if and only if b is even, which in turn is equivalent to $m \equiv 1 \bmod 8$.

The Galois group of k_4/k is generated by the element σ, whose action on the

generators of the extension k_4/k is given by the following table:

α	i	$\sqrt{m}$	$\sqrt{a+2bi}$
$\sigma(\alpha)$	$-i$	$-\sqrt{m}$	$\sqrt{m}/\sqrt{a+2bi}$
$\sigma^2(\alpha)$	i	$\sqrt{m}$	$-\sqrt{a+2bi}$

We now will construct cyclic octic extensions k_8/k containing k_4. It follows from elementary Galois theory (or see [38]) that, to this end, we have to solve the diophantine equation

$$\alpha^2 - (a+2bi)\beta^2 - (a-2bi)\gamma^2 = 0 \tag{8}$$

in the ring $\mathbb{Z}[i]$ of Gaussian integers. A solution (α,β,γ) of this equation is called primitive if $\gcd(\alpha,\beta)=1$.

Theorem 8. *Let $m = a^2+4b^2$ be a sum of two squares. Then $\sqrt{a+2bi}$ generates a cyclic quartic extension k_4 of $k=\mathbb{Q}(\sqrt{-m}\,)$, which is unramified if and only if b is even.*

Assume that b is even. Then the extension k_4/k can be embedded in a cyclic octic extension if and only if equation (8) is solvable. Let (α,β,γ) be a primitive solution of (8); then the extension $k_8 = k\big(\sqrt{\alpha+\beta\sqrt{a+2bi}}\,\big)$ is a cyclic octic extension of $k=\mathbb{Q}(\sqrt{-m}\,)$ unramified outside of 2 and containing k_4. The extension k_8/k is unramified everywhere if and only if $a+2b\equiv\pm1 \bmod 8$.

The proof of Theorem 8 is done step by step.

1. The extension k_8/k is cyclic of degree 8. For proving the cyclicity of k_8/k we use a classical result in Galois theory (see [34, Section 8.4*]; each of the following statements is completely elementary). Let K/k be a normal extension with Galois group G, and let $L=K(\sqrt{\mu}\,)$ be a quadratic extension.

(1) ([34, F8.9]) L/k is normal if and only if for every $\sigma\in G$ there is an $\alpha_\sigma\in K$ such that $\mu^{\sigma-1}=\alpha_\sigma^2$.

(2) ([34, F8.10]) Let L/k be normal. Then we can define an element $[\beta]$ in the second cohomology group $H^2(G,\mu_2)$ with values in $\mu_2=\{-1,+1\}$ by setting

$$\beta(\sigma,\tau) = \alpha_\sigma^\tau\alpha_\tau\alpha_{\sigma\tau}^{-1}.$$

(3) ([34, F8.11]) If L/k is normal, then $[\beta]$ is the element of the second cohomology group attached to the group extension

$$1 \longrightarrow \mu_2 \longrightarrow \mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K/k) \longrightarrow 1.$$

(4) ([34, Example 6, p. 142]) If K/k is cyclic of even degree, then L/k is cyclic if and only if $\alpha_\sigma^\nu = -1$, where σ generates $G = \mathrm{Gal}(K/k)$ and where $\nu = \sum_{\tau\in G}\tau$.

Set $\sqrt{a-2bi} = \sqrt{m}/\sqrt{a+2bi}$, $\mu = \alpha + \beta\sqrt{a+2bi}$ and $\nu = \alpha + \gamma\sqrt{a-2bi}$. We find

$$\mu^{\sigma+1} = \alpha\alpha' + \alpha\beta'\sqrt{a-2bi} + \alpha'\beta\sqrt{a+2bi} + \beta\beta'\sqrt{m} = \mu_\sigma^2$$

for

$$\mu_\sigma = \frac{\alpha + \beta\sqrt{a+2bi} + i\beta'\sqrt{a-2bi}}{1+i},$$

where we have used $\alpha = i\alpha'$ and $\gamma = i\beta'$, as well as $(a-2bi)\gamma^2 = \alpha^2 - (a+2bi)\beta^2$. With $\alpha_\sigma = \mu_\sigma/\mu$ and $\nu = (1+\sigma)(1+\sigma^2)$ we now find

$$\mu_\sigma^{1+\sigma^2} = -\beta\beta'\sqrt{m} \qquad \mu^{1+\sigma^2} = (a-2bi)\gamma^2$$
$$\mu_\sigma^\nu = -(\beta\beta')^2 m \qquad \mu^\nu = (\gamma\gamma')^2 m = -\mu_\sigma^\nu.$$

Thus $\alpha_\sigma^\nu = (\mu_\sigma/\mu)^\nu = -1$, which proves the claim.

2. The extension k_8/k is unramified outside of 2. This follows from a standard argument (see e.g. [39, 29]): if

$$\alpha^2 - \mu\beta^2 - \mu'\gamma^2 = 0,$$

then

$$2(\alpha + \beta\sqrt{\mu}\,)(\alpha + \gamma\sqrt{\mu'}\,) = \big(\alpha + \beta\sqrt{\mu} + \gamma\sqrt{\mu'}\,\big)^2. \tag{9}$$

This implies the claim because the ideal generated by $\alpha + \beta\sqrt{\mu}$ and its conjugate $\alpha + \gamma\sqrt{\mu'}$ is not divisible by any prime ideal with odd norm.

Equation (9) is a special case of the following simple but useful observation:

Lemma 9. *Assume that $Ax^2 - By^2 - Cz^2 = 0$. Then*

$$2(x\sqrt{A} + y\sqrt{B}\,)(x\sqrt{A} + z\sqrt{C}\,) = (x\sqrt{A} + y\sqrt{B} + z\sqrt{C}\,)^2. \tag{10}$$

Proof. This is a straightforward calculation. See also [33]. □

Corollary 10. *Let $m = a^2+4b^2$. Then $\sqrt{a+2bi}$ and $\sqrt{2a+2\sqrt{m}}\,)$ generate the same quadratic extension over k_2. If $m = p$ is prime and $t^2 - pu^2 = -1$, then we also have $k_4 = k_2(\sqrt{\varepsilon}\,)$ for $\varepsilon = t + u\sqrt{p}$.*

PROOF. From $t^2 - mu^2 = -1$ we get $1 + t^2 - mu^2 = 0$, so (10) holds with $A = 1$, $B = -1$ and $C = m$. This shows that

$$2(a + 2bi)(a + \sqrt{m}\,) = (a + 2bi + \sqrt{m}\,)^2$$

and proves the first claim. Similarly, $t^2 - mu^2 + 1 = 0$ gives

$$2(t + i)(t + u\sqrt{m}\,) = (t + i + u\sqrt{m}\,)^2.$$

Next $t^2 - mu^2 = -1$ implies $t^2 + 1 = mu^2$ and $t - i = -i(a + 2bi)\rho^2$ as in Subsection 2.2. This shows that $\sqrt{i(t-i)}$ and $\sqrt{a+2bi}$ generate the same quadratic extension of $F = \mathbb{Q}(i)$. Observe that since $2i = (1+i)^2$ is a square, we also have $F(\sqrt{i(t-i)}\,) = F(\sqrt{2(t-i)}\,)$. □

3. The extension k_8/k is unramified above (2) *if* $\left(\frac{2}{a+2b}\right) = 1$. We choose the sign of a in such a way that $a \equiv 1 \bmod 4$; since b is even, we have $a \equiv 1, 5 \bmod 8$, and the following congruences hold modulo 4:

$$a \equiv 1 \bmod 8 a \equiv 5 \bmod 8$$
$$\left(\frac{i + \sqrt{a+2bi}}{1+i}\right)^2 \equiv \sqrt{a+2bi} \equiv 2 + 2i + \sqrt{a+2bi}$$
$$\left(\frac{2 + i + \sqrt{a+2bi}}{1+i}\right)^2 \equiv 2 + \sqrt{a+2bi} \equiv\ 2i + \sqrt{a+2bi}.$$

In Corollary 13 below we will show that we can always choose a primitive solution (α, β, γ) of (8) in such a way that $(2+2i) \mid \alpha$, $\beta \equiv 1 \bmod 2$ and $\gamma = i\overline{\beta} \equiv i \bmod 2$.

$x \bmod 2$	$\alpha \bmod 4$	$\beta \bmod 4$
0	0	$\pm 1 + bi$
1	$2 + 2i$	$\pm 1 + (b+2)i$

Thus in the first case we have $\alpha + \beta\sqrt{a+2bi} \equiv \pm(1+bi) \bmod 4$, which is a square modulo 4 if $a \equiv 1 \bmod 8$ and $4 \mid b$, i.e., if $a + 2b \equiv 1 \bmod 8$; moreover we have $\alpha + \beta\sqrt{a+2bi} \equiv 2 + 2i \pm (1 + (b+2)i) \bmod 4$, which is a square modulo 4 if $a \equiv 5 \bmod 8$ and $b \equiv 2 \bmod 4$, i.e., if $a + 2b \equiv 1 \bmod 8$.

This completes the proof of Theorem 8.

A little surprisingly, the diophantine equation (8) in $\mathbb{Z}[i]$ can be reduced to an equation in rational integers (see [28, p. 76]):

Proposition 11. *Let $m = a^2 + 4b^2$ for integers $a \equiv 1 \bmod 2$ and b. Then the following statements are equivalent:*

1) *Equation* (8) *is solvable.*
2) $\left[\frac{a+2bi}{\pi}\right] = 1$ *for all* $\pi \mid (a-2bi)$*;*
3) *The primes* $p \mid m$ *have inertia degree* 1 *in* $\mathbb{Q}(i, \sqrt{a+2bi}\,)$
4) $\left(\frac{2b}{p}\right) = +1$ *for all primes* $p \mid m$*.*
5) *The equation*
$$Q(r,s) = br^2 + ars - bs^2 = 2x^2. \tag{11}$$
is solvable.

Proof. For proving that 1) $\Longrightarrow$ 2), recall that ternary quadratic equations such as (8) are solvable globally if and only if they are everywhere locally solvable. Since we may disregard one place because of the product formula, all we need to check is solvability at the primes dividing $a \pm 2bi$ since we are allowed to omit the prime $1+i$ above 2. This proves the equivalence of 1) and 2); the third statement is a translation of 2) using the decomposition law in quadratic extensions.

For showing that 2) and 4) are equivalent we prove that $\left[\frac{a+2bi}{\pi}\right] = \left(\frac{2b}{p}\right)$ for every prime $\pi \mid (a-2bi)$ with norm p. In fact, observe that $2bi \equiv a \bmod \pi$; this shows that $\left[\frac{a+2bi}{\pi}\right] = \left[\frac{4bi}{\pi}\right] = \left[\frac{2b}{\pi}\right] = \left(\frac{2b}{p}\right)$, where we have used simple properties of residue symbols (see [30, Chapter 4]) and the fact that $2i = (1+i)^2$ is a square.

Finally we prove that 4) and 5) are equivalent. To this end we observe that (11) is solvable in the rationals if and only if it is solvable everywhere locally. We may omit proving solvability in $\mathbb{Q}_2$ by the product formula. Now $br^2+ars-bs^2 = 2x^2$ can be written in the form $(2br+as)^2 - ms^2 = 8bx^2$; this norm equation is solvable if and only if $\left(\frac{2b}{p}\right) = +1$ for all $p \mid m$. □

The fact that (8) and (11) are simultaneously solvable suggests that there may exist an algebraic relation between its solutions. Such a relation does indeed exist:

Lemma 12. *Let* $Q = Q_b = (b, a, -b)$ *be a quadratic form with discriminant* $m = a^2 + 4b^2$*. If* (11) *has a solution in nonzero integers, then*
$$\alpha = 2x(1+i), \quad \beta = r + si, \quad \gamma = s + ri \tag{12}$$
satisfy Equation (8)*. Moreover,* $\gcd(r,s) \mid \gcd(\alpha, \beta)$*.*

Proof. We find
$$\begin{aligned} \alpha^2 &= 8x^2 i, \\ (a+2bi)\beta^2 &= (a+2bi)(r^2 - s^2 + 2rsi) = a(r^2-s^2) - 4brs + Q(r,s)\cdot bi \\ &= a(r^2-s^2) - 4brs + 4x^2 i, \end{aligned}$$

$$(a-2bi)\gamma^2 = -a(r^2-s^2)+4brs+4x^2i,$$

which immediately implies the first claim.

Clearly the square of $\gcd(r,s)$ divides $2x^2$, hence $\gcd(r,s) \mid x$. This implies $\gcd(r,s) \mid \gcd(\alpha,\beta,\gamma)$ via (12). □

Observe that we do not claim that every solution of (8) comes from a solution of (11) via the formulas (12).

Corollary 13. *Replacing b by $-b$ if necessary we can always find a solution (α,β,γ) of (8) such that $(2+2i) \mid \alpha$, $\beta \equiv 1 \bmod 2$ and $\gamma \equiv i \bmod 2$. In this case, we have $\alpha \equiv (2+2i)x \bmod 4$ and $\beta \equiv \pm 1 + (b+2x)i \bmod 4$.*

Proof. Assume that $br^2+ars-bs^2 = 2x^2$ has a solution, which we assume to be primitive ($\gcd(r,s)=1$); since b is even and a is odd, we must have $2 \mid rs$. If r is even, replacing b by $-b$ and (r,s) by $(s,-r)$ we get a primitive solution in which s is even.

Thus we may assume that r is odd and s is even. Reducing $br^2+ars-bs^2 = 2x^2$ modulo 4 shows that $2x^2 \equiv b+s \bmod 4$, which implies $s \equiv b+2x \bmod 4$ as claimed. The other claims follow from Lemma 12. □

We now give some explicit examples.

The case $m=p$ for primes $p \equiv 1 \bmod 8$. If $m=p$ is prime, then $\left[\frac{a+2bi}{a-2bi}\right] = \left(\frac{2a}{p}\right) = 1$ if and only if $p \equiv 1 \bmod 8$. Here are a few examples:

p	h	$a+2bi$	α	β	γ	μ
17	4	$1+4i$	$2+2i$	1	i	$2+2i+\sqrt{1+4i}$
41	8	$5+4i$	$2+2i$	1	i	$2+2i+\sqrt{5+4i}$
73	4	$-3+8i$	$6-6i$	$1+2i$	$2-i$	$6-6i+(1+2i)\sqrt{-3+8i}$
89	12	$5+8i$	$10+10i$	$3+2i$	$2+3i$	$10+10i+(3+2i)\sqrt{5+8i}$
97	4	$9+4i$	$2+2i$	1	i	$2+2i+\sqrt{9+4i}$

The extension $k_8 = k_4(\sqrt{\mu})$ is unramified outside 2, and unramified everywhere if and only if $h \equiv 0 \bmod 8$ (or, equivalently, if $a+2b \equiv \pm 1 \bmod 8$). The first few examples of unramified extensions are

p	h	$a+2bi$	α	β	γ	μ
41	8	$5+4i$	$2+2i$	1	i	$2+2i+\sqrt{5+4i}$
113	8	$-7+8i$	$2+2i$	$1+2i$	$2+i$	$2+2i+(1+2i)\sqrt{-7+8i}$
137	8	$-11+4i$	$2+2i$	1	i	$2+2i+\sqrt{-11+4i}$
257	16	$1+16i$	$4+4i$	1	i	$4+4i+\sqrt{1+16i}$

The case $m = pq$ for primes $p \equiv q \equiv 1 \bmod 8$. In this case, the class of $(2, 2, n)$ with $n = \frac{1-pq}{2}$ is a square. Since the forms $(p, 0, q)$ are not equivalent to $(2, 2, n)$, the class group contains a subgroup of type $(2, 4)$. It contains $(4, 4)$ if and only if the class of $(p, 0, q)$ is a square, which happens if and only if $\left(\frac{p}{q}\right) = 1$.

Case A: $\left(\frac{p}{q}\right) = -1$. In this case, the 2-class group has type $(4, 2)$, the square class being generated by $(2, 2, n)$. Since 2 splits in the three quadratic extension $k(i)$, $k(\sqrt{p}\,)$ and $k(\sqrt{q}\,)$, one of them can be embedded into an unramified C_4-extension. By Rédei–Reichardt, this C_4-extension is generated by the square root of $a + 2bi$, where $m = a^2 + 4b^2$.

Writing $m = c^2 + 4d^2$ as a sum of squares in an essentially different way does not produce anything new because of

$$k_2(\sqrt{a + 2bi}\,) = k_2(\sqrt{p(a + 2bi)}\,) = k_2(\sqrt{c + 2di}\,).$$

Since $\left(\frac{p}{q}\right) = -1$, this implies that exactly one among the two equations of type (6) has a solution.

The unramified extension $k_2(\sqrt{p}, \sqrt{a + 2bi}\,)$ of type $(2, 4)$ over k is the full Hilbert 2-class field if and only if $\left(\frac{2}{a+2b}\right) = -1$. Observe that $\left(\frac{2}{a+2b}\right) = \left(\frac{2}{c+2d}\right)$ since 2 splits in both or in neither of the two quartic extensions.

p	q	Cl$(-4pq)$	generators	$(b, a, -b)$	$\left(\frac{2}{a+2b}\right)$	$(r,\ s,\ x)$
17	41	$(4, 2)$	$(19, 10, 38)$	$(8, 21, -8)$	-1	$(1, 0, 2)$
			$(29, 24, 29)$	$(12, 11, -12)$	-1	$-$
17	73	$(16, 2)$	$(3, 2, 414)$	$(2, 35, -2)$	$+1$	$(1, 0, 1)$
			$(17, 0, 73)$	$(10, 29, -10)$	$+1$	$-$
17	97	$(24, 2)$	$(3, 2, 550)$	$(16, 25, -16)$	$+1$	$(1, 2, 1)$
			$(17, 0, 97)$	$(20, 7, -20)$	$+1$	$-$
17	113	$(20, 2)$	$(35, -4, 55)$	$(18, 25, -18)$	-1	$(5, -2, 8)$
			$(17, 0, 113)$	$(10, 39, -10)$	-1	$-$
41	89	$(20, 2)$	$(31, 6, 118)$	$(10, 57, -10)$	-1	$(6, -1, 2)$
			$(65, 48, 65)$	$(30, 7, -30)$	-1	$-$
41	97	$(28, 2)$	$(3, 2, 1326)$	$(8, 61, -8)$	-1	$(1, 0, 2)$
			$(41, 0, 97)$	$(28, 29, -28)$	-1	$-$

Case B: $\left(\frac{p}{q}\right) = +1$. Let $m = pq = a^2 + 4b^2$. Writing $\pi = a_1 + 2b_1 i$ and $\rho = a_2 + 2b_2 i$ we find $\pi\rho = a_1a_2 - 4b_1b_2 + 2(a_1b_2 + a_2b_1)i$ and $\pi\overline{\rho} = a_1a_2 + 4b_1b_2 + 2(a_1b_2 - a_2b_1)i$. Since $\left[\frac{\overline{\pi}}{\pi}\right] = 1$ etc., we find $\left[\frac{\pi\rho}{\overline{\pi}}\right] = \left[\frac{\rho}{\overline{\pi}}\right] = \left[\frac{\rho}{\pi}\right] = \left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4$. This shows that the solvability conditions $\left[\frac{a+2bi}{\pi}\right] = +1$ are equivalent to $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = 1$.

Note that $\left(\frac{2}{a+2b}\right) = \left[\frac{1+i}{a+2bi}\right] = \left(\frac{2}{pq}\right)_4\left(\frac{pq}{2}\right)_4$, where $\left(\frac{m}{2}\right)_4 = (-1)^{(m-1)/8}$ for integers $m \equiv 1 \bmod 8$.

Theorem 14. *Assume that $m = pq = a^2 + 4b^2$ is the product of two primes $p \equiv q \equiv 1 \bmod 8$ with $\left(\frac{p}{q}\right) = 1$. Then the quartic extension $k(\sqrt{a+2bi}\,)/k$ can be embedded into an unramified cyclic octic extension if and only if $\left(\frac{2}{pq}\right)_4\left(\frac{pq}{2}\right)_4 = \left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = 1$. More precisely, the following statements are true:*

(1) *The primes above 2 split in the quartic extension $k(\sqrt{a+2bi}\,)/k$ if and only if $\left(\frac{2}{pq}\right)_4\left(\frac{pq}{2}\right)_4 = 1$.*

(2) *Equation (8) is solvable if and only if $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = 1$.*

(3) *The equation $Q(r,s) = 2x^2$, where $Q = (b, a, -b)$, is solvable in integers if and only if $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = 1$.*

(4) *The cyclic octic extension k_8/k constructed from a solution of (8) is unramified above the primes dividing (2) if and only if $\left(\frac{2}{pq}\right)_4\left(\frac{pq}{2}\right)_4 = 1$.*

Proof. The condition $\left(\frac{b}{p}\right) = 1$ is equivalent to $\left(\frac{a_1b_2+a_2b_1}{p}\right) = 1$, which by Burde's rational reciprocity law is equivalent to $\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = 1$. □

In the table below, ε denotes the values of $\left(\frac{p}{q}\right)_4$ and $\left(\frac{q}{p}\right)_4$, respectively.

p	q	Cl$(-4pq)$	generators	$(b,a,-b)$	$\left(\frac{2}{a+2b}\right)$	ε	$(r,\ s,\ x)$
17	89	$(4,4)$	$(11,8,139)$	$(14,27,-14)$	$+1$	-1	–
			$(19,16,83)$	$(6,37,-6)$	$+1$	$+1$	–
17	137	$(8,4)$	$(5,2,466)$	$(24,5,-24)$	-1	-1	–
			$(35,-8,67)$	$(20,27,-20)$	-1	$+1$	–
41	73	$(12,4)$	$(3,2,998)$	$(26,17,-26)$	-1	$+1$	–
			$(29,-18,106)$	$(14,47,-14)$	-1	-1	–
41	113	$(8,4)$	$(7,2,662)$	$(34,3,-34)$	$+1$	-1	–
			$(23,-12,203)$	$(6,67,-6)$	$+1$	$+1$	–
73	89	$(8,8)$	$(19,2,342)$	$(32,49,-32)$	$+1$	$+1$	$(1,0,4)$
			$(26,-18,253)$	$(8,79,-8)$	$+1$	$+1$	$(1,0,2)$

The cyclic quartic extensions of $\mathbb{Q}(\sqrt{-17\cdot 137}\,)$ are generated by

$$\sqrt{5+48i}, \quad \sqrt{-51+4\sqrt{17}}, \quad \sqrt{-3699+316\sqrt{137}}$$

Since $(1+i)$ is inert in $\mathbb{Q}(\sqrt{5+48i}\,)/\mathbb{Q}(i)$, this extension cannot be embedded into a cyclic quartic unramified extension by Theorem 14.(1). Similarly, $1+4i$ is inert in this extension since $\left[\frac{11+4i}{1+4i}\right] = \left(\frac{10}{17}\right) = -1$.

Let us now make a few simple remarks on special cases where the equation

$$br^2 + ars - bs^2 = 2x^2 \tag{13}$$

is solvable.

(1) $b = 2d^2$: then $(r, s, x) = (b, a, bd)$ is a solution. Note that $p = a^2 + 4b^2 = a^2 + (2d)^4$ in this case.

(2) $b = d^2$: then $(r, s, x) = (2b, a + e, f)$ is a solution, where $p = e^2 + 2f^2$.

4. 2-descent on elliptic curves

In this section we will give an exposition of Apéry's lecture [1]. The forms Q_b also show up in several other investigations of elliptic curves with primes $p = a^2 + 4b^2$ as parameters (see e.g. [42]), and we have selected Apéry's article mainly because his presentation was the least polished. Apéry starts by recalling a conjecture made by Mordell in Debrecen 1968: for each prime $p \equiv 5 \bmod 8$, the curve

$$y^2 = px^4 + 1 \tag{14}$$

has a nontrivial (i.e., $(x, y) \neq (0, \pm 1)$) rational point (this is also predicted by the more general parity conjecture). Since (14) is a curve of genus 1 with a rational point, it is an elliptic curve. The conjecture that (14) has nontrivial rational points is equivalent to the conjecture that the elliptic curve has Mordell-Weil rank 1 (the fact that the rank cannot be larger follows from the computation of the Selmer groups).

Consider more generally an elliptic curve

$$E : y^2 = x(x^2 + Ax + B)$$

defined over $\mathbb{Q}$ with a rational torsion point $(0, 0)$ of order 2. Each rational affine point on E has the form (x, y) with

$$x = b_1 \frac{m}{e^2}, \quad y = b_1 \frac{mn}{e^3},$$

and comes from a rational point on one of the torsors

$$T : n^2 = b_1 m^4 + am^2 e^2 + b_2 e^4$$

with $b_1 b_2 = B$ and b_1 squarefree.

The curve

$$E' : y^2 = x(x^2 + A'x + B'), \quad \text{with} \quad A' = -2Ax \text{ and } B' = A^2 - 4B,$$

is 2-isogenous to E.

Specializing to $A = 0$ and $B = p$ we find that the elliptic curves

$$E : y^2 = x(x^2 + p) \quad \text{and} \quad E' : y^2 = x(x^2 - 4p) \tag{15}$$

have the torsors

$$n^2 = pm^4 + e^4 \quad \text{and} \quad n^2 = m^4 - 4pe^4, \quad n^2 = pm^4 - 4e^4.$$

By the theory of 2-descent on elliptic curves, (15) has rank $r \le 1$, with equality if and only if the torsor $n^2 = pm^4 - 4e^4$ has a nontrivial rational point.

Now consider the torsor

$$Z^2 = pX^4 - 4Y^4$$

(we are using Apéry's notation) and write $p = a^2 + 4b^2$. From

$$pX^4 = Z^2 + 4Y^4 = (Z + 2iY^2)(Z - 2iY^2)$$

we get, using unique factorization in $\mathbb{Z}[i]$,

$$Z + 2iY^2 = (a + 2bi)(\xi + i\eta)^4,$$

where $X = \xi^2 + \eta^2$. Comparing real and imaginary parts yields

$$Y^2 = b(\xi^4 - 6\xi^2\eta^2 + \eta^4) + 2a\xi\eta(\xi^2 - \eta^2). \tag{16}$$

Setting $r = \xi^2 - \eta^2$ and $s = 2\xi\eta$, we find

$$X^2 = r^2 + s^2, \quad Y^2 = br^2 + ars - bs^2. \tag{17}$$

Given the last pair of equations we parametrize the Pythagoren equation $X^2 = r^2 + s^2$ via $r = \xi^2 - \eta^2$, $s = 2\xi\eta$ and $X = \xi^2 + \eta^2$, plug the results into the second equation and retrieve (16).

Thus finding a rational point on E boils down to finding a simultanous representation of squares for the pair of forms $Q = (1, 0, 1)$ and $Q_b(b, a, -b)$.

Example. For $p = 797$, we have $a = 11$ and $b = 13$. We find

$$\begin{aligned} \xi &= 1462 & \eta &= 771 \\ X &= 2731885 & Y &= 1773371 \\ x &= \frac{5948166935620325}{3144844703641} & y &= \frac{458544116976814482315845}{5576976396940543811} \end{aligned}$$

since $x = p\frac{X^2}{Y^2}$ and $y = p\frac{XZ}{Y^3}$, where $Z = 210600981540301$.

5. Cyclic quartic fields

In the late 1940s, HASSE was interested in the explicit arithmetic of abelian extensions; in 1948 he presented a memoir [24] on the computation of unit groups and class numbers of cyclic cubic and quartic fields, and in 1952 he published his book [25] on the investigation of class numbers of abelian number fields.

The quadratic form Q_b shows up in Hasse's treatment of cyclic quartic number fields in [24]. Since this work has remained largely obscure we would like to provide as much background as is necessary to begin to appreciate Hasse's results.

Let $K/\mathbb{Q}$ be a cyclic quartic extension; let F denote its conductor, and H the subgroup of the group D of nonzero ideals in $\mathbb{Q}$ coprime to F that corresponds to this extension by class field theory. Thus $D/H \simeq \mathrm{Gal}(K/\mathbb{Q})$; let χ be the ray class character on D/H, and $T = -\sum \chi(t)^{-1} e(t)$ the corresponding Gauss sum.

Let k denote the quadratic subfield of K; its conductor f divides F, hence we can write $F = fG$ for some integer G. Hasse proves that there exist integers a, b such that $f = a^2 + 4b^2$ and

$$K = \mathbb{Q}\left(\sqrt{\chi(-1)G\frac{f + a\sqrt{f}}{2}}\right).$$

His first main result is a description of an integral basis of K in terms of invariants of the field, that is, in terms of Gauss sums. If τ denotes the Gauss sum attached to χ^2, then the algebraic integers in k have the form $\frac{1}{2}(x + y\tau)$ with $x \equiv \tau y \bmod 2$. Hasse succeded in determining the ring of integers in K in a similar way. In fact, for elements $x \in k$ and $y \in \mathbb{Q}(i)$ he observes that every element of K can be represented in the form

$$[x, y] = \frac{1}{2}\left(x + \frac{y\,T + \overline{y}\,\widetilde{T}}{2}\right),$$

where $\overline{y}$ denotes the complex conjugate of y and where $\widetilde{T} = \chi(-1)\overline{T}$.

The ring of integers in K consists of all elements $[x, y]$ with $x \in \mathcal{O}_k$ and $y \in \mathbb{Z}[i]$ such that

$$x \equiv F \cdot \frac{\mathrm{Tr}\left(\frac{1+i}{2}y\right) + \mathrm{Tr}\left(\frac{1-i}{2}y\right)\,\tau}{2} \bmod 2,$$

where Tr denotes the trace of $\mathbb{Q}(i)/\mathbb{Q}$.

Now Hasse observes that the product $x(y\,T + \overline{y}\,\widetilde{T})$ can be written in the form

$$x(y\,T + \overline{y}\,\widetilde{T}) = (x \circ y)\,T + \overline{x \circ y}\,\widetilde{T},$$

where

$$x \circ y = \frac{x_0 y + x_1(a - 2bi)\overline{y}}{2}, \quad \text{with } y \in \mathbb{Z}[i],$$

and where x_0 and x_1 are determined by the equation $x = \frac{1}{2}(x_0 + x_1\tau)$. This defines an action of $k^\times$ on $\mathbb{Q}(i)^\times$ (which induces an action of $\mathcal{O}_k$ on $\mathbb{Z}[i]$); in fact, the operator product $x \circ y$ has the following formal properties:

Lemma 15. *For all $x \in k^\times$ and all $y \in \mathbb{Q}(i)$ we have*

(1) $1 \circ y = y$.

(2) $(x_1x_2) \circ y = x_1 \circ (x_2 \circ y)$.

(3) *$x \circ y$ is $\mathbb{Q}$-bilinear: $qx \circ y = x \circ qy = q(x \circ y)$ for all $q \in \mathbb{Q}$.*

(4) *$x \circ iy = i(x' \circ y)$, where x' is the conjugate of x.*

(5) *$x \circ y = 0$ if and only if $x = 0$ or $y = 0$.*

Hasse uses this action for simplifying the numerical computation (he was working with pencil and paper!) of products in the number field K. The computation of squares, for example, is facilitated by the observation that

$$[x, y]^2 = \left[\frac{1}{2}\left(x^2 + \chi(-1)G\frac{N(y)f + \phi(y)\tau}{2}\right), x \circ y\right],$$

where N and S denote the trace in $\mathbb{Q}(i)/\mathbb{Q}$ and where ϕ is the binary quadratic form defined for $y = r + si$ by

$$\phi(y) = \frac{1}{2}S((a + 2bi)y^2) = ar^2 - 4brs - as^2.$$

In the expressions giving the action of the Galois group on $[x, y]$, the form

$$\widehat{\phi}(y) = -\frac{1}{4}S(i(a + 2bi)y^2) = br^2 + ars - bs^2$$

shows up, for which Hasse observes the identity (see [24, (19)]

$$\widehat{\phi}(\alpha \circ y) = N(\alpha)\widehat{\phi}(y)$$

for $\alpha \in \mathcal{O}_k$ and $y \in \mathbb{Z}[i]$, where N denotes the norm.

Hasse's goal was characterizing the unit groups of cyclic quartic extensions in a way similar to the real quadratic case, where the fundamental unit is uniquely determined by the minimal solution of the Pell equation $T^2 - mU^2 = 4$.

In the real cyclic case $K/\mathbb{Q}$, let k denote the quadratic subfield of K. The unit group E_K of K is described by the following invariants:

(1) the unit group E_k of the quadratic subfield,

(2) the group $E_{K/k}$ of relative units satisfying $N_{K/k}\eta = \pm 1$, and

(3) the unit index $Q = (E_K : E_{K/k}E_k)$.

These invariants are characterized as follows:

(1) The unit index Q is either 1 or 2;

(2) There is a unit η such that the group $E_{K/k}$ is generated by -1, η and its conjugate η'.

This unit η can be chosen in an essentially unique way among its conjugates etc., and this unit is then called *the* relative fundamental unit of K. Hasse's main result is

Theorem 16. *The relative fundamental unit η of K is the relative unit $\varepsilon \neq \pm 1$ with the property that $|S_{K/\mathbb{Q}}(\varepsilon^2)|$ is minimal.*

It seems that such geometric investigations of units quickly become too technical when cyclic quartic extensions are replaced by number fields of higher degree.

ACKNOWLEDGEMENTS. I thank the referee for the very careful reading of the manuscript.

References

[1] R. APÉRY, Points rationels sur certaines courbes algébriques, Journées Arithmétiques de Bordeaux 1974, *Astérisque* **24–25** (1975), 229–235.

[2] S. N. ARTEHA, Method of hidden parameters and Pell's equation, *JPJ Algebra Number Theory Appl.* **2** (2002), 21–46.

[3] L. BAPOUNGUÉ, Sur la résolubilité de l'équation $ax^2 + 2bxy - kay^2 = \pm 1$, Thèse Univ. Caen, 1989, see also *C. R. Acad. Sci. Paris* **309** (1989), 235–238.

[4] L. BAPOUNGUÉ, Un critère de résolution pour l'équation diophantienne $ax^2+2bxy-kay^2 = \pm 1$, *Expos. Math.* **16** (1998), 249–262.

[5] L. BAPOUNGUÉ, Sur la résolubilité de l'équation $ax^2 + 2bxy - 8ay^2 = \pm 1$, *IMHOTEP, J. Afr. Math. Pures Appl.* **3** (2000), 97–111.

[6] L. BAPOUNGUÉ, Sur les solutions génerales de l'équation diophantienne $ax^2+2bxy-kay^2 = \pm 1$, *Expos. Math.* **18** (2000), 165–175.

[7] L. BAPOUNGUÉ, The diophantine equation $ax^2+2bxy-4ay^2 = \pm 1$, *Intern. J. Math. Math. Sci.* **35** (2003), 2241–2253.

[8] A. BARKER-HOYT, Gauss Composition and Bhargava's Cube Law, master thesis Univ. Maine, 2005.

[9] E. BENJAMIN and C. SNYDER, Elements of order four in the narrow class group of real quadratic number fields, *J. Australian Math. Soc.* (*to appear*).

[10] M. BHARGAVA, Gauss composition and generalizations, Algorithmic Number Theory, Sydney, 2002, pp. 1–8, Lecture Notes in Comput. Sci., 2369, *Springer, Berlin*, 2002.

[11] E. Brown, Representation of discriminantal divisors by binary quadratic forms, *J. Number Theory* **3** (1971), 213–225.

[12] E. Brown, Discriminantal divisors and binary quadratic forms, *Glasgow Math. J.* **13** (1972), 69–73.

[13] H. Cohn and G. Cooke, Parametric form of an eight class field, *Acta Arith.* **30** (1976), 367–377.

[14] G. Cooke, Construction of Hilbert class field extension of $K = \mathbb{Q}(\sqrt{-41})$, unpublished lecture notes Cornell Univ., 1974.

[15] D. A. Cox, Primes of the form $x^2 + ny^2$, Fermat, Class Field Theory, and Complex Multiplication, *John Wiley*, 1989.

[16] P. Epstein, Zur Auflösbarkeit der Gleichung $x^2 - Dy^2 = -1$, *J. Reine Angew. Math.* **171** (1934), 243–252.

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

[18] D. Flath, Introduction to Number Theory, *Wiley & Sons, New York*, 1989.

[19] A. Gérardin, Sur l'èquation $x^2 - Ay^2 = 1$, *L'Ens. Math.* **19** (1917), 316–318, *Sphinx-Œdipe* **12** June 15, 1917, 1–3.

[20] A. Grytczuk, F. Luca and M. Wojtowicz, The negative Pell equation and Pythagorean triples, *Proc. Japan Acad.* **76** (2000), 91–94.

[21] S. Günther, Ueber einen Specialfall der Pell'schen Gleichung, *Blätter für das Bayerische Gymnasial- und Realschulwesen* **17** (1882), 19–24.

[22] K. Hardy and K. Williams, On the solvability of the diophantine equation $dV^2 - 2eVW - dW^2 = 1$, *Pac. J. Math.* **124** (1986), 145–158.

[23] D. S. Hart, Solution of an indeterminate problem, *Analyst* **5** (1878), 118–119.

[24] H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, *Abh. Deutsch. Akad. Wiss. Berlin* (1950), 3–95, *Math. Abh.* III, 289–379.

[25] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, *Akademie Verlag, Berlin*, 1952.

[26] C. Herz, in Seminar on Complex Multiplication, *Springer*.

[27] P. Kaplan, Unités de norme -1 de $\mathbb{Q}(\sqrt{p})$ et corps de classes de degré 8 de $\mathbb{Q}(\sqrt{-p})$ où p est un nombre premier congru à 1 modulo 8, *Acta Arith.* **32** (1977), 239–243.

[28] F. Lemmermeyer, Die Konstruktion von Klassenkörpern, Ph. D. thesis, *Univ. Heidelberg*, 1994.

[29] F. Lemmermeyer, Rational quartic reciprocity, *Acta Arithmetica* **67** (1994), 387–390.

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

[31] F. Lemmermeyer, Higher descent on Pell conics, I. *From Legendre to Selmer*, arXiv: 0311309v1; II. *Two centuries of missed opportunities*, arXiv: 0311296v1; III. *The first 2-descent*, arXiv: 0311310v1.

[32] F. Lemmermeyer, Binary Quadratic Forms and Counterexamples to Hasse's Local-Global Principle, preprint 2010.

[33] F. Lemmermeyer, Relations in the 2-class group of quadratic number fields, *J. Austr. Math. Soc.* **93** (2012), 115–120.

[34] F. Lorenz and F. Lemmermeyer, Algebra I, *Elsevier/Springer-Verlag*, 2007.

[35] G. Pall, Discriminantal divisors of binary quadratic forms, *J. Number Theory* **1** (1969), 525–532.

[36] 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.

[37] L. Rédei, Über die Pellsche Gleichung $t^2 - du^2 = -1$, *J. Reine Angew. Math.* **173**.

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

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

[40] G. Sansone, Sulle equazioni indeterminate delle unità di norma negativa dei corpi quadratici reali, *Rend. Acad. d. L. Roma* **2** (1925), 479–484.

[41] G. Sansone, Ancora sulle equazioni indeterminate delle unità di norma negativa dei corpi quadratici reali, *Rend. Acad. d. L. Roma* **2** (1925), 548–554.

[42] R. J. Stroeker and J. Top, On the equation $Y^2 = (X + p)(X^2 + p^2)$, *Rocky Mt. J. Math.* **24** (1994), 1135–1161.

[43] J. J. Sylvester, Mathematical question 6243, *Educational Times* **34** (1881), 21–22.

FRANZ LEMMERMEYER
MÖRIKEWEG 1
73489 JAGSTZELL
GERMANY

E-mail: hb3@ix.urz.uni-heidelberg.de

(Received March 29, 2015; revised July 27, 2015)