Parametric families of real quadratic fields

and the class number one problem

András Biró

(Rényi Institute, Budapest)

Online Number Theory Seminar, May 31, 2024

Let $K = \mathbf{Q}(\sqrt{d})$, where $\mathbf{Q}$ is the rational field, d is a fundamental discriminant, let $h(d)$ be the class number of K, and let

$$\chi_d(n) = \left(\frac{d}{n}\right)$$

be the Kronecker symbol.

Dirichlet Class Number Formula:

For $d < 0$ we have

$$h(d) = \frac{w\,|d|^{1/2}}{2\pi} L(1, \chi_d),$$

where w is the number of roots of unity in K.

For $d > 0$ we have

$$h(d) \log \epsilon_d = d^{1/2} L(1, \chi_d),$$

where $\epsilon_d > 1$ is the fundamental unit in K.

First let $d < 0$. For this case Gauss conjectured that

$$h\left(|d|\right) \to \infty$$

as $|d| \to \infty$.

This was proved by Heilbronn in 1934. Today we can see that it is an immediate consequence of Dirichlet's Class Number Formula above and Siegel's theorem:

$$L(1, \chi) \gg_\epsilon q^{-\epsilon}$$

for a primitive character with conductor q.

HOWEVER: this is ineffective!

The problem of determining all imaginary quadratic fields with class number 1 remained open for a long time.

This was first solved by Heegner in 1952, but his proof was not accepted at that time, and then it was also solved independently by Baker and by Stark in the 1960s.

The best effective lower bound known today is

$$h(d) \gg (\log |d|)^{1-\epsilon},$$

and it is due to Goldfeld, Gross and Zagier.

Now let $d > 0$. For this case Gauss conjectured that there are infinitely many d with class number 1. This problem is still unsolved.

For $d > 0$, we cannot separate the class number and the fundamental unit in the Dirichlet Class Number Formula.

However, for some special families of real quadratic fields (where the fundamental unit is very small), the situation is analoguous to the imaginary case: Dirichlet's formula and Siegel's theorem imply ineffectively that there are only finitely many solutions of the class number one problem, but the effective determination of these finitely many solutions is a separate problem.

Example (Yokoi's family): $d = n^2 + 4$ with an integer n and we assume that d is squarefree. In this case the fundamental unit can be determined explicitly, and one has

$$\log d \ll \log \epsilon_d \ll \log d.$$

THEOREM 1 (Biró, 2003). *Yokoi's conjecture is true, i.e. if* $d = n^2 + 4$ *for an integer* n, d *is squarefree and* $h(d) = 1$, *then* $n = 1, 3, 5, 7, 13$ *or* 17.

In fact the method of Goldfeld, Gross and Zagier works also for $d > 0$, and it gives

$$h(d) \log \epsilon_d \gg (\log d)^{1-\epsilon} .$$

In the case of the Yokoi family this gives

$$h(d) \gg (\log d)^{-\epsilon} .$$

So this argument does not prove Yokoi's conjecture, but it is not very far from that.

Considering Yokoi's family $d = n^2 + 4$, two questions arise:

Can one define similar families of real quadratic fields, where the fundamental unit is small?

If yes, can one solve the class number one problem for that family?

There are some results of this kind, for example:

THEOREM 2 (Biró, 2003). *Chowla's conjecture is true, i.e. if* $d = 4n^2 + 1$ *for an integer* n, d *is squarefree and* $h(d) = 1$, *then* $n \leq 13$.

THEOREM 3 (Byeon, Kim and Lee, 2007). *Mollin's conjecture is true, i.e. if* $d = n^2 - 4$ *for an integer* n, d *is squarefree and* $h(d) = 1$, *then* $n \leq 21$.

In fact every such discriminant is of Richaud-Degert type, which means the following: $d = (an)^2 + ka$ for $\pm k = 1, 2$ or 4.

We have the following theorem for the case $k = 4$:

THEOREM 4 (Biró, Lapkova 2012). *If* $d = (an)^2 + 4a$ *is squarefree for* a *and* n *positive integers and* $d > 1253$, *then* $h(d) > 1$.

It can be expected that the method works for the other values of k.

What is special about these discriminants?
Their continued fraction expansion is very short, and it can be given explicitly:

If $d = 4n^2 + 1$, let $\alpha = \frac{1-2n+\sqrt{d}}{2}$, then its regular continued fraction expansion has the form

$$\alpha = \left[0, \overline{1, 1, 2n-1}\right].$$

If $d = n^2 - 4$, let $\alpha = \frac{2-n+\sqrt{d}}{2}$, then we have

$$\alpha = \left[0, \overline{1, n-2}\right].$$

If $d = (an)^2 + 4a$, let $\alpha = \frac{-an+\sqrt{d}}{2}$, then we have

$$\alpha = [0, \overline{n, an}].$$

There are more such quadratic polynomials, they were characterized by Schinzel:

For a quadratic irrational α let us denote by $lp\,(\alpha)$ the length of the shortest period of the continued fraction expansion of α.

THEOREM 5 (Schinzel, 1961). *Let $f(n) = an^2 + bn + c$ with integers a, b, c satisfying $a > 0$ and $\Delta := b^2 - 4ac \neq 0$. Then we have that $lp\left(\sqrt{f(n)}\right)$ is bounded for $n \geq 1$ if and only if a is a square and Δ divides $4(2a, b)^2$.*

In every such case the fundamental unit can be determined explicitly, and one has

$$\log d \ll \log \epsilon_d \ll \log d.$$

It is likely that for every fixed f with the above property our method is suitable to solve the class number one problem.

We now describe the method very shortly.

Let $d > 0$ be a fundamental discriminant. Let R be the ring of algebraic integers of $K = \mathbf{Q}(\sqrt{d})$, denote by $I(K)$ the set of nonzero ideals of R and by $P(K)$ the set of nonzero principal ideals of R. Let $N(a)$ be the norm of an $a \in I(K)$. Let $q > 2$ be an integer with $(q, d) = 1$, and let χ be a primitive character with conductor q. Remember that

$$\chi_d(n) = \left(\frac{d}{n}\right)$$

is the Kronecker symbol. For $\Re s > 1$ define

$$\zeta_K(s) = \sum_{a \in I(K)} \frac{1}{N(a)^s}, \quad \zeta_K(s, \chi) = \sum_{a \in I(K)} \frac{\chi(N(a))}{N(a)^s},$$

and

$$\zeta_{P(K)}(s, \chi) = \sum_{a \in P(K)} \frac{\chi(N(a))}{N(a)^s}.$$

It is well-known that $\zeta_K(s) = \zeta(s)L(s, \chi_d)$. Twisting by χ, we easily see that

$$\zeta_K(s, \chi) = L(s, \chi)L(s, \chi\chi_d).$$

If $h(d) = 1$, then

$$\zeta_K(s,\chi) = \zeta_{P(K)}(s,\chi),$$

by definition. Hence

$$\zeta_{P(K)}(s,\chi) = L(s,\chi)L(s,\chi\chi_d).$$

Let χ be an odd primitive character modulo q. It is well-known that for a primitive character ψ with $\psi(-1) = -1$ and with conductor f one has

$$L(0,\psi) = -\frac{1}{f}\sum_{a=1}^{f} a\psi(a) \neq 0,$$

so

$$q\zeta_{P(K)}(0,\chi) = \left(\sum_{a=1}^{q} a\chi(a)\right)\left(\frac{1}{qd}\sum_{b=1}^{qd} b\chi(b)\chi_d(b)\right).$$

Hence the algebraic integer $\sum_{a=1}^{q} a\chi(a)$ divides the left-hand side, this is the basis of the proof. To use this fact we need a formula for the left-hand side.

Once we have a formula for the special value at 0 of the partial zeta function belonging to the principal ideal class, we can use elementary algebraic number theory: we use the above divisibility condition with finitely many well-chosen fixed characters χ to get a contradiction with the class number one condition.

In the case of the Yokoi family I gave such a simple formula without using the continued fraction expansion.

Then in a joint paper with Andrew Granville in 2012 we generalized that formula for any quadratic number field, expressing the special value at 0 of a partial zeta function as above in terms of the continued fraction expansion of $\omega_D = \frac{1+\sqrt{D}}{2}$. Since the continued fraction expansion is explicitly known in all of the examples given above, so we can use this formula in every case.

We now state that formula for the special value:

Let D be an odd squarefree number and $K = \mathbf{Q}(\sqrt{D})$. Let $\omega_D = \frac{1+\sqrt{D}}{2}$, then its regular continued fraction expansion has the form

$$\omega_D = [a_0, \overline{a_1, a_2, \ldots, a_l}] \, ,$$

and let $\alpha := \omega_D - a_0$. For $1 \leq j \leq l$ define the relatively prime positive integers p_j and q_j by

$$\frac{p_j}{q_j} = [0, a_1, a_2, \ldots, a_j] \, ,$$

and write

$$\alpha_0 := -\alpha, \ \alpha_j := p_j - q_j \alpha \text{ for } 1 \leq j \leq l.$$

For $1 \leq j \leq l$ introduce the quadratic forms

$$Q_j \left(x, y \right) = \left(\alpha_{j-1} x + \alpha_j y \right) \left(\overline{\alpha_{j-1}} x + \overline{\alpha_j} y \right) = A_j x^2 + B_j xy + C_j y^2$$

with rational integer coefficients A_j, B_j, C_j.
Let χ be an odd primitive character modulo $q > 1$ with $(q, 2D) = 1$.

Then by a paper of Biro and Granville from 2012 we have that $\zeta_{P(K)}(0,\chi)$ equals the sum of

$$\frac{2}{q^2}\sum_{j=1}^{l}\sum_{1\leq u,v\leq q-1} uv\chi\left((-1)^j\left(A_ju^2+B_juv+C_jv^2\right)\right)$$

and

$$\frac{E_\chi}{q^2}\chi\left(-D\right)\left(\frac{D}{q}\right)\sum_{j=1}^{l}a_j\overline{\chi\left((-1)^j A_j\right)}$$

with an algebraic integer E_χ.

Therefore in order to apply our method for a given family of real quadratic fields we need the following two properties of the family:

(1) The size of the logarithm of fundamental unit, i.e. $\log \epsilon_d$ should be small compared to $\sqrt{D}$ to ensure through the ineffective theorem of Siegel that the family has finitely many elements of class number one.

(2) We should know explicitly the continued fraction expansion of $\sqrt{D}$.

Having these conditions for a certain family does not mean automatically that our method works. It just means that we can make the first steps of the proof, and we can hope that choosing the characters appropriately we can determine every field of class number one in the family.

As we mentioned earlier, in the above examples we have $\log d \ll \log \epsilon_d \ll \log d$.

The problem is more difficult in a family where the fundamental unit is larger. For example, if we take a family where $\log \epsilon_d$ may be as large as $\log^2 d$, then the Goldfeld-Gross-Zagier reasoning gives only

$$h(d) \gg (\log d)^{-1-\epsilon},$$

which is very far from a solution of the class number one problem.

Several such families are known, e.g. the following family was introduced by Hendy in 1974:

For integers $b \geq 0$, $c > 0$, $n \geq 2$ write

$$D = D_{n,b,c} := \left(b\left(1 + bc\right)^n + c\right)^2 + 4\left(1 + bc\right)^n,$$

and assume that D is squarefree. Let $K = K_{n,b,c} = \mathbf{Q}\left(\sqrt{D_{n,b,c}}\right)$. The fundamental unit ϵ_D can be computed explicitly and $\log \epsilon_d \ll \log^2 D$.

If we assume that bc is not too large in terms of n, precisely we assume $bc > 0$ and $\log(1 + bc) = n^{o(1)}$, then we have

$$\log \epsilon_D \gg \log^{2-o(1)} D.$$

Indeed, if $\omega_D = \frac{1+\sqrt{D}}{2}$, then its regular continued fraction expansion has the form

$$\omega_D = \left[a_0, \overline{a_1, a_2, \ldots, a_{2n+1}}\right].$$

We know explicitly the coefficients:

$$a_0 = \frac{1}{2}\left(b\left(1 + bc\right)^n + c + 1\right),$$

for $0 \leq i \leq n-1$ we have

$$a_{2i+1} = b\left(1+bc\right)^{i}, \quad a_{2i+2} = b\left(1+bc\right)^{n-1-i},$$

finally

$$a_{2n+1} = b\left(1+bc\right)^{n} + c.$$

For the fundamental unit we have

$$\epsilon_D = \frac{b\left(1+bc\right)^{n} + c + \sqrt{D}}{2}\left(\frac{b^2\left(1+bc\right)^{n} + 2 + bc + b\sqrt{D}}{2\left(1+bc\right)}\right)^{n}.$$

We were able to solve the problem for this family under the condition that b is divisible by a certain fixed positive integer N_0.

THEOREM 6 (Biró, 2022). *Let* $b \geq 0$, $c > 0$, $n \geq 2$ *be integers, assume that* $D_{n,b,c}$ *is squarefree and the field* $K_{n,b,c} = \mathbf{Q}\left(\sqrt{D_{n,b,c}}\right)$ *has class number one. Suppose that* N_0 *divides* b, *where* N_0 *denotes the product of* 5^2, 7, 41, 61, *and* 1861. *Then* $b = 0$, *and* $c \in \{1,3,5,7,13,17\}$.

The $b = 0$ case of Theorem 6 is exactly the statement of Yokoi's Conjecture (i.e. Theorem 1 above), so Theorem 6 is a generalization of Yokoi's Conjecture.

It is possible that similar statements may be proved with other specific values of N_0. However, we cannot show it with $N_0 = 1$, i.e. the class number one problem for the entire family remains open.

So there are open problems for families having $\log \epsilon_D \ll \log^2 D$. But it would be even more interesting to consider families having even larger, explicitly determined fundamental units. For example it would be good to consider a family with $\log \epsilon_D \gg \log^3 D$.

However, as far as I know, such a family is not known!

An interesting family was given by Yamamoto in 1971. His construction is based on his following general theorem.

THEOREM 7 (Yamamoto, 1971). *Let $p_1 < p_2 < \ldots < p_n$ be rational primes. Assume that there exist infinitely many real quadratic fields F satisfying the following condition:*
Every p_i is decomposed in F into the product of two principal prime ideals.
Then there exists a positive constant c_0 depending only on p_i and n such that

$$\log \epsilon > c_0 \, log^{n+1} D$$

for sufficiently large D, where D is the discriminant and ϵ is the fundamental unit of F.

The proof is elementary, it depends on the following observation:

Assume that I_j, $1 \leq j \leq J$ are principal ideals in a quadratic field F with the following properties. Each I_j is relatively prime to its conjugate and $N\left(I_j\right) < \sqrt{D}/2$. Then

$$\epsilon \geq \prod_j \left(\frac{\sqrt{D}}{2N\left(I_j\right)} \right).$$

And under the conditions of the theorem we can construct many such ideals: if P_i is a prime ideal divisor of p_i, then

$$\prod_i P_i^{k_i}$$

is such an ideal, if its norm is smaller than $\sqrt{D}/2$. The above observation gives the result.

Then he gave a concrete family: Let $p \neq q$ be rational primes such that q does not divide $p-1$, and for positive integers k put

$$D = \left(p^k q + p + 1\right)^2 - 4p.$$

This family satisfies the above conditions with $n = 2$ by the following simple facts:

We have $D \equiv 1$ mod 4, $D \equiv 1$ mod p, $D \equiv (p-1)^2$ mod q, and

$$D - \left(p^k q + p + 1\right)^2 = -4p, \qquad D - \left(p^k q + p - 1\right)^2 = 4p^k q.$$

For larger n no such example is known.

In the above family

$$D = \left(p^k q + p + 1\right)^2 - 4p$$

we have $\log \epsilon > \log^3 D$, but the fundamental unit is not known explicitly. In fact, I do not know any upper bound for the fundamental unit. Therefore, not only the effective determination of the fields with class number one is not known, but I cannot decide even the following problem:

Problem. *Are there infinitely many fields with class number one in the Yamamoto family?*