Djordjo Milovic
Department of Mathematics
University College London
djordjo.milovic@ucl.ac.uk

Research Stieltjes Prize 2016

Divisibility by 16 of class numbers in families

In 2016 Djordjo Milovic has been awarded the Stieltjes Prize for one of the two best PhD theses in mathematics in the Netherlands. The prize was awarded for his thesis entitled *On the 16-rank of Class Groups of Quadratic Number Fields*, which he completed at Leiden University. After a membership at the Institute for Advanced Study in Princeton he became a Research Associate at University College London. In this article he describes his current research on class numbers in families.

The negative Pell equation

In number theory, an important generalization of the ring of rational integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

is the ring of integers of a number field. One of the main applications of such rings of integers is that they help us study integral solutions to polynomial equations over the usual integers $\mathbb{Z}$. For example, let d be a positive squarefree integer, and for simplicity assume that d is even. As we will see, the existence of integral solutions $x, y \in \mathbb{Z}$ to the *negative Pell equation*

$$x^2 - dy^2 = -1 \qquad (1)$$

is intricately related to certain arithmetic invariants of the *quadratic number ring*

$$\mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d} : m, n \in \mathbb{Z}\}.$$

Addition and multiplication in $\mathbb{Z}[\sqrt{d}]$ is straightforward, defined exactly as one would expect:

$$(m_1 + n_1\sqrt{d}) + (m_2 + n_2\sqrt{d}) = (m_1 + m_2) + (n_1 + n_2)\sqrt{d}$$

and

$$(m_1 + n_1\sqrt{d})(m_2 + n_2\sqrt{d}) = (m_1 m_2 + d n_1 n_2) + (m_1 n_2 + m_2 n_1)\sqrt{d}.$$

However, the resulting arithmetic in $\mathbb{Z}[\sqrt{d}]$ can be quite tricky. Unlike in the case of $\mathbb{Z}$, an element in $\mathbb{Z}[\sqrt{d}]$ need not have unique factorization into irreducible elements. For instance, in $\mathbb{Z}[\sqrt{10}]$, the element 6 has two essentially distinct factorizations, namely $2 \cdot 3$ and $(4 + \sqrt{10})(4 - \sqrt{10})$.

Unique factorization is recovered after passing to *ideals*. An ideal in $\mathbb{Z}[\sqrt{d}]$ (or in any ring) is a set of elements $\mathfrak{a}$ closed under addition and contagious under multiplication; more precisely, for all elements α_1 and α_2 of $\mathfrak{a}$ and any element β of $\mathbb{Z}[\sqrt{d}]$, the elements $\alpha_1 + \alpha_2$ and $\alpha_1\beta$ belong to $\mathfrak{a}$. In this language, unique factorization in $\mathbb{Z}[\sqrt{d}]$ is equivalent to the statement that every ideal in $\mathbb{Z}[\sqrt{d}]$ is *principal*, i.e., that it is the set of multiples of some α in $\mathbb{Z}[\sqrt{d}]$ (in which case we say that α is a *generator* of that principal ideal). To measure the failure of ideals to be principal, one attaches to $\mathbb{Z}[\sqrt{d}]$ an invariant called the *(ordinary) class group* Cl_d and defined as the quotient of the group of *all* non-zero ideals of $\mathbb{Z}[\sqrt{d}]$ by the subgroup of those that are principal. Hence, if every ideal happens to be principal, this quotient is trivial, and so unique factorization in $\mathbb{Z}[\sqrt{d}]$ is equivalent to the statement that the class group Cl_d is the trivial group of one element.

A closely related invariant is the *narrow class group* Cl_d^+, defined as the quotient of the group of all non-zero ideals of $\mathbb{Z}[\sqrt{d}]$ by the subgroup of those that are principal *and* have a generator $m + n\sqrt{d}$ of positive *norm*, i.e., satisfying $(m + n\sqrt{d})(m - n\sqrt{d}) = m^2 - dy^2 > 0$. Since the norm is multiplicative, and since the element $\sqrt{d}$ has norm $-d < 0$, one deduces that the class group Cl_d coincides with the narrow class group Cl_d^+ exactly when $\mathbb{Z}[\sqrt{d}]$ has an element of norm -1; in other words, $\mathrm{Cl}_d = \mathrm{Cl}_d^+$ if and only if the negative Pell equation (1) is solvable with $x, y \in \mathbb{Z}$.

A burgeoning area of research in number theory is *arithmetic statistics,* the study of how various arithmetic invariants behave on average. In our case, one might be interested in knowing *how often* (1) is solvable over the integers, that is, how often the ordinary and the narrow class groups coincide. This is a very difficult question. To get a first sense of its intricacies, notice that (1) cannot have

an integral solution whenever d has a prime factor $\ell \equiv 3 \bmod 4$; for in that case, reducing the equation modulo ℓ (i.e., comparing remainders upon division by ℓ) would give $x^2 \equiv -1 \bmod \ell$, which cannot happen when $\ell \equiv 3 \bmod 4$. The set of even squarefree integers with no prime factors congruent to 3 modulo 4 has natural density 0 in the set of all even squarefree integers, so to ask in a meaningful way how often (1) is solvable, one has to restrict attention to a very thin subset of squarefree integers. Despite these and other challenges, in 1993, Stevenhagen [18] managed to formulate a precise conjecture as to what the answer should be and backed it up with both a convincing heuristic argument and carefully collected numerical data. About a decade ago, Fouvry and Klüners [4, 5] actually proved first cases of Stevenhagen's conjecture.

Consider now a negative Pell equation of a very particular shape, namely the equation

$$x^2 - 2py^2 = -1, \tag{2}$$

where p is an odd prime number. In this case, the 2-part of the narrow class group Cl_{2p}^{+} is *cyclic*, so it becomes somewhat easier to analyze whether or not $\mathrm{Cl}_{2p}^{+} = \mathrm{Cl}_{2p}$. Stevenhagen's conjecture for negative Pell equations of this shape states that if

$$\delta(X) = \frac{\#\{p \text{ prime}, p \leq X, (2) \text{ is solvable over } \mathbb{Z}\}}{\#\{p \text{ prime}, p \leq X\}},$$

then the limit $\lim_{X\to\infty} \delta(X)$ exists and is equal to $\frac{1}{3}$. It was already known to Stevenhagen in 1993 that

$$\frac{5}{16} \leq \liminf_{X\to\infty} \delta(X) \leq \limsup_{X\to\infty} \delta(X) \leq \frac{3}{8}.$$

While these are still the best known unconditional bounds, Koymans and the author [10] recently improved the upper bound to $\frac{11}{32}$ conditional on a standard technical conjecture in analytic number theory, and a forthcoming work of the author will improve the lower bound to $\frac{21}{64}$. The path to these results passes through class groups of certain *imaginary* quadratic number fields. The connection between Cl_{2p}^{+} and class groups Cl_{-p} and Cl_{-2p} of the quadratic number rings $\mathbb{Z}[\sqrt{-p}]$ and $\mathbb{Z}[\sqrt{-2p}]$, respectively, has been known for quite some time [12,17]. In this article, we will focus on the class group Cl_{-2p} for primes $p \equiv 3 \bmod 4$. Although information about these class groups has no direct bearing on the negative Pell equation (2), the method first developed to study these class groups [15] has since been applied in several settings, including in the aforementioned work [10].

The main theorem and basic strategy

The 2-part of the class group Cl_{-2p} is also cyclic, i.e., of the form $\mathbb{Z}/2^k\mathbb{Z}$ for some positive integer k, and so the 2-part of Cl_{-2p} is entirely determined by the highest power of 2 dividing the size of Cl_{-2p}, called the *class number* and denoted by h_{-2p}. In practice, to get better and better bounds for the solvability of (2), one has to obtain results about the natural density of primes for which higher and higher powers of 2 divide the size of Cl_{-2p}. Again, although it has no applications to the solvability of (2), one can study these questions for the groups Cl_{-2p} for primes $p \equiv 3 \bmod 4$ (and it turns out that methods developed in this setting were later applicable to (2)). The best previous result was due to Hasse in 1969 [7], who proved that

$$\lim_{X\to\infty} \frac{\#\{p \text{ prime}, p \leq X, p \equiv 3 \bmod 4, 8 \text{ divides } h_{-2p}\}}{\#\{p \text{ prime}, p \leq X\}} = \frac{1}{8}.$$

One can view the method of proof in this case as a special case of a method developed by Stevenhagen [16], where one constructs an auxiliary number field M, called a *governing field*, where the divisibility by 8 of the size of Cl_{-2p} is related to how the principal ideal generated by p factors into ideals in the ring of integers of M. In this case, one can take

$$M = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}}).$$

Once a governing field is constructed, one can apply the Chebotarev Density Theorem, which counts the natural density of primes p giving rise to a specified factorization type. Subsequent progress came to a halt as no one could construct any analogous governing fields for divisibility by 16. Far from constructing a governing field, [15] took an entirely different approach. The novelty was to apply a sieving technique originally due to Vinogradov [20] and subsequently improved by Vaughan [19] and Friedlander, Iwaniec, Mazur and Rubin [6], among others. This sieving technique, which we call here the *method of sums of type I and type II*, produces qualitatively different results from the Chebotarev Density Theorem, and its successful application to the aforementioned problems about class groups already suggests a drastic change in behavior between divisibility by 8 and divisibility by 16.

The main theorem is as follows. The condition that 8 divides the size of Cl_{-2p} for a prime $p \equiv 3 \bmod 4$ turns out simply to be that $p \equiv 15 \bmod 16$. One can write such a prime as

$$p = u^2 - 2v^2 \text{ with } u, v > 0 \text{ and } u \equiv 1 \bmod 16. \tag{3}$$

Leonard and Williams [13] then proved in 1982 that

$$16 \text{ divides } h_{-2p} \Leftrightarrow \text{the Jacobi symbol } \left(\frac{v}{u}\right) \text{ is equal to } 1. \tag{4}$$

The Jacobi symbol is an extension of the *Legendre symbol*; in this case, it can take the values 1 and -1, and, if u were a prime itself, the symbol $(\frac{v}{u})$ would equal 1 if and only if there existed an integer n with $v \equiv n^2 \bmod u$. The main theorem of [15] is the following.

Theorem 1. *For each prime $p \equiv 15 \bmod 16$, choose rational integers u and v as in* (3). *Then there exists an absolute constant $C > 0$ such that for every real number $X > 1$, we have*

$$\left| \sum_{\substack{p \leq X,\ p \text{ prime} \\ p \equiv 15 \bmod 16}} \left(\frac{v}{u}\right) \right| \leq CX^{\frac{199}{200}}.$$

Since the number of primes $p \equiv 15 \bmod 16$ up to X is approximately $\frac{1}{8}\frac{X}{\log X}$, and since

$$\lim_{X\to\infty} \frac{CX^{\frac{199}{200}}}{\frac{1}{8}\frac{X}{\log X}} = 0,$$

colloquially the theorem says that the Jacobi symbol $(\frac{v}{u})$ is equally often 1 and -1 as one traverses the primes $p \equiv 15 \bmod 16$, which in turn implies that

$$\lim_{X\to\infty} \frac{\#\{p \text{ prime}, p \leq X, p \equiv 3 \bmod 4, 16 \text{ divides } h_{-2p}\}}{\#\{p \text{ prime}, p \leq X\}} = \frac{1}{16}.$$

The new qualitative behavior that we mentioned above is exemplified by the power-saving bound in Theorem 1 — the savings of $X^{\frac{1}{100}}/\log X$ is substantially larger than the savings of $\log X$ that one would get from the Chebotarev Density Theorem.

The proof of Theorem 1 proceeds by applying the methods of sums of type I and type II not over the usual integers $\mathbb{Z}$, as is the case in most applications in the literature, but over the quadratic ring $\mathbb{Z}[\sqrt{2}]$. In this setting, the method relies in an essential way on the construction of a (well-behaved) sequence $\{s_{\mathfrak{a}}\}_{\mathfrak{a}}$ indexed by non-zero *ideals* of $\mathbb{Z}[\sqrt{2}]$ such that

$$s_{\mathfrak{p}} = \left(\frac{v}{u}\right) \tag{5}$$

when $\mathfrak{p}$ is the principal prime ideal generated by $u+v\sqrt{2}$ or $u-v\sqrt{2}$ with u and v as in (3). One immediate reason that this may be a challenging task is that the choice of u and v in (3) is not unique — the reader can check that one gets another valid choice for u and v by multiplying $u+v\sqrt{2}$ by $577+408\sqrt{2}$.

Some ideas of the proof

Class groups of quadratic number rings were first studied by Gauss, albeit in the language of binary quadratic forms. Although this language has largely fallen out of fashion in favor of the modern notions of number rings and ideals, we will nevertheless present several key ideas used in the proof of Theorem 1 in the setting of binary quadratic forms, both because these ideas can thus be expressed in an elementary way and because it is in this setting that these ideas were first discovered.

A *binary quadratic form over* $\mathbb{Z}$ is a homogeneous quadratic polynomial with integer coefficients; in other words, it is a polynomial of the type

$$f(x,y) = ax^2+bxy+cy^2, \quad a,b,c \in \mathbb{Z}. \tag{6}$$

We sometimes call $f(x,y)$ a *form* for short. The form f is said to be *primitive* if $\gcd(a,b,c)=1$. The *discriminant* of f is the integer $\Delta = b^2-4ac$. The set of all binary quadratic forms over $\mathbb{Z}$, which we denote by $V_{\mathbb{Z}}$, is in one-to-one correspondence with the set of ordered triples of integers; in fact, we will sometimes use the shorthand (a,b,c) to denote the form in (6).

The set $V_{\mathbb{Z}}$ is acted on by the group $\mathrm{SL}_2(\mathbb{Z})$ of 2-by-2 matrices of determinant 1 with integer entries. This action is essentially tantamount to a linear change of coordinates. To be precise, if

$$\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

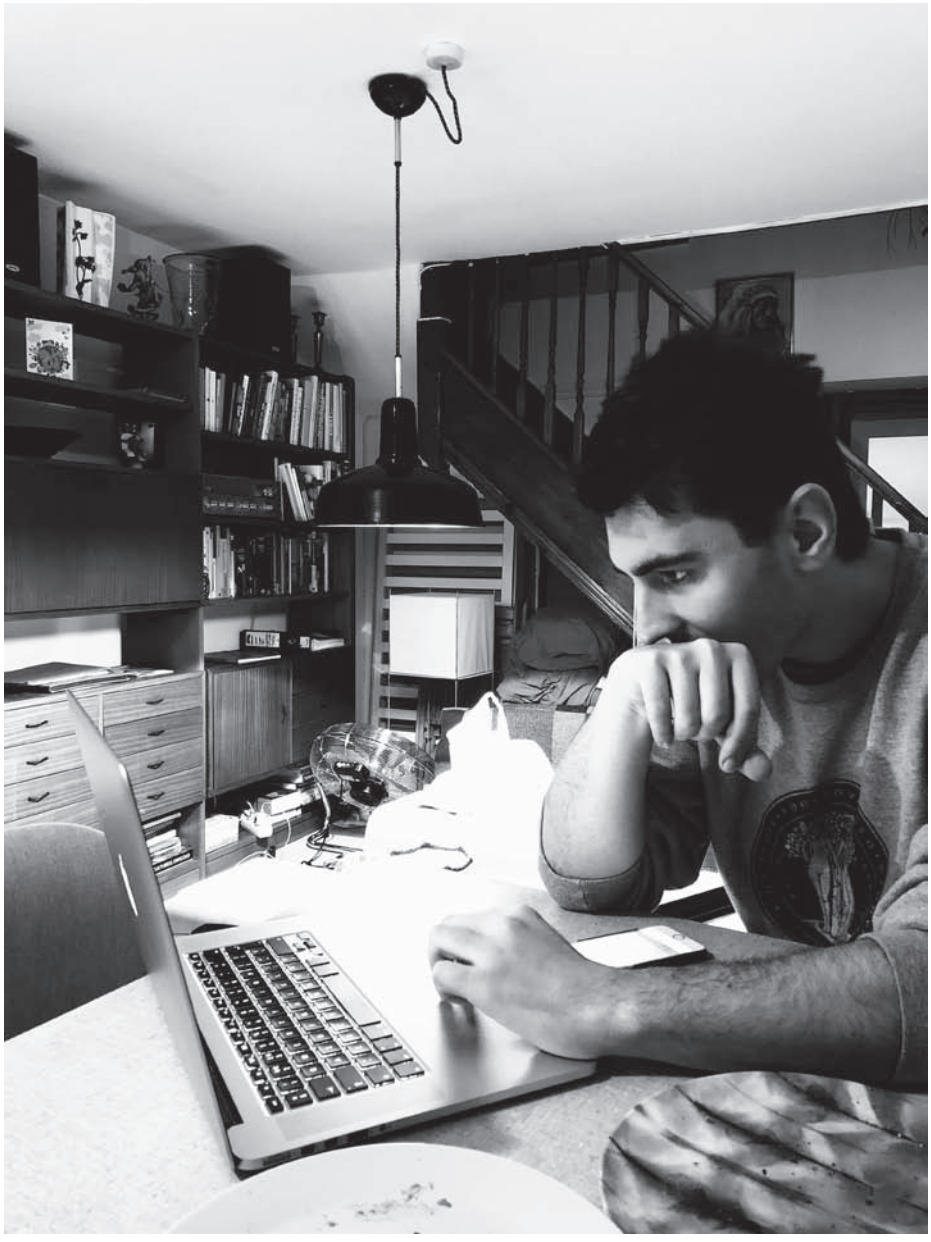
then we define the right action of γ on a form $f(x,y)=ax^2+bxy+cy^2$ by setting

$$\begin{aligned} f^{\gamma}(x,y) = {} & a(rx+sy)^2 \\ & + b(rx+sy)(tx+uy) \\ & + c(tx+uy)^2. \end{aligned}$$

Two forms (a,b,c) and (a',b',c') are said to be *equivalent* if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \cdot (a,b,c) = (a',b',c')$. We write $[a,b,c]$ for the equivalence class of the form (a,b,c); hence

$$\begin{aligned} [a,b,c] = [& ar^2+brt+ct^2, \\ & 2ars+bru+bst+2ctu, \\ & as^2+bsu+cu^2] \end{aligned}$$

whenever r, s, t, and u are integers satisfying $ru-st=1$. Equivalent forms always have the same discriminant. We denote set of equivalence classes of primitive forms of a non-square discriminant Δ by $\mathrm{Cl}(\Delta)$. Gauss proved that the set $\mathrm{Cl}(\Delta)$ is actually an abelian group — in other words, there is a commutative composition law on the set of classes of forms of discriminant Δ. For a beautiful modern proof of this fact, we encourage the reader to read about Bhargava's cubes of integers [1]. The class group of interest Cl_{-2p} is isomorphic to the



Djordjo Milovic

group $\mathrm{Cl}(-8p)$ corresponding to discriminant $-8p$.

Since $\mathrm{Cl}(\Delta)$ is an abelian group, we will denote the group operation induced by the composition law by $+$. In other words, if A and B are two classes of discriminant Δ, we will denote their composition simply by $A+B$; similarly, given an integer $n \geq 1$, we will write nA to denote the composition of A by itself n times. The identity element in $\mathrm{Cl}(\Delta)$, which we denote by I, is

$$I = \begin{cases} [1,0,-\Delta/4] & \text{if } \Delta \equiv 0 \bmod 4, \\ [1,1,(1-\Delta)/4] & \text{if } \Delta \equiv 1 \bmod 4, \end{cases}$$

and the inverse of the class $[a,b,c]$ is $[a,-b,c]$, so that

$$[a,b,c] + [a,-b,c] = I.$$

Dirichlet gave a simple formula for the composition law for forms of a certain type: if $a_1, a_2, b, c \in \mathbb{Z}$, then

$$[a_1,b,a_2c] + [a_2,b,a_1c] = [a_1a_2,b,c].$$

Leonard and Williams [13] made use of this formula for certain forms of discriminant $\Delta = -8p$, where p is a prime number congruent to 15 modulo 16. If p is such a prime and u and v are as in (3), we set $A = [u,4v,2u]$. Then the discriminant of A is indeed $16v^2 - 8u^2 = -8p$. Dirichlet's composition law implies that $2A = A + A = [u^2,4v,2]$. Acting on the form $(u^2,4v,2)$ by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

we see that $2A = [u^2,4v,2] = [2,0,p]$. Now, since $0 = -0$, we see that $4A = 2A + 2A = I$. After checking that $A \neq I$, one deduces that A is an element of order 4 in $\mathrm{Cl}(-8p) \cong \mathrm{Cl}_{-2p}$. This is significant because the machinery to check that a class is a 4th power is well-developed (see for instance [17]), while checking if a class is an 8th power is generally out of reach (see [14] for one place where it can be done). By checking if an element of order 4 is a 4th power, one can check for the existence of elements of order 16 and thereby obtain the crucial criterion (4).

We finish by presenting the other key application of the theory of binary quadratic forms in the proof of Theorem 1. As we mentioned before, a significant obstacle to using the method of sums of type I and type II is to construct an appropriate sequence $\{s_{\mathfrak{a}}\}_{\mathfrak{a}}$. For the method to work well, this needs to be done for *all* non-zero ideals in $\mathbb{Z}[\sqrt{2}]$ and not just for prime ideals $\mathfrak{p}$ as in (5). First, we say that an element $m + n\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$ is *odd and totally positive* if and only if

$$m \text{ is odd, } m > 0 \text{ and } m^2 - 2n^2 > 0. \quad (7)$$

So suppose that $\mathfrak{a}$ is a principal ideal of $\mathbb{Z}[\sqrt{2}]$ that has an odd and totally positive generator $u + v\sqrt{2}$. To obtain the desired property (5), we wish to define $s_{\mathfrak{a}} = \left(\frac{v}{u}\right)$ (possibly up to some well-controlled factors). However, as $(3+2\sqrt{2})(3-2\sqrt{2}) = 1$, the elements $u + v\sqrt{2}$ and

$$\begin{aligned}&(u+v\sqrt{2})(3+2\sqrt{2}) \\ &\quad = (3u+4v) + (2u+3v)\sqrt{2}\end{aligned}$$

both generate the same principal ideal in $\mathbb{Z}[\sqrt{2}]$. Moreover, if $u + v\sqrt{2}$ is odd and totally positive, then so is $(3u+4v) + (2u+3v)\sqrt{2}$. However, it is *not* always true that the corresponding Jacobi symbols $\left(\frac{v}{u}\right)$ and $\left(\frac{2u+3v}{3u+4v}\right)$ are equal. Hence, as stated, the value of $s_{\mathfrak{a}}$ is *not* well-defined! To overcome this, we proved the following result [15, Proposition 2, p. 979]. For an odd and totally positive element $\alpha = m + n\sqrt{2}$ of $\mathbb{Z}[\sqrt{2}]$, we define $[\alpha]$ to be the Jacobi symbol $\left(\frac{n}{m}\right)$.

Theorem 2. *Suppose $u + v\sqrt{2}$ is an odd and totally positive element of $\mathbb{Z}[\sqrt{2}]$. Then $[u+v\sqrt{2}] = [(u+v\sqrt{2})(3+2\sqrt{2})^4]$. In other words,*

$$\left(\frac{v}{u}\right) = \left(\frac{408u+577v}{577u+816v}\right).$$

The proof of Theorem 2 was initially discovered using a surprising identity involving binary quadratic forms. The Jacobi symbols are first interpreted as Artin symbols via class field theory, and the claim in the theorem is ultimately reduced to the claim that, if

$$\begin{aligned}u' + v'\sqrt{2} &= (577u+816v) \\ &\quad + (408u+577v)\sqrt{2} \\ &= (u+v\sqrt{2})(3+2\sqrt{2})^4,\end{aligned}$$

then $[u,16v,32u] = [u',16v',32u']$. This last claim follows immediately upon noticing that the matrix

$$\begin{pmatrix} 17 & 96 \\ 3 & 17 \end{pmatrix}$$

transforms the form $(u,16v,32u)$ into the form $(u',16v',32u')$. The upshot of Theorem 2 is that if $\mathfrak{a}$ is a principal ideal of $\mathbb{Z}[\sqrt{2}]$ that has an odd and totally positive generator α, then the quantity

$$\begin{aligned}&[\alpha] + [\alpha(3+2\sqrt{2})^1] \\ &\quad + [\alpha(3+2\sqrt{2})^2] \\ &\quad + [\alpha(3+2\sqrt{2})^3]\end{aligned}$$

depends only on $\mathfrak{a}$ and *not* on the choice of odd and totally positive generator α. After attaching proper weights to the four summands above, one obtains a well-defined sequence $s_{\mathfrak{a}}$ satisfying the property (5) and conducive to the method of sums of type I and type II [15, (3.5), p. 993].

Concluding remarks

The method used in Theorem 1 has since been used by Koymans and the author to prove analogous theorems for the class groups Cl_{-2p} with $p \equiv 1 \bmod 4$ as well as for the class groups Cl_{-p} [9, 10]. The latter result relies on a conjecture about short character sums, although Koymans recently published an unconditional proof [8]. Under a similar short character sum conjecture, however, one can prove much more — a governing field for divisibility by 16 of h_{-p} *does not exist* [11]. This confirms the suspicions first brought up in [15] that a genuinely new type of behavior enters into play when studying class group elements of order 16.

Biography

- Research Associate, 2017 onward, University College London.
- Member, 2016–2017, Institute for Advanced Study (Princeton).
- PhD in Mathematics (cum laude), 2013–2016, Universiteit Leiden and Université Paris-Sud (Orsay).
- MA in Mathematics (cum laude), 2011–2013, Université Paris-Sud (Orsay) and Università degli Studi di Milano.
- BA in Mathematics (cum laude), 2007–2011, Princeton University.

References

1 M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Ann. of Math.* 159(1) (2004), 217–250.

2 H. Cohn and J.C. Lagarias, On the existence of fields governing the 2-invariants of the classgroup of $\mathbb{Q}(\sqrt{dp})$ as p varies, *Math. Comp.* 41(164) (1983), 711–730.

3 H. Cohn and J.C. 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? *Colloq. Math. Soc. János Bolyai* 34 (1984), 257–280.

4 E. Fouvry and J. Klüners, On the negative Pell equation, *Ann. of Math. (2)* 172(3) (2010), 2035–2104.

5 E. Fouvry and J. Klüners, The parity of the period of the continued fraction of $\sqrt{d}$, *Proc. Lond. Math. Soc. (3)* 101(2) (2010), 337–391.

6 J.B. Friedlander, H. Iwaniec, B. Mazur and K. Rubin, The spin of prime ideals, *Invent. Math.* 193(3) (2013), 697–749.

7 H. Hasse, Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, *J. Number Theory* 1 (1969), 231–234.

8 P. Koymans, The 16-rank of $\mathbb{Q}(\sqrt{-p})$, arXiv: 1809.07167, 2018.

9 P. Koymans and D. Milovic, On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$, *Int. Math. Res. Notices* rny010 (2018), 1–22.

10 P. Koymans and D. Milovic, Spins of prime ideals and the negative Pell equation $x^2 - 2py^2 = -1$, arXiv:1611.10337, 2018.

11 P. Koymans and D. Milovic, Joint distribution of spins, arXiv:1809.09597, 2018.

12 P. Kaplan and K.S. Williams, On the strict class number of $\mathbb{Q}(\sqrt{2p})$ modulo 16, $p \equiv 1 \pmod 8$ prime, *Osaka J. Math.* 21 (1984), 23–29.

13 P.A. Leonard and K.S. Williams, On the divisibility of the class numbers of $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-2p})$ by 16, *Canad. Math. Bull.* 25(2) (1982), 200–206.

14 D. Milovic, On the infinitude of $\mathbb{Q}(\sqrt{-p})$ with class number divisible by 16, *Acta Arith.* 178(3) (2017), 201–233.

15 D. Milovic, On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \bmod 4$, *Geom. Func. Anal.* 27(4) (2017), 973–1016.

16 P. Stevenhagen, Ray class groups and governing fields, in *Théorie des nombres, Année 1988/89, Fasc. 1*, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1989, p. 93.

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

18 P. Stevenhagen. The number of real quadratic fields having units of negative norm, *Experiment. Math.* 2(2) (1993), 121–136.

19 R.C. Vaughan, Mean Value Theorems in Prime Number Theory, *J. London Math. Soc. (2)* 10 (1975), 153–162.

20 I.M. Vinogradov, The method of trigonometrical sums in the theory of numbers, *Trav. Inst. Math. Stekloff* 23 (1947), 3–109.