Class Number Theory

Steven Finch

May 26, 2005

The problem of representing an integer as a sum of squares, or more generally as the value of a quadratic form, is very old and challenging [1, 2, 3, 4, 5, 6, 7]. We will barely scratch the surface of this enormous literature.

0.1. Form Class Group. A binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$ is **primitive** if a, b, c are relatively prime and has **discriminant** $\delta_f = b^2 - 4ac$. The form f is **positive definite** if the matrix

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

is positive definite (meaning $a > 0$ and $\delta_f < 0$) and **indefinite** if $\delta_f > 0$. An integer d is a discriminant δ_f for some form f if and only if $d \equiv 0, 1 \bmod 4$. A discriminant $D \neq 0, 1$ is a **fundamental discriminant** assuming that

$$D = \begin{cases} m & \text{if } m \equiv 1 \bmod 4, \\ 4m & \text{if } m \equiv 2, 3 \bmod 4 \end{cases}$$

for some square-free integer m. Every nonsquare discriminant d can be uniquely expressed as De^2 where D is a fundamental discriminant and $e \geq 1$. A partial listing of fundamental discriminants appears in Table 1 and the correspondence $m \leftrightarrow D$ will be needed later [8].

Table 1 *Interplay between m and D*, $-163 \leq D \leq 136$

m	-3	-1	-7	-2	-11	-15	-19	-5	-23	-6	-31	-35	$\ldots$	-163
D	-3	-4	-7	-8	-11	-15	-19	-20	-23	-24	-31	-35	$\ldots$	-163
m	5	2	3	13	17	21	6	7	29	33	37	10	$\ldots$	34
D	5	8	12	13	17	21	24	28	29	33	37	40	$\ldots$	136

Assume that D is a fundamental discriminant. Two quadratic forms f, g with $\delta_f = D = \delta_g$ are **properly equivalent** if there is a linear change of variables

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \qquad ru - st = 1, \qquad r, s, t, u \in \mathbb{Z}$$

for which $f(x,y) = g(x',y')$ always. We say that f, g are in the same **form class** and define the **form class number**

$$h^+(D) = \begin{cases} \text{the number of classes of primitive positive} \\ \text{definite forms of discriminant } D & \text{if } D < 0, \\ \text{the number of classes of primitive} \\ \text{indefinite forms of discriminant } D & \text{if } D > 0. \end{cases}$$

For example, $h^+(-4) = 1$ and $x^2 + y^2$ is a representative element of the unique form class of discriminant -4; $h^+(-20) = 2$ and x^2+5y^2, $2x^2+2xy+3y^2$ are representative elements of the two corresponding classes of discriminant -20.

It is possible to endow the set of form classes, for fixed D, with the structure of an abelian group. We simply illustrate in the case $D = -4$:

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = x_3^2 + y_3^2$$

where

$$x_3 = x_1x_2 - y_1y_2, \qquad y_3 = x_1y_2 + y_1x_2;$$

and in the case $D = -20$:

$$(x_1^2 + 5y_1^2)(x_2^2 + 5y_2^2) = x_4^2 + 5y_4^2,$$

$$(x_1^2 + 5y_1^2)(2x_2^2 + 2x_2y_2 + 3y_2^2) = 2x_5^2 + 2x_5y_5 + 3y_5^2,$$
$$(2x_1^2 + 2x_1y_1 + 3y_1^2)(2x_2^2 + 2x_2y_2 + 3y_2^2) = x_6^2 + 5y_6^2$$

where

$$x_4 = x_1x_2 - 5y_1y_2, \qquad y_4 = x_1y_2 + y_1x_2,$$

$$x_5 = x_1x_2 - y_1x_2 - 3y_1y_2, \qquad y_5 = x_1y_2 + 2y_1x_2 + y_1y_2,$$

$$x_6 = 2x_1x_2 + x_1y_2 + y_1x_2 - 2y_1y_2, \qquad y_6 = x_1y_2 + y_1x_2 + y_1y_2.$$

This multiplication is called **Gaussian composition** and is perhaps best understood via the following section.

We discuss two variations of the preceding. If the determinant of the linear transformation $(x,y) \mapsto (x',y')$ is allowed to be $ru - st = \pm 1$, then the corresponding number of equivalence classes is [9]

$$\hat{h}(D) = \frac{1}{2}\left(h^+(D) + 2^{\omega(D)-1}\right)$$

where $\omega(n)$ denotes the number of distinct prime factors of $|n|$. Rephrasing, $h^+(D)$ is the number of orbits under the action of the matrix group $\mathrm{SL}_2(\mathbb{Z})$ on the primitive binary quadratic forms of discriminant D, while $\hat{h}(D)$ is the same under the action of $\mathrm{GL}_2(\mathbb{Z})$. For instance, $h^+(-23) = 3 > 2 = \hat{h}(-23)$ and $h^+(136) = 4 > 3 = \hat{h}(136)$.

The second variation seems quite artificial but is actually important. Two quadratic forms f, g with $\delta_f = D = \delta_g$ are **vulgarly equivalent** if there is a linear change of variables

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \qquad ru - st = \theta = \pm 1, \qquad r, s, t, u \in \mathbb{Z}$$

for which $f(x, y) = \theta\, g(x', y')$ always. Note the factor θ in front of g. Define $h(D)$ to be the number of vulgar equivalence classes of primitive quadratic forms of discriminant D. Note here that forms are not assumed to be positive definite for $D < 0$. As an example, $h^+(12) = 2 > 1 = h(12)$ since the forms $-3x^2 + y^2$ and $-x^2 + 3y^2$ are not properly equivalent, but are vulgarly equivalent via the assignment $(x', y') = (y, x)$.

0.2. Ideal Class Group. Let $m \neq 0, 1$ be a square-free integer. The **quadratic number field**

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q} + \mathbb{Q}\sqrt{m} = \left\{u + v\sqrt{m} : u, v \in \mathbb{Q}\right\}$$

is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{m}$. An element $\alpha \in \mathbb{Q}(\sqrt{m})$ is an **algebraic integer** if it is a zero of a monic polynomial $z^2 + bz + c$ with $b, c \in \mathbb{Z}$. The set of algebraic integers of $\mathbb{Q}(\sqrt{m})$ is the subring

$$\mathcal{O}_m = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m} & \text{if } m \equiv 2, 3 \bmod 4, \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \bmod 4 \end{cases}$$

of $\mathbb{Q}(\sqrt{m})$, often called the **maximal order** or simply the **integers**. Using the correspondence between the **radicand** m and the fundamental discriminant D, we have

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{D}), \qquad \mathcal{O}_m = \mathbb{Z} + \mathbb{Z}\frac{D+\sqrt{D}}{2}.$$

For example, $\mathcal{O}_{-1}$ is the ring of Gaussian integers. In $\mathcal{O}_{-5}$, we have a surprising failure of unique factorization:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

More will be said about this momentarily.

An **ideal** I of $\mathcal{O}_m$ is an additive subgroup of $\mathcal{O}_m$ with the property that, if $\alpha \in I$ and $\rho \in \mathcal{O}_m$, then $\rho\alpha \in I$. The set

$$(\alpha) = \{\rho\alpha : \rho \in \mathcal{O}_m\}$$

is the ideal of all multiples of a single element $\alpha \in \mathcal{O}_m$ and is called a **principal ideal**. The ideal

$$(\alpha_1, \alpha_2) = \{\rho_1\alpha_1 + \rho_2\alpha_2 : \rho_1, \rho_2 \in \mathcal{O}_m\}$$

is **nonprincipal** if $(\alpha_1, \alpha_2) \neq (\alpha_3)$ for any $\alpha_3 \in \mathcal{O}_m$. The **product** IJ of two ideals is the ideal of all finite sums of products of the form $\alpha\beta$ with $\alpha \in I$ and $\beta \in J$. In $\mathcal{O}_{-5}$, the principal ideal (6) can be written as

$$\begin{aligned}(6) &= (2)(3) = I_1^2 I_2 I_3 \\ &= \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) = I_1 I_2 I_1 I_3\end{aligned}$$

where

$$I_1 = \left(2, 1+\sqrt{-5}\right) = \left(2, 1-\sqrt{-5}\right),$$
$$I_2 = \left(3, 1+\sqrt{-5}\right), \qquad I_3 = \left(3, 1-\sqrt{-5}\right).$$

Thus the two distinct factorizations of the number 6 in $\mathcal{O}_{-5}$ come from permuting I_1, I_2, I_3 in the factorization of the ideal (6).

Given $\alpha = u + v\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, define its **conjugate** $\bar{\alpha} = u - v\sqrt{m}$ and its **norm** $N(\alpha) = \alpha\bar{\alpha} = u^2 - mv^2$. If $\alpha \in \mathcal{O}_m$, then clearly $\bar{\alpha} \in \mathcal{O}_m$ and $N(\alpha) \in \mathbb{Z}$. Given an ideal I of $\mathcal{O}_m$, define its conjugate $\bar{I} = \{\bar{\alpha} : \alpha \in I\}$ and its norm $N(I) = \gcd\{N(\alpha) : \alpha \in I\}$. For example, if I is the principal ideal (α), then $\bar{I} = (\bar{\alpha})$ and $N(I) = |N(\alpha)|$. If I and J are two ideals, then $N(IJ) = N(I)N(J)$; also $I\bar{I} = (N(I))$ is principal.

Two ideals I, J of $\mathcal{O}_m$ are **strictly equivalent** if there exist $\alpha, \beta \in \mathcal{O}_m$ such that

$$(\alpha)I = (\beta)J, \qquad N(\alpha\beta) > 0.$$

We say that I, J are in the same **narrow ideal class** and define H_m^+ to be the finite abelian group of ideals modulo this relation. If the requirement that $N(\alpha\beta) > 0$ is removed, we instead say that I, J are in the same **wide ideal class** and define H_m analogously. H_m^+ is called the **narrow class group** and its cardinality h_m^+ is the **narrow class number**. The name for H_m is often abbreviated simply to **class group**. The **class number** h_m can be found in terms of h_m^+ via

$$h_m = \begin{cases} h_m^+ & \text{if } m < 0 \text{ or } (m > 0 \text{ and } N(\varepsilon) = -1), \\ \frac{1}{2}h_m^+ & \text{if } m > 0 \text{ and } N(\varepsilon) = 1 \end{cases}$$

where ε is the **fundamental unit** of $\mathcal{O}_m$ (to be defined in the next section). Group-theoretic properties of H_m and the efficient computation of h_m have attracted much attention in recent years.

It turns out that the abelian group of classes of primitive binary quadratic forms of discriminant D is isomorphic to the narrow class group H_m^+, where the interplay $m \leftrightarrow D$ was described earlier. In particular, Gaussian composition of forms can be elegantly written using ideals and $h^+(D) = h_m^+$; see Tables 2 and 3 [10]. By the same reasoning, we have $h(D) = h_m$ but no interpretation of $\hat{h}(D)$ in ideal class theory seems to be useful. Our convention for treating the discriminant D as an argument and the radicand m as a subscript is perhaps new.

Table 2 *Class Numbers as Functions of* m, $-163 \le m \le 34$

m	-1	-2	-3	-5	-6	-7	-10	-11	-13	-14	-15	-17	$\dots$	-163
h_m	1	1	1	2	2	1	2	1	2	4	2	4	$\dots$	1
$\hat{h}_m$	1	1	1	2	2	1	2	1	2	3	2	3	$\dots$	1
m	2	3	5	6	7	10	11	13	14	15	17	19	$\dots$	34
h_m^+	1	2	1	2	2	2	2	1	2	4	1	2	$\dots$	4
h_m	1	1	1	1	1	2	1	1	1	2	1	1	$\dots$	2
$\hat{h}_m$	1	2	1	2	2	2	2	1	2	4	1	2	$\dots$	3

Table 3 *Class Numbers as Functions of* D, $-163 \le D \le 136$

D	-3	-4	-7	-8	-11	-15	-19	-20	-23	-24	-31	-35	$\dots$	-163
$h(D)$	1	1	1	1	1	2	1	2	3	2	3	2	$\dots$	1
$\hat{h}(D)$	1	1	1	1	1	2	1	2	2	2	2	2	$\dots$	1
D	5	8	12	13	17	21	24	28	29	33	37	40	$\dots$	136
$h^+(D)$	1	1	2	1	1	2	2	2	1	2	1	2	$\dots$	4
$h(D)$	1	1	1	1	1	1	1	1	1	1	1	2	$\dots$	2
$\hat{h}(D)$	1	1	2	1	1	2	2	2	1	2	1	2	$\dots$	3

A maximal order $\mathcal{O}_m$ is a UFD (unique factorization domain) if and only if it is a PID (principal ideal domain), which is true if and only if $h_m = 1$. Also, $h_m \le 2$ if and only if any two decompositions of $\alpha \in \mathcal{O}_m$ into products of irreducible elements must possess the same number of factors [11, 12, 13, 14]. Hence the class number measures, in a vague sense, how far $\mathcal{O}_m$ is from being a UFD.

0.3. Fundamental Unit. Let $m > 1$ be square-free. A **unit** $\varepsilon \in \mathcal{O}_m$ satisfies $N(\varepsilon) = \pm 1$; it is the **fundamental unit** if $\varepsilon > 1$ and every other unit is of the form $\pm\varepsilon^n$, $n \in \mathbb{Z}$. Here is a conceptually simple algorithm for computing ε. If $m \equiv 2, 3 \bmod 4$, calculate mb^2 for $b = 1, 2, 3, \dots$ and stop at the first integer mb_0^2 that differs from a square a_0^2 by exactly ± 1; then $\varepsilon = a_0 + b_0\sqrt{m}$. If $m \equiv 1 \bmod 4$, stop instead at the first integer mb_0^2 that differs from a square a_0^2 by exactly ± 4; then $\varepsilon = (a_0 + b_0\sqrt{m})/2$. In both cases, we assume that $a_0 \ge 1$.

Two alternative algorithms involve continued fractions [15, 16]. For the first, define

$$\mu = \begin{cases} \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \bmod 4, \\ \sqrt{m} & \text{if } m \equiv 2, 3 \bmod 4 \end{cases} = \frac{P_0 + \sqrt{m}}{Q_0}$$

and let the (eventually periodic) continued fraction expansion of μ be

$$\mu = c_0 + \frac{1|}{|c_1} + \frac{1|}{|c_2} + \frac{1|}{|c_3} + \cdots .$$

Define

$$P_{j+1} = c_j Q_j - P_j, \qquad Q_{j+1} = \frac{m - P_{j+1}^2}{Q_j}$$

for $j \geq 0$, so that

$$\frac{P_j + \sqrt{m}}{Q_j} = c_j + \frac{1|}{|c_{j+1}} + \frac{1|}{|c_{j+2}} + \frac{1|}{|c_{j+3}} + \cdots$$

and hence

$$\varepsilon = \prod_{j=1}^{\lambda} \frac{P_j + \sqrt{m}}{Q_j}$$

where λ is the period length of the continued fraction expansion for μ.

The second possesses a curiously ambiguous outcome. Let

$$\sqrt{m} = d_0 + \frac{1|}{|d_1} + \frac{1|}{|d_2} + \frac{1|}{|d_3} + \cdots$$

and define

$$A_0 = d_0, \qquad A_1 = d_0 d_1 + 1, \qquad B_0 = 1, \qquad B_1 = d_1,$$
$$A_k = d_k A_{k-1} + A_{k-2}, \qquad B_k = d_k B_{k-1} + B_{k-2},$$

for $k \geq 2$, so that

$$\frac{A_k}{B_k} = d_0 + \frac{1|}{|d_1} + \frac{1|}{|d_2} + \cdots + \frac{1|}{|d_k} = \text{the } k^{\text{th}} \text{ convergent of } \sqrt{m}.$$

Let l denote the period length of the continued fraction expansion for $\sqrt{m}$. It can be proved that, if $m \not\equiv 5 \bmod 8$, then $\varepsilon = A_{l-1} + B_{l-1}\sqrt{m}$. If $m \equiv 5 \bmod 8$, however, all we can conclude is that $A_{l-1} + B_{l-1}\sqrt{m}$ is either ε or ε^3. See Tables 4 and 5 [17].

Table 4 *Fundamental Unit* ε *and Norm* $N(\varepsilon)$ *as Functions of* m, $2 \leq m \leq 17$

m	2	3	5	6	7	10	11	13	14	15	17
ε	$\frac{1+\sqrt{2}}{1}$	$\frac{2+\sqrt{3}}{1}$	$\frac{1+\sqrt{5}}{2}$	$\frac{5+2\sqrt{6}}{1}$	$\frac{8+3\sqrt{7}}{1}$	$\frac{3+\sqrt{10}}{1}$	$\frac{10+3\sqrt{11}}{1}$	$\frac{3+\sqrt{13}}{2}$	$\frac{15+4\sqrt{14}}{1}$	$\frac{4+\sqrt{15}}{1}$	$\frac{4+\sqrt{17}}{1}$
$N(\varepsilon)$	-1	$+1$	-1	$+1$	$+1$	-1	$+1$	-1	$+1$	$+1$	-1

Table 5 *Fundamental Unit* ε *and Norm* $N(\varepsilon)$ *as Functions of* D, $5 \le D \le 37$

D	5	8	12	13	17	21	24	28	29	33	37
ε	$\frac{1+\sqrt{5}}{2}$	$\frac{1+\sqrt{2}}{1}$	$\frac{2+\sqrt{3}}{1}$	$\frac{3+\sqrt{13}}{2}$	$\frac{4+\sqrt{17}}{1}$	$\frac{5+\sqrt{21}}{2}$	$\frac{5+2\sqrt{6}}{1}$	$\frac{8+3\sqrt{7}}{1}$	$\frac{5+\sqrt{29}}{2}$	$\frac{23+4\sqrt{33}}{1}$	$\frac{6+\sqrt{37}}{1}$
$N(\varepsilon)$	-1	-1	$+1$	-1	-1	$+1$	$+1$	$+1$	-1	$+1$	-1

A fast method to compute the set of square-free $m > 1$ for which $N(\varepsilon) = -1$ (equivalently, l is odd) is not known [18, 19, 20, 21, 22, 23]. Likewise, the set of $m \equiv 5 \bmod 8$ for which $A_{l-1} + B_{l-1}\sqrt{m} = \varepsilon^3$ remains only partially understood [24, 25, 26, 27, 28, 29, 30]. Since ε can be exponentially large in m, the **regulator** $\ln(\varepsilon)$ is often used instead [31]. Hallgren [32, 33] recently gave a polynomial-time algorithm for computing $\ln(\varepsilon)$ that is based on a quantum Fourier transform period finding technique.

Another formula is $\varepsilon = (x + y\sqrt{D})/2$, where x, y are the smallest positive integer solutions of the Pell equation $x^2 - Dy^2 = \pm 4$. It follows immediately that $N(\varepsilon) = -1$ if and only $x^2 - Dy^2 = -4$. Let us define $\varepsilon^+ = (z + w\sqrt{D})/2$, where z, w are the smallest positive integer solutions of $z^2 - Dw^2 = 4$. Clearly $h^+(D)\ln(\varepsilon^+) = 2h(D)\ln(\varepsilon)$ for all $D > 0$; we will need ε^+ later.

0.4. Ideal Statistics over D. The study of ideal class numbers as functions of fundamental discriminant D (equivalently, radicand m) has occupied mathematicians for centuries. Heegner [34], Stark [35, 36, 37], Baker [38], Deuring [39] and Siegel [40, 41] solved Gauss' class number one problem: $h(D) = 1$ for $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$ and for no other $D < -163$. See [42, 43, 44, 45, 46, 47, 48, 49, 50, 51] for related work in the imaginary case. With respect to the real case, Gauss conjectured that $h(D) = 1$ for infinitely many $D > 0$, but a proof remains unknown.

Siegel [52, 53, 54, 55, 56] showed that

$$\ln(h(D)) \sim \ln(\sqrt{-D}) \qquad \text{as } D \to -\infty,$$

$$\ln(h(D)\ln(\varepsilon)) \sim \ln(\sqrt{D}) \qquad \text{as } D \to \infty$$

and the following mean value results apply [57, 58, 59, 60]:

$$\sum_{0<-D<x} h(D) \sim \frac{c}{3\pi}x^{3/2}, \qquad \sum_{0<D<x} h(D)\ln(\varepsilon) \sim \frac{c}{6}x^{3/2}$$

as $x \to \infty$, where [61]

$$c = \prod_p \left(1 - \frac{1}{p^2(p+1)}\right) = 0.8815138397...$$

and the infinite product is over all primes p. We may alternatively write

$$\lim_{x\to\infty} \mathrm{E}\left(\frac{h(D)}{\sqrt{-D}}\,|\,0<-D<x\right)=\frac{\pi c}{6}=0.4615595671...$$

$$\lim_{x\to\infty} \mathrm{E}\left(\frac{h(D)\ln(\varepsilon)}{\sqrt{D}}\,|\,0<D<x\right)=\frac{\pi^2 c}{12}=0.7250160726...$$

because $\sum_{0<-D<x} 1 \sim (3/\pi^2)x \sim \sum_{0<D<x} 1$ and since partial summation contributes an additional factor of $3/2$.

Taniguchi [62] conjectured a second-order analog

$$\sum_{0<-D<x} h(D)^2 \sim \frac{\pi^2 c'}{144}x^2, \qquad \sum_{0<D<x} h(D)^2 \ln(\varepsilon)^2 \sim \frac{\pi^4 c'}{576}x^2$$

as $x\to\infty$, where [63]

$$c'=\prod_p\left(1-\frac{3}{p^3}+\frac{2}{p^4}+\frac{1}{p^5}-\frac{1}{p^6}\right)=0.6782344919....$$

With regard to extreme values, Granville & Soundararajan [64] suggested that perhaps

$$\max_{|D|<x} L(D)=e^{\gamma}(\ln\ln x+\ln\ln\ln x+c''+o(1))$$

where γ is Euler's constant,

$$L(D)=\begin{cases}\dfrac{\pi h(D)}{\sqrt{-D}} & \text{if } D<-4,\\ \dfrac{2h(D)\ln(\varepsilon)}{\sqrt{D}} & \text{if } D>4\end{cases}$$

and

$$c''=\int_0^1\frac{\tanh(y)}{y}dy+\int_1^\infty\frac{\tanh(y)-1}{y}dy=0.8187801401...$$

Is it possible in any of these formulas, when $D>0$, to somehow separate the class number and the regulator?

0.5. Cohen-Lenstra Heuristics. We merely state certain conjectures due to Cohen & Lenstra [65, 66, 67, 68, 69, 70]. Define $\tilde{H}_m$ to be the odd part of the class group H_m, that is, $\tilde{H}_m$ is the subgroup of all elements in H_m of odd order. Let [71, 72]

$$C=\prod_{j=2}^{\infty}\zeta(j)=2.2948565916...,$$

$$\Delta = \frac{\pi^2}{6}\prod_p\left(1+\frac{1}{p^2(p-1)}\right) = 2.2038565964...$$

and, when q is prime,

$$\eta(q) = \prod_{k=1}^{\infty}\left(1-\frac{1}{q^k}\right)$$

(which appeared in [73] for the special case $q = 2$). For random $m < 0$, it is believed that

- the probability that $\tilde{H}_m$ is cyclic is

$$\frac{\pi^2}{18}\frac{\zeta(3)}{\zeta(6)}\frac{1}{C\eta(2)} = 0.9775748102...$$

- if p is an odd prime, the probability that $p|h_m$ is

$$1-\eta(p) = \begin{cases} 0.4398739220... & \text{if } p=3, \\ 0.2396672041... & \text{if } p=5, \\ 0.1632045929... & \text{if } p=7 \end{cases}$$

and, likewise, for random $m > 0$,

- the probability that $\tilde{H}_m$ is cyclic is

$$\frac{3}{10}\frac{\Delta}{C\eta(2)} = 0.9976305717...$$

- if p is an odd prime, the probability that $p|h_m$ is

$$1-\left(1-\frac{1}{p}\right)^{-1}\eta(p) = \begin{cases} 0.1598108831... & \text{if } p=3, \\ 0.0495840051... & \text{if } p=5, \\ 0.0237386917... & \text{if } p=7 \end{cases}$$

- the probability that $h_m = 1$, given that m itself is prime, is

$$\frac{1}{2C\eta(2)} = 0.7544581722....$$

A proof of any of these conjectures would be a welcome breakthrough! See [74] for partial results concerning the prime $p = 3$.

0.6. Form Statistics over d. Given a nonsquare discriminant d, define $h^+(d)$ and $\varepsilon^+(d)$ exactly as before (with D simply replaced by d). We had no need of such generalizations until now. See Table 6 [75].

Table 6 *Class Number $h^+(d)$ for $-23 \leq d \leq 32$; also $\varepsilon^+(d)$ for $5 \leq d \leq 32$*

d	-3	-4	-7	-8	-11	-12	-15	-16	-19	-20	-23
$h^+(d)$	1	1	1	1	1	1	2	1	1	2	3
d	5	8	12	13	17	20	21	24	28	29	32
$h^+(d)$	1	1	2	1	1	1	2	2	2	1	2
$\varepsilon^+(d)$	$\frac{3+\sqrt{5}}{2}$	$\frac{3+2\sqrt{2}}{1}$	$\frac{2+\sqrt{3}}{1}$	$\frac{11+3\sqrt{13}}{2}$	$\frac{33+8\sqrt{17}}{1}$	$\frac{9+4\sqrt{5}}{1}$	$\frac{5+\sqrt{21}}{2}$	$\frac{5+2\sqrt{6}}{1}$	$\frac{8+3\sqrt{7}}{1}$	$\frac{27+5\sqrt{29}}{2}$	$\frac{3+2\sqrt{2}}{1}$

Lipschitz [76], Mertens [77] and Siegel [78] proved that

$$\sum_{0<-d<x} h^+(d) \sim \frac{\pi}{18\zeta(3)} x^{3/2}, \qquad \sum_{0<d<x} h^+(d)\ln(\varepsilon^+) \sim \frac{\pi^2}{18\zeta(3)} x^{3/2}$$

as $x \to \infty$, where the sums are taken over all $d \equiv 0, 1 \bmod 4$ that are not squares. Their efforts confirmed conjectures of Gauss [79, 80, 81, 82]:

$$\sum_{\substack{0<-d<4x, \\ 4|d}} h^+(d) \sim \frac{4\pi}{21\zeta(3)} x^{3/2}, \qquad \sum_{\substack{0<d<4x, \\ 4|d}} h^+(d)\ln(\varepsilon^+) \sim \frac{4\pi^2}{21\zeta(3)} x^{3/2}.$$

When searching through the literature, it is helpful to be aware of Gauss's convention (that $d = 4k$ or, equivalently, $f(x, y) = ax^2+2bxy+cy^2$) versus Eisenstein's convention (no parity requirement on the middle coefficient). We have adopted the latter, as do most contemporary authors. For example,

$$\lim_{x\to\infty} \mathrm{E}\left(\frac{h^+(d)}{\sqrt{-d}} \,|\, 0 < -d < 4x,\, d = 4k\right) = \frac{\pi}{7\zeta(3)} = 0.3733591557... = \frac{1.1729423808...}{\pi}$$

in Gauss' scheme and

$$\lim_{x\to\infty} \mathrm{E}\left(\frac{h^+(d)\ln(\varepsilon^+)}{\sqrt{d}} \,|\, 0 < d < x\right) = \frac{\pi^2}{6\zeta(3)} = 1.3684327776... = 2(0.6842163888...)$$

in Eisenstein's scheme. A second-moment analog of the latter is due to Barban [83, 84, 85, 86, 87, 88, 89]:

$$\begin{aligned} \lim_{x\to\infty} \mathrm{E}\left(\frac{h^+(d)^2\ln(\varepsilon^+)^2}{d} \,|\, 0 < d < x\right) &= \prod_p \left(1 + \frac{3p^2-1}{(p^2-1)p(p+1)}\right) \\ &= 2.5965362904.... = \frac{29}{18}(1.6116432147...) \end{aligned}$$

In fact, the probability distributions [90, 91, 92, 93, 94, 95]

$$\lim_{x\to\infty} \mathrm{P}\left\{\ln\left(\frac{h^+(d)\ln(\varepsilon^+)}{\sqrt{d}}\right) \le s \mid 0 < d < x\right\},$$

$$\lim_{x\to\infty} \mathrm{P}\left\{\ln\left(\frac{\pi h^+(d)}{\sqrt{-d}}\right) \le s \mid 0 < -d < x\right\}$$

both coincide with the distribution of $S = \sum_p X_p$, an infinite sum of independent random variables, where

$$X_p = \begin{cases} 0 & \text{with probability } \frac{1}{p}, \\ -\ln\left(1 - \frac{1}{p}\right) & \text{with probability } \frac{1}{2}\left(1 - \frac{1}{p}\right), \\ -\ln\left(1 + \frac{1}{p}\right) & \text{with probability } \frac{1}{2}\left(1 - \frac{1}{p}\right) \end{cases}$$

for each prime number p.

We mention finally Hooley's conjecture [96]

$$\sum_{\substack{0<d<4x, \\ 4|d}} h^+(d) \sim \frac{25}{12\pi^2} x \ln(x)^2$$

and wonder if this (and other attempts to separate the class number and the regulator when $d > 0$) someday can be verified.

0.7. Continued Fraction Period Length. Table 7 exhibits the period length l_m of the continued fraction expansion for $\sqrt{m}$, where $m > 1$ is square-free [97].

Table 7 *Period Length as a Function of* m, $2 \le m \le 31$

m	2	3	5	6	7	10	11	13	14	15	17	19	21	22	23	26	29	30	31
l_m	1	2	1	2	4	1	2	5	4	2	1	6	6	6	4	1	5	2	8

Very little can be said about the behavior of l_m. Podsypanin [98, 99] proved that

$$l_m = O\left(\sqrt{m}\ln(\ln(m))\right)$$

as $m \to \infty$, assuming the truth of the extended Riemann hypothesis. Williams [100, 101] gave evidence that the big O, on the one hand, can be replaced by

$$\frac{e^\gamma}{\ln(\varphi)} = 3.7012232975...$$

where φ is the Golden mean, or even

$$\frac{12e^{\gamma}\ln(2)}{\pi^2} = 1.5010271229....$$

It seems likely, on the other hand, that the values 1.05 or even 1.08 will *not* suffice. Pen & Skubenko [102] and Golubeva [103, 104] proved the inequality [105]

$$\frac{\ln(\varepsilon)}{\ln(4\sqrt{m})} < l_m < \frac{4\ln(\varepsilon)}{\ln(\varphi)} = 4(2.0780869212...)\ln(\varepsilon)$$

involving the fundamental unit ε of $\mathbb{Q}(\sqrt{m})$. This subject turns out to be related to what are called **Lévy constants** [106, 107, 108, 109]:

$$\beta(\xi) = \lim_{k\to\infty} \frac{\ln(B_k)}{k}$$

where A_k/B_k is the k^{th} convergent of the quadratic irrational ξ. Let Σ denote the set of all such $\beta(\xi)$. It is known that $\Sigma \subseteq [\ln(\varphi), \infty)$ and that $\pi^2/(12\ln(2))$ is a limit point of Σ. It is also likely that Σ has a structure similar to the Markov spectrum [110] in the sense that a left hand portion of Σ probably consists only of isolated points and a right hand portion of Σ is much denser.

Let $3 < p \equiv 3 \mod 4$ be prime and assume that $h_p = 1$. An astonishing formula due to Hirzebruch [111, 112, 113, 114] states that

$$h_{-p} = \frac{1}{3}\sum_{j=1}^{l}(-1)^{l-j}d_j$$

where d_1, d_2, $\ldots$, d_l is the sequence of denominators in one period of the continued fraction expansion for $\sqrt{p} - \lfloor\sqrt{p}\rfloor$. For example, $h_{23} = 1$ and $h_{-23} = (-1 + 3 - 1 + 8)/3 = 3$. Is an elementary proof of this theorem possible? What can be said if instead $p \equiv 1 \mod 4$?

As an aside, there exist precisely twenty-one square-free integers m for which the pair $(\mathcal{O}_m, |N|)$ is a Euclidean domain, that is, for which $|N|$ is compatible with the division algorithm [16, 115, 116, 117, 118]. Both $(\mathcal{O}_{14}, |N|)$ and $(\mathcal{O}_{69}, |N|)$ fail to be Euclidean, although $h_{14} = 1 = h_{69}$. An alternative function $N' : \mathcal{O}_{69} \to \mathbb{Z}$ can be constructed so that $(\mathcal{O}_{69}, |N'|)$ is Euclidean [119, 120, 121, 122, 123]; the proof turns out to be computer-assisted. Does such a construction exist for $\mathcal{O}_{14}$ [124, 125]?

As another aside, $h(j^2+4) > 1$ for odd $j > 17$ and $h(4k^2+1) > 1$ for $k > 13$. The arguments $j^2 + 4$ and $4k^2 + 1$ are assumed to be square-free. These two inequalities, known respectively as Yokoi's conjecture and Chowla's conjecture, were proved only recently by Biró [126, 127, 128, 129, 130].

We have not discussed prime-producing polynomials [131], asymptotic $h(d)$-averages over subsets [132, 133], the theory of genera [1] or Dirichlet L-series, although the definition of $L(D)$ earlier provides some foreshadowing of an upcoming essay [134].

References

[1] D. A. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*, Wiley, 1989; MR1028322 (90m:11016).

[2] D. A. Buell, *Binary Quadratic Forms. Classical Theory and Modern Computations*, Springer-Verlag, 1989; MR1012948 (92b:11021).

[3] P. Ribenboim, *My Numbers, My Friends. Popular Lectures on Number Theory*, Springer-Verlag, 2000, pp. 112–174; MR1761897 (2002d:11001).

[4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966; MR0195803 (33 #4001).

[5] H. Cohn, *A Second Course in Number Theory*, Wiley, 1962; reissued as *Advanced Number Theory*, Dover, 1980, MR0133281 (24 #A3115).

[6] H. L. Keng, *Introduction to Number Theory*, Springer-Verlag, 1982; MR0665428 (83f:10001).

[7] R. A. Mollin, *Quadratics*, CRC Press, 1996; MR 97e:11135.

[8] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A003657, A003658, and A037449.

[9] J. Jonasson, *Classes of Integral Binary Quadratic Forms*, Masters thesis, Göteborg University (2001).

[10] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A000924, A003646, A003649, A003652, A006641, A104888, A106029, A106030, A106031 and A106032.

[11] L. Carlitz, A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* 11 (1960) 391–392; MR0111741 (22 #2603).

[12] J. M. Masley, Where are number fields with small class number? *Number Theory, Carbondale 1979*, Proc. Southern Illinois conf., ed. M. B. Nathanson, Lect. Notes in Math. 751, Springer-Verlag, 1979, pp. 221–242; MR0564932 (81f:12004).

[13] A. Czogala, Arithmetic characterization of algebraic number fields with small class numbers, *Math. Z.* 176 (1981) 247–253; MR0607964 (82e:12006).

[14] F. Di Franco and F. Pace, Arithmetical characterization of rings of algebraic integers with class number three and four, *Boll. Un. Mat. Ital. D* 4 (1985) 63–69; MR0871911 (88c:11062).

[15] R. A. Mollin, K. Cheng and B. Goddard, The Diophantine equation $AX^2 - BY^2 = C$ solved via continued fractions, *Acta Math. Univ. Comenian.* 71 (2002) 121–138; MR1980374 (2004c:11031).

[16] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, $3^{\rm rd}$ ed., Springer-Verlag, 2004, pp. 104–105, 115–118; MR2078267 (2005c:11131).

[17] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A014000, A014046, A048941, A048942, A053370, A053371, A053372, A053373, A053374 and A053375.

[18] B. D. Beach and H. C. Williams, A numerical investigation of the Diophantine equation $x^2 - dy^2 = -1$, *Proc. $3^{\rm rd}$ Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Boca Raton, 1972, ed. F. Hoffman, R. B. Levow and R. S. D. Thomas, Congr. Numer. 6, Utilitas Math., 1972, pp. 37–68; MR0347729 (50 #231).

[19] P. Morton, On Rédei's theory of the Pell equation, *J. Reine Angew. Math.* 307/308 (1979) 373–398; MR0534233 (81f:12005).

[20] J. C. Lagarias, On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$, *Trans. Amer. Math. Soc.* 260 (1980) 485–508; MR0574794 (81g:10029).

[21] P. Stevenhagen, Frobenius distributions for real quadratic orders, *J. Théor. Nombres Bordeaux* 7 (1995) 121–132; MR1413571 (97g:11118).

[22] S. R. Finch, Pell-Stevenhagen constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 119–120.

[23] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A003654, A003814, and A031396.

[24] P. Kaplan and K. S. Williams, Pell's equations $X^2 - mY^2 = -1, -4$ and continued fractions, *J. Number Theory* 23 (1986) 169–182; MR0845899 (87g:11035).

[25] A. J. Stephens and H. C. Williams, Some computational results on a problem of Eisenstein, *Théorie des nombres*, Proc. 1987 Québec conf., ed. J.-M. De Koninck and C. Levesque, de Gruyter, 1989, pp. 869–886; MR1024611 (91c:11066).

[26] H. C. Williams, Eisenstein's problem and continued fractions, *Utilitas Math.* 37 (1990) 145–157; MR1068514 (91h:11018).

[27] N. Ishii, P. Kaplan and K. S. Williams, On Eisenstein's problem, *Acta Arith.* 54 (1990) 323–345; MR1058895 (91f:11024).

[28] K. S. Williams and N. Buck, Comparison of the lengths of the continued fractions of $\sqrt{D}$ and $\frac{1}{2}(1+\sqrt{D})$, *Proc. Amer. Math. Soc.* 120 (1994) 995–1002; MR1169053 (94f:11062).

[29] P. Stevenhagen, On a problem of Eisenstein, *Acta Arith.* 74 (1996) 259–268; MR1373712 (97b:11138).

[30] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A107996, A107997, A107998, A107999 and A108160.

[31] M. J. Jacobson, R. F. Lukes and H. C. Williams, An investigation of bounds for the regulator of quadratic fields, *Experiment. Math.* 4 (1995) 211–225; MR1387478 (97d:11173).

[32] S. Hallgren, Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem, *Proc. 34*$^{\text{th}}$ *ACM Symp. on Theory of Computing (STOC)*, Montreal, ACM, 2002, pp. 653–658; http://www.cse.psu.edu/~sjh26/.

[33] R. Jozsa, Notes on Hallgren's efficient quantum algorithm for solving Pell's equation, quant-ph/0302134.

[34] K. Heegner, Diophantische Analysis und Modulfunktionen, *Math. Z.* 56 (1952) 227–253; MR0053135 (14,725j).

[35] H. M. Stark, A complete determination of the complex quadratic fields of class-number one, *Michigan Math. J.* 14 (1967) 1–27; MR0222050 (36 #5102).

[36] H. M. Stark, On the "gap" in a theorem of Heegner, *J. Number Theory* 1 (1969) 16–27; MR0241384 (39 #2724).

[37] H. M. Stark, A historical note on complex quadratic fields with class-number one, *Proc. Amer. Math. Soc.* 21 (1969) 254–255; MR0237461 (38 #5743).

[38] A. Baker, Linear forms in the logarithms of algebraic numbers. I, *Mathematika* 13 (1966) 204-216; MR0220680 (36 #3732).

[39] M. Deuring, Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins, *Invent. Math.* 5 (1968) 169–179; MR0228464 (37 #4044).

[40] C. L. Siegel, Zum Beweise des Starkschen Satzes, *Invent. Math.* 5 (1968) 180–191; *Gesammelte Abhandlungen*, v. 4, ed. K. Chandrasekharan and H. Maass, Springer-Verlag, 1966, pp. 41–52; MR0228465 (37 #4045).

[41] S. Chowla, The Heegner-Stark-Baker-Deuring-Siegel theorem, *J. Reine Angew. Math.* 241 (1970) 47–48; MR0258762 (41 #3408).

[42] A. Baker, Imaginary quadratic fields with class number 2, *Annals of Math.* 94 (1971) 139–152; MR0299583 (45 #8631).

[43] H. M. Stark, A transcendence theorem for class-number problems, *Annals of Math.* 94 (1971) 153–173; MR0297715 (45 #6767).

[44] H. M. Stark, On complex quadratic fields with class-number two, *Math. Comp.* 29 (1975) 289–302; MR0369313 (51 #5548).

[45] H. L. Montgomery and P. J. Weinberger, Notes on small class numbers, *Acta Arith.* 24 (1973/74) 529–542; MR0357373 (50 #9841).

[46] J. Oesterlé, Nombres de classes des corps quadratiques imaginaires, *Astérisque* 121–122 (1985) 309–323; MR0768967 (86k:11064).

[47] S. Arno, The imaginary quadratic fields of class number 4, *Acta Arith.* 60 (1992) 321–334; MR1159349 (93b:11144).

[48] C. Wagner, Class number 5, 6 and 7, *Math. Comp.* 65 (1996) 785–800; MR1333327 (96g:11135).

[49] S. Arno, M. L. Robinson and F. S. Wheeler, Imaginary quadratic fields with small odd class number, *Acta Arith.* 83 (1998) 295–330; MR1610549 (99a:11123).

[50] M. Watkins, Class numbers of imaginary quadratic fields, *Math. Comp.* 73 (2004) 907–938; MR2031415 (2005a:11175).

[51] D. Goldfeld, Gauss's class number problem for imaginary quadratic fields, *Bull. Amer. Math. Soc.* 13 (1985) 23–37; MR0788386 (86k:11065).

[52] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, *Acta Arith.* 1 (1935) 83-86; *Gesammelte Abhandlungen*, v. I, ed. K. Chandrasekharan and H. Maass, Springer-Verlag, 1966, pp. 406–409.

[53] H. Heilbronn, On Dirichlet series which satisfy a certain functional equation, *Quart. J. Math.* 9 (1938) 194–195; *Collected Papers*, ed. E. J. Kani and R. A. Smith, Wiley, 1988, pp. 343–344.

[54] T. Estermann, On Dirichlet's L functions, *J. London Math. Soc.* 23 (1948) 275–279; MR0027797 (10,356c).

[55] S. Chowla, A new proof of a theorem of Siegel, *Annals of Math.* 51 (1950) 120–122; MR0033313 (11,420e).

[56] D. M. Goldfeld, A simple proof of Siegel's theorem, *Proc. Nat. Acad. Sci. U.S.A.* 71 (1974) 1055; MR0344222 (49 #8962).

[57] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Amer. Math. Soc., 1963, pp. 320–323; MR0160743 (28 #3954).

[58] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993, pp. 232–234, 261–263, 290–293; MR1228206 (94i:11105).

[59] D. Goldfeld and J. Hoffstein, Eisenstein series of 1/2-integral weight and the mean value of real Dirichlet L-series, *Invent. Math.* 80 (1985) 185–208; MR0788407 (86m:11029).

[60] B. A. Datskovsky, A mean-value theorem for class numbers of quadratic extensions, *A Tribute to Emil Grosswald: Number Theory and Related Analysis*, ed. M. Knopp and M. Sheingorn, Amer. Math. Soc., 1993, pp. 179–242; MR1210518 (94m:11137).

[61] S. R. Finch, Artin's constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 104–109.

[62] T. Taniguchi, A mean value theorem for the square of class numbers of quadratic fields, math.NT/0410531.

[63] P. Sebah, Calculation of Taniguchi's constant, unpublished note (2005).

[64] A. Granville and K. Soundararajan, The distribution of values of $L(1,\chi_d)$, *Geom. Funct. Anal.* 13 (2003) 992–1028; math.NT/0206031; MR2024414 (2005d:11129).

[65] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields, *Number Theory, Noordwijkerhout 1983*, Proc. 13^{th} Journées Arithmétiques, ed. H. Jager, Lect. Notes in Math. 1068, Springer-Verlag, 1984, pp. 33–62; MR0756082 (85j:11144).

[66] D. A. Buell, Class groups of quadratic fields. II, *Math. Comp.* 48 (1987) 85–93; MR0866100 (87m:11109).

[67] D. A. Buell, The last exhaustive computation of class groups of complex quadratic number fields, *Number Theory*, Proc. 1996 Canad. Number Theory Assoc. Ottawa conf., ed. R. Gupta and K. S. Williams, Amer. Math. Soc., 1999, pp. 35–53; MR1684589 (2000d:11156).

[68] L. C. Washington, Some remarks on Cohen-Lenstra heuristics, *Math. Comp.* 47 (1986) 741–747; MR0856717 (87j:11115).

[69] M. J. Jacobson, Experimental results on class groups of real quadratic fields (extended abstract), *Proc. 1998 Algorithmic Number Theory Sympos. (ANTS-III)*, Portland, ed. J. P. Buhler, Lect. Notes in Comp. Sci. 1423, Springer-Verlag, 1998, pp. 463–474; MR1726094 (2000h:11119).

[70] H. te Riele and H. Williams, New computations concerning the Cohen-Lenstra heuristics, *Experiment. Math.* 12 (2003) 99–113; MR2002677 (2005d:11183).

[71] S. R. Finch, Abelian group enumeration constants, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 273–276.

[72] S. R. Finch, Euler totient constants, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 115–118.

[73] S. R. Finch, Digital search tree constants, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 354–361.

[74] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields. II, *Proc. Royal Soc. London Ser. A* 322 (1971) 405–420; *Collected Papers of Hans Arnold Heilbronn*, ed. E. J. Kani and R. A. Smith, Wiley, 1988, pp. 532–547; MR0491593 (58 #10816).

[75] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A000037, A014600, A014601, A033313, A033317, A077425, A077428, A078355, A079896 and A087048.

[76] R. Lipschitz, Über die asymptotischen Gesetze von gewissen Gattungen zahlentheoretischer Functionen, *Monatsberichte der Königlichen Preussische Akademie der Wissenschaften zu Berlin. Sitzung der physikalisch-mathematischen Klasse* (1865) 174–185.

[77] F. Mertens, Über einige asymptotische Gesetze der Zahlentheorie, *J. Reine Angew. Math.* 77 (1874) 289–338.

[78] C. L. Siegel, The average measure of quadratic forms with given determinant and signature, *Annals of Math.* 45 (1944) 667–685; *Gesammelte Abhandlungen*, v. II, ed. K. Chandrasekharan and H. Maass, Springer-Verlag, 1966, pp. 473–491; MR0012642 (7,51a).

[79] I. M. Vinogradov, On the mean value of the number of classes of properly primitive forms of negative discriminant (in Russian), *Soobchsheniya Kharkovskogo Matematicheskogo Obshestva* 16 (1918) 10–38; Engl. transl. in *Selected Works*, ed. L. D. Faddeev, R. V. Gamkrelidze, A. A. Karacuba, K. K. Mardzhanishvili and E. F. Miscenko, Springer-Verlag, 1985, pp. 28–52.

[80] T. Shintani, On zeta-functions associated with the vector space of quadratic forms, *J. Fac. Sci. Univ. Tokyo Sect. I A Math.* 22 (1975) 25–65; MR0384717 (52 #5590).

[81] J. Hoffstein and M. Rosen, Average values of L-series in function fields, *J. Reine Angew. Math.* 426 (1992) 117–150; MR1155750 (93c:11022).

[82] F. Chamizo and H. Iwaniec, On the Gauss mean-value formula for class number, *Nagoya Math. J.* 151 (1998) 199–208; MR1650293 (99h:11041).

[83] M. B. Barban, Linnik's "great sieve" and a limit theorem for the class number of ideals of an imaginary quadratic field (in Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* 26 (1962) 573–580; MR0151441 (27 #1426).

[84] M. B. Barban, The "large sieve" method and its application to number theory (in Russian), *Uspehi Mat. Nauk* 21 (1966) 51–102; Engl. transl. in *Russian Math. Surveys* 21 (1966) 49–103; MR0199171 (33 #7320).

[85] M. B. Barban and G. Gordover, On moments of the number of classes of purely radical quadratic forms with negative determinant (in Russian), *Dokl. Akad. Nauk SSSR* 167 (1966) 267–269; Engl. transl. in *Soviet Math. Dokl.* 7 (1966) 356–358; MR0197401 (33 #5566).

[86] D. Wolke, Moments of the number of classes of primitive quadratic forms with negative discriminant, *J. Number Theory* 1 (1969) 502–511; MR0252322 (40 #5543).

[87] A. F. Lavrik, The moments of the number of classes of primitive quadratic forms of negative determinant (in Russian), *Dokl. Akad. Nauk SSSR* 197 (1971) 32–35; Engl. transl. in *Soviet Math. Dokl.* 12 (1971) 399–403; MR0280446 (43 #6166).

[88] M. Jutila, On character sums and class numbers, *J. Number Theory* 5 (1973) 203–214; MR0335449 (49 #230).

[89] P. Sebah, Calculation of Barban's constant, unpublished note (2005).

[90] S. Chowla and P. Erdös, A theorem on the distribution of the values of L-functions, *J. Indian Math. Soc.* 15 (1951) 11–18; MR0044566 (13,439a).

[91] A. S. Fainleib, The limit theorem for the number of classes of primitive quadratic forms with negative determinant (in Russian), *Dokl. Akad. Nauk SSSR* 184 (1969) 1048–1049; Engl. transl. in *Soviet Math. Dokl.* 10 (1969) 206–207; MR0244157 (39 #5474).

[92] P. D. T. A. Elliott, The distribution of the quadratic class number, *Litovsk. Mat. Sb.* 10 (1970) 189–197; MR0285505 (44 #2723).

[93] P. D. T. A. Elliott, *Probabilistic Number Theory. II. Central Limit Theorems*, Springer-Verlag, 1980, pp. 313–329; MR0560507 (82h:10002b).

[94] E. Stankus, Elementary method for estimating the complex moments of $L(1, \chi_D)$ (in Russian), *Litovsk. Mat. Sb.* 22 (1982) 160–170; Engl. transl. in *Lithuanian Math. J.* 22 (1982) 170–177; MR0659029 (83i:10054).

[95] M. Peter, The distribution of class numbers of pure number fields, http://omnibus.uni-freiburg.de/~mp4/.

[96] C. Hooley, On the Pellian equation and the class number of indefinite binary quadratic forms, *J. Reine Angew. Math.* 353 (1984) 98–131; MR0765829 (86d:11032).

[97] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A035015 and A107356.

[98] E. V. Podsypanin, The length of the period of a quadratic irrationality (in Russian), Studies in Number Theory, 5, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)* 82 (1979) 95–99, 166; Engl. transl. in *J. Soviet Math.* 18 (1982) 919–923; MR0537024 (80h:12002).

[99] J. Robertson, Comment on a proof by Podsypanin, unpublished note (2006).

[100] H. C. Williams, A numerical investigation into the length of the period of the continued fraction expansion of $\sqrt{D}$, *Math. Comp.* 36 (1981) 593–601; MR0606518 (82f:10011).

[101] C. D. Patterson and H. C. Williams, Some periodic continued fractions with long periods, *Math. Comp.* 44 (1985) 523–532; MR0777283 (86h:11113).

[102] A. S. Pen and B. F. Skubenko, An upper bound of the period of a quadratic irrationality (in Russian), *Mat. Zametki* 5 (1969) 413–418; MR0245524 (39 #6830).

[103] E. P. Golubeva, The length of a period of quadratic irrationality (in Russian), *Mat. Sbornik* 123 (1984) 120–129; Engl. transl. in *Math. USSR Sbornik* 51 (1985) 119–128; MR0728933 (85f:11044).

[104] E. P. Golubeva, On the lengths of the periods of a continued fraction expansion of quadratic irrationalities and on the class numbers of real quadratic fields (in Russian), Anal. Teor. Chisel i Teor. Funktsii. 8, *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* 160 (1987) 72–81, 297–298; Engl. transl. in *J. Soviet Math.* 52 (1990) 3049–3056; MR0906845 (88j:11055).

[105] S. R. Finch, Porter-Hensley constants, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 156–160.

[106] C. Faivre, Distribution of Lévy constants for quadratic numbers, *Acta Arith.* 61 (1992) 13–34; MR1153919 (93c:11057).

[107] E. P. Golubeva, An estimate for the Lévy constant for $\sqrt{p}$, and a class one number criterion for $\mathbb{Q}(\sqrt{p})$ (in Russian), Anal. Teor. Chisel i Teor. Funkts. 14, *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov (POMI)* 237 (1997) 21–30, 227; Engl. transl. in *J. Math. Sci.* 95 (1999) 2185–2191; MR1691280 (2000d:11129.

[108] E. P. Golubeva, The spectrum of Lévy constants for quadratic irrationalities (in Russian), Anal. Teor. Chisel i Teor. Funkts. 16, *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov (POMI)* 263 (2000) 20–33, 237; Engl. transl. in *J. Math. Sci.* 110 (2002) 3040–3047; MR1756334 (2001b:11065).

[109] E. P. Golubeva, On the spectra of Lévy constants for quadratic irrationalities and class numbers of real quadratic fields (in Russian), Anal. Teor. Chisel i Teor. Funkts. 17, *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov (POMI)* 276 (2001) 20–40, 349; Engl. transl. in *J. Math. Sci.* 118 (2003) 4740–4752; MR1850361 (2002k:11199).

[110] S. R. Finch, Freiman's constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 199–203.

[111] F. E. P. Hirzebruch, Hilbert modular surfaces, *Enseign. Math.* 19 (1973) 183–281; MR0393045 (52 #13856).

[112] P. Chowla and S. Chowla, On Hirzebruch sums and a theorem of Schinzel, *Acta Arith.* 24 (1973) 223–224; also in *Proc. Nat. Acad. Sci. U.S.A.* 69 (1972) 3745; MR0332717 (48 #11043) and MR0319942 (47 #8483).

[113] A. Schinzel, On two conjectures of P. Chowla and S. Chowla concerning continued fractions, *Annali Mat. Pura Appl.* 98 (1974) 111–117; MR0340187 (49 #4943).

[114] H. W. Lu, Hirzebruch sums and Hecke operators, *J. Number Theory* 38 (1991) 185–195; MR1111370 (92f:11153).

[115] K. Inkeri, Über den Euklidischen Algorithmus in quadratischen Zahlkörpern, *Annales Acad. Sci. Fennicae. Ser. A. I. Math.-Phys.* (1947) n. 41; MR0025498 (10,15g).

[116] H. Chatland and H. Davenport, Euclid's algorithm in real quadratic fields, *Canadian J. Math.* 2 (1950) 289–296; MR0041885 (13,15h).

[117] E. S. Barnes and H. P. F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms. I, *Acta Math.* 87 (1952) 259–323; MR0053162 (14,730a).

[118] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A003174 and A003246.

[119] D. W. Dubois and A. Steger, A note on division algorithms in imaginary quadratic number fields, *Canad. J. Math.* 10 (1958) 285–286; MR0094325 (20 #844).

[120] H. W. Lenstra, On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* 42 (1977) 201–224; MR0480413 (58 #576).

[121] D. A. Clark, A quadratic field which is Euclidean but not norm-Euclidean, *Manuscripta Math.* 83 (1994) 327–330; MR1277533 (95f:11086).

[122] G. Niklasch, On the verification of Clark's example of a Euclidean but not norm-Euclidean number field, *Manuscripta Math.* 83 (1994) 443–446; MR1277541 (95f:11087).

[123] D. A. Clark, Non-Galois cubic fields which are Euclidean but not norm-Euclidean, *Math. Comp.* 65 (1996) 1675–1679; MR1355007 (97a:11169).

[124] E. Bedocchi, L'anneau $\mathbb{Z}[\sqrt{14}]$ et l'algorithme euclidien, *Manuscripta Math.* 53 (1985) 199–216; MR0807095 (87b:11102).

[125] E. Bedocchi, On the second minimum of a quadratic form and its applications (in Italian), *Riv. Mat. Univ. Parma* 15 (1989) 175–190; MR1064256 (91i:11074).

[126] M. Y. Zhang, On Yokoi's conjecture, *Math. Comp.* 64 (1995) 1675–1685; MR1308464 (95m:11117).

[127] F. Lu, A lower bound for the exceptional field in Yokoi's conjecture (in Chinese), *J. China Univ. Sci. Tech.* 26 (1996) 385–391; MR1434628 (97m:11136).

[128] J. Beck, Diophantine approximation and quadratic fields, *Number Theory*, Proc. 1996 Eger conf., ed. K. Györy, A. Pethö and V. T. Sos, de Gruyter, 1998, pp. 55–93; MR1628833 (99k:11108).

[129] A. Biró, Yokoi's conjecture, *Acta Arith.* 106 (2003) 85–104; MR1956977 (2003k:11162).

[130] A. Biró, Chowla's conjecture, *Acta Arith.* 107 (2003) 179–194; MR1970822 (2004a:11113).

[131] M. J. Jacobson and H. C. Williams, New quadratic polynomials with high densities of prime values, *Math. Comp.* 72 (2003) 499–519; MR1933834 (2003k:11146).

[132] P. C. Sarnak, Class numbers of indefinite binary quadratic forms. II, *J. Number Theory* 21 (1985) 333–346; MR0814010 (87h:11027).

[133] O. M. Fomenko, Class numbers of indefinite binary quadratic forms (in Russian), Anal. Teor. Chisel i Teor. Funkts. 17, *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)* 276 (2001) 312–333, 354–355; Engl. transl. in *J. Math. Sci.* 118 (2003) 4918–4932; MR1850375 (2002d:11039).

[134] S. R. Finch, Quadratic Dirichlet L-series, unpublished note (2005).