The Class Number 1 Problem

Sjoerd de Vries

1 Introduction and history

These are notes written for a seminar talk at the university of Bonn. It introduces the class number 1 problem and sets the stage for Baker's solution using transcendental number theory. The proof is completed in the next seminar talk.

In a first course on algebraic number theory, one encounters the class group and shows that it is finite. In modern language then, the class number of a number field K is the size of its class group, which in turn is defined as

$$\mathrm{Cl}(K) = \frac{\{\text{fractional ideals of } K\}}{\{\text{principal fractional ideals of } K\}}.$$

Here a fractional ideal of K is an additive subgroup of K which is closed under multiplication from $\mathcal{O}_K$; it is principal if it is of the form $x\mathcal{O}_K$ for some $x \in K$. Then $|\mathrm{Cl}(K)| = 1$ if and only if $\mathcal{O}_K$ is a PID if and only if $\mathcal{O}_K$ is a UFD.
Class numbers have a rich history and weren't always thought of the way they are now. They originally arose from the theory of quadratic forms; this point of view is explained further below. Aside from the difference in (mathematical and written) language, Gauss conjectured in his Disquisitiones (1801) that there are only finitely many imaginary quadratic number fields having a given class number. In fact, he made the following very precise conjecture (now known as the *class number problem* (for $n = 1$)):

Theorem 1.1. Let $d > 0$ be square-free. The only number fields of the form $\mathbb{Q}(\sqrt{-d})$ with class number 1 are the ones with $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

Several decades earlier, Euler noticed that $x^2 - x + 41$ is prime for $x = 1, 2, \ldots, 40$. This probably makes one wonder two things:

1. Why does this happen?
2. Are there other polynomials of a similar form which have such a property?

In 1905, Rabinovitch (not the same as the one from the Rabinowitsch trick in algebraic geometry) stated the following theorem which goes a long way towards answering these questions:

Theorem 1.2. Let $-d < 0$ and $-d \equiv 1 \mod 4$. Then $x^2 - x + (1 + d)/4$ is prime for $x = 1, 2, \ldots, (d - 3)/4$ if and only if $\mathbb{Q}(\sqrt{-d})$ has class number 1.

Since $d = 163$ satisfies the requirements, the polynomial $x^2 - x + 41$ is special; and if theorem 1.1 is true, no "more successful" quadratic prime-generating polynomials of this form exist.
The aim of these notes is to relate the notions of quadratic forms, class numbers, and L-functions.

Last edited: 04 December 2019.

1.1 Quadratic forms

Consider a binary quadratic form $f(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$; we will also denote it by (a,b,c). Define its *discriminant* to be $\Delta = b^2 - 4ac$, i.e. -4 times the determinant of the matrix form of f.
Two forms f and g are called *equivalent* if they can be obtained from each other by applying an integral unimodular substitution; i.e. $g(x,y) = f(X,Y)$ for $(X,Y)^T = M(x,y)^T$ for some matrix $M \in \mathrm{SL}_2(\mathbb{Z})$. Since determinants are multiplicative, the discriminant descends to equivalence classes of forms.

Definition 1.3. An integer $r \in \mathbb{Z}$ is said to be *represented* by a quadratic form f if $f(m,n) = r$ for some $m,n \in \mathbb{Z}$.

Proposition 1.4. Equivalent forms represent the same integers.

Proof. Suppose $M \in \mathrm{SL}_2(\mathbb{Z})$ sends f to g; that is, if

$$f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

then

$$g(X,Y) = \begin{pmatrix} X & Y \end{pmatrix} M^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Then if $f(m,n) = r$, it follows that $g(M^{-1}(m,n)) = r$, and M^{-1} has integer coefficients since $\det M = 1$. □

Example 1.5. There can (and often do) exist inequivalent forms with the same discriminant. For instance, let $\Delta = -20$, and

$$f(x,y) = x^2 + 5y^2;$$
$$g(x,y) = 2x^2 + 2xy + 3y^2.$$

For f and g to be equivalent, we need an integer matrix such that

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix},$$

so in particular $\alpha^2 + 5\gamma^2 = 2$; but of course this has no integer solutions.

1.2 The link with the class group

The theory of quadratic forms is equivalent to the theory of quadratic number fields. The correspondence is already hinted at in the terminology: the discriminant of a form corresponds to the discriminant of a quadratic number field. The class number $h(\Delta)$ for forms is the number of inequivalent forms of discriminant Δ, and this is the same as the size of the ideal class group of the quadratic field of discriminant Δ (assumed to be square-free).
We know from algebraic number theory that the ideal class group is finite, and indeed we can prove it in an elementary way for quadratic forms:

Proposition 1.6. There are only finitely many equivalence classes of forms for a given discriminant $-d < 0$.

Proof. We first show that every form has a canonical representative.
We define for

$$M = \begin{pmatrix} m & n \\ o & l \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \text{ the map } \varphi_M : z \mapsto \frac{mz+n}{oz+l}$$

which maps the complex upper-half plane $\bar{\mathbb{H}} = \mathbb{H} \cup \{\infty\}$ to itself. Moreover, to any form $f = (a, b, c)$ of discriminant $-d < 0$, we associate the complex number $w_f := (-b+\sqrt{-d})/2a \in \mathbb{H}$. Suppose now that f and g are equivalent forms under the transformation M, i.e. $g(x, y) = f(M(x, y)^T)$. A calculation shows that then $\varphi_M(w_g) = w_f$. This gives us our canonical representative: given a class of forms, we pick the unique representative f such that w_f lies in the fundamental domain $\mathcal{F}$ of $\mathrm{SL}_2(\mathbb{Z})$, i.e. the area of $\bar{\mathbb{H}}$ where $-1/2 < \Re(z) < 1/2$ and $|z| > 1$, plus half the boundary of this domain. Then $\mathcal{F}$ contains a unique point for each $\mathrm{SL}_2(\mathbb{Z})$-orbit of points in $\bar{\mathbb{H}}$, as is proved in any introductory textbook on modular forms.
We call forms f with $w_f \in \mathcal{F}$ *reduced*. For a reduced form (a, b, c), since $\Im(w_f) = d/2a$, we get a bound on a. Since $\Re(w_f) = -b/2a$, we get a bound on $|b|$. Finally, c is determined by a, b and d, so there are only finitely many reduced forms for a given discriminant, and hence only finitely many equivalence classes of forms. □

The above proposition allows us to define the classical class number:

Definition 1.7. Let $\Delta < 0$ be square-free. The *class number* of Δ is the number of inequivalent forms of discriminant Δ.

Of course, we all know that the number field $\mathbb{Q}(\sqrt{-5})$ has class number two and discriminant -20. It is no coincidence that in Example 1.5, the discriminant in question was also -20. We will briefly sketch how the two theories relate.
Gauss showed that equivalence classes of quadratic forms of a given discriminant form an abelian group; the exact formulas are rather complicated, but essentially the construction of the group structure is a generalisation of the formula

$$(x^2 + cy^2)(X^2 + cY^2) = (Xx + cYy)^2 + c(xY - yX)^2,$$

where the right-hand side is a form in the variables $Xx + cYy$ and $xY - yX$. Details can be found in [3], section 4.2.
So how do we move between groups of forms and ideal class groups? The dictionary is quite simple: consider the map of sets

$$\begin{aligned} \{\text{forms of discriminant } \Delta < 0\} &\longrightarrow \{\text{ideals in } \mathcal{O}_{\mathbb{Q}(\sqrt{\Delta})}\} \\ (a, b, c) &\longmapsto \left(a, \frac{-b+\sqrt{\Delta}}{2}\right). \end{aligned}$$

It turns out that equivalent forms get sent to equivalent ideals, i.e. ideals differing by a scalar from $\mathbb{Q}(\sqrt{\Delta})$. Quotienting out equivalence of forms on the left and equivalence of ideals on the right, we then get an induced map

$$\{\text{reduced forms of discriminant } \Delta < 0\} \longrightarrow \mathrm{Cl}(\mathbb{Q}(\sqrt{\Delta})),$$

and this is a bijection. Hence, the classical and modern notions of class numbers agree.

In 1801, Gauss conjectured that for any $n \in \mathbb{N}$, there are only finitely many negative discriminants with $h(-d) = n$; moreover, he made tables of discriminants with class numbers 1, 2 and 3, and

conjectured that they were complete. The class number problem is the problem of finding a complete list of discriminants for any given class number. Today, we have complete lists of all negative discriminants with class number ≤ 100. In 1966, Baker and Stark (independently) were the first to solve the class number 1 problem by proving Gauss' table was indeed complete, and in 1971 they solved the class number 2 problem as well. We now proceed to introduce the tools needed to understand Baker's proof.

2 Preparations for the proof

2.1 The Kronecker symbol

Let K be a quadratic number field of discriminant Δ. The Kronecker symbol is the multiplicative character on $\mathbb{Z}$ defined on primes p as

$$\left(\frac{\Delta}{p}\right) = \begin{cases} 1 & p \text{ splits in } K; \\ -1 & p \text{ is inert}; \\ 0 & p \text{ is ramified}. \end{cases}$$

On units, we set

$$\left(\frac{\Delta}{1}\right) = 1; \qquad \left(\frac{\Delta}{-1}\right) = \operatorname{sign}(\Delta).$$

Another, more ad-hoc definition is that the Kronecker symbol extends the Legendre symbol on odd primes: more precisely, we define

$$\left(\frac{\Delta}{n}\right) = \left(\frac{\Delta}{u}\right) \prod_{p|n} \left(\frac{\Delta}{p_i}\right)^{a_i},$$

where $n = up_1^{a_1} \dots p_k^{a_k}$. The symbol is then defined as above on units, as the Legendre symbol on odd primes, and as

$$\left(\frac{\Delta}{2}\right) = \begin{cases} 0 & 2 \mid \Delta; \\ 1 & \Delta \equiv \pm 1 \mod 8; \\ -1 & \Delta \equiv \pm 3 \mod 8. \end{cases}$$

Depending on the situation, one description is often easier to use than the other. We note that the Kronecker symbol is multiplicative in the numerator and the denominator (except in some exceptional cases we will not consider).

Remark 2.1. In fact, the Kronecker symbol is a primitive Dirichlet character of modulus Δ. We know (for instance by the Kronecker-Weber theorem, but there are more elementary ways to show this) that any quadratic field can be embedded into a cyclotomic field; in fact $\mathbb{Q}(\sqrt{\Delta}) \hookrightarrow \mathbb{Q}(\zeta_\Delta)$. Galois theory gives a map

$$(\mathbb{Z}/\Delta\mathbb{Z})^\times \cong \operatorname{Gal}(\mathbb{Q}(\zeta_\Delta)/\mathbb{Q}) \to \operatorname{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}) \cong \{\pm 1\},$$

inducing a primitive Dirichlet character; this is precisely the Kronecker symbol.

2.2 L-functions

Let $\chi : (Z/n\mathbb{Z})^\times \to \mathbb{C}$ be a Dirichlet character. We can extend it to $\mathbb{Z}$ by setting $\chi(x) := \chi(\bar{x})$ for $(x, n) = 1$, and zero otherwise. For any such character, we define the *Dirichlet L-function* as

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_p (1 - \chi(p) p^{-s})^{-1},$$

which is defined for $\Re(s) > 1$ and can be extended to all of $\mathbb{C}$ by analytic continuation.
Dirichlet proved that if χ is the Kronecker symbol for $\mathbb{Q}(\sqrt{-d})$ $(0 > -d \equiv 1 \mod 4)$, then

$$L(1, \chi) = \frac{2\pi h(-d)}{w\sqrt{d}},$$

where w denotes the number of units in $\mathbb{Q}(\sqrt{-d})$. This relates L-functions and class numbers, and the strategy for the proof of the class number one problem relies on finding bounds for specific products of L-functions.
We will use the following later:

Lemma 2.2. Let ζ denote the Riemann zeta function and let $p \in \mathbb{R}_{>0}$. Then

$$\lim_{s \to 1} \zeta(2s - 1)(1 - p^{2s-2}) = -\log p.$$

Proof. Expanding $\zeta(2s - 1)$ as a Laurent series about $s = 1$ gives

$$\zeta(2s - 1) = \frac{1}{2s - 2} + O(1),$$

and expanding $1 - p^{2s-2}$ as a Taylor series about $s = 1$ gives

$$1 - p^{2s-2} = (s - 1) \cdot -2p^{2s-2} \log p + O((s - 1)^2).$$

When multiplying the two, in the limit only one term survives, and evaluates to

$$\lim_{s \to 1} \frac{-2(s - 1)p^{2s-2} \log p}{2(s - 1)} = -\log p.$$

□

2.3 Prerequisite facts

As a final preparation, we collect some facts which we will use in the next section. We will not give an elaborate justification for these; the integrals can be looked up in integration tables or verified numerically.

Fact 1: For $0 > -d \equiv 1 \mod 4$, we have

$$\sum_{n|l} \left(\frac{-d}{n} \right) = \frac{1}{2} \cdot \#\{\text{representations of } l \text{ by } f\}$$

as f runs over a complete set of reduced forms of discriminant $-d$. The reason is that the Kronecker symbol is related to ramification of primes, and there is a relationship between representations of l by a form of discriminant $-d$ and an ideal of norm l in $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-d})$.

Fact 2: Let $r \in \mathbb{Z}$ and consider the integral

$$I_r(s) = \int_{-\infty}^{\infty} \frac{\exp(-i\pi ur\sqrt{d}/ka)}{(u^2+1)^s} \mathrm{d}u$$

where $s > 1$ is a real number. Then $I_r(1) = \pi \exp(-\pi|r|\sqrt{d}/ka)$, and in fact

$$I_0(s) = \sqrt{\pi}\frac{\Gamma(s-1/2)}{\Gamma(s)}.$$

Fact 3: For $\chi(n) = \left(\frac{k}{n}\right)$ and $f = (a,b,c)$ a quadratic form,

$$\sum_{j=1}^{k} \chi(f(j,y)) = \chi(a) \sum_{j=1}^{k} \chi(j^2) \exp(2\pi ijy/k).$$

The right-hand side is known as a Gauss sum, a sum of a product of two characters.
The formula arises from the fact that the set $\{n \mapsto \exp(2\pi inl/k) \mid 1 \leq l \leq k\}$ forms an orthonormal basis for functions $\mathbb{Z}/k\mathbb{Z} \to \mathbb{C}$. Thus we can write

$$\chi(f(j,y)) = \sum_{l=1}^{k} \langle \chi, \exp(2\pi il/k)\rangle \exp(lf(j,y)/k),$$

and manipulating the sum on the right gives the required expression.

3 Baker's solution

We now start the proof of the class number 1 problem following Baker. This will consist of the calculation of an expression of a product of L-functions evaluated at $s = 1$, and next week this will be used along with linear forms in logarithms to provide an upper bound for the discriminant when $\mathrm{Cl}(K) = 1$.
From now on, let $k > 0$ and $-d < 0$ be coprime integers, both square-free and congruent to 1 mod 4. Denote by χ and χ' the Kronecker symbols for k and $-d$, respectively. Denote by $\mathcal{F}$ the finite set

$$\mathcal{F} := \{\text{reduced forms } ax^2 + bxy + cy^2 \mid b^2 - 4ac = -d\},$$

and consider the product of L-functions $L(s,\chi)L(s,\chi\chi')$. We calculate

$$\begin{aligned} L(s,\chi)L(s,\chi\chi') &= \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \left(\frac{k}{m}\right) m^{-s} \left(\frac{-kd}{n}\right) n^{-s} \\ &= \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \left(\frac{k}{mn}\right)\left(\frac{-d}{n}\right) (mn)^{-s} \\ &= \sum_{l=1}^{\infty}\sum_{n|l} \left(\frac{k}{l}\right) l^{-s} \left(\frac{-d}{n}\right) \end{aligned}$$

using the substitution $l = mn$. From Fact 1, we have that

$$\sum_{n|l} \left(\frac{-d}{n}\right) = \frac{1}{2} \cdot \#\{\text{representations of } l \text{ by } f \in \mathcal{F}\},$$

and so the expression simplifies to

$$\frac{1}{2}\sum_{f\in\mathcal{F}}\sum_{x,y\in\mathbb{Z}}{}'\chi(f)f^{-s}, \tag{1}$$

where the choice of representatives in $\mathcal{F}$ does not matter, and the $'$ indicates that $(x,y)\neq(0,0)$. Next we isolate the $y=0$-sum and use that $f(x,y)=f(-x,-y)$ to obtain

$$(1)=\sum_{f\in\mathcal{F}}\sum_{x=1}^{\infty}\chi(ax^2)(ax^2)^{-s}+\sum_{f\in\mathcal{F}}\sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty}\chi(f)f^{-s}. \tag{2}$$

The first term becomes

$$\sum_{x=1}^{\infty}\chi(x^2)x^{-2s}\sum_{f\in\mathcal{F}}\chi(a)a^{-s},$$

and since $\chi(x^2)=0$ whenever $(x,k)>1$ and equals 1 otherwise, the first sum is just $\zeta(2s)$ without the terms n^{-2s} with $(n,x)>1$, so we get for this first term

$$\zeta(2s)\prod_{p|k}(1-p^{-2s})\sum_{f\in\mathcal{F}}\chi(a)a^{-s}.$$

The second term will be rewritten also, using a Fourier series. To do so, we consider the functions (where $f\in\mathcal{F}$ ranges over representatives of classes)

$$g_f(v):=a(x+vy)^2+\frac{d}{4a}y^2 \tag{3}$$

which obey $g_f(b/2a)=f$, and define

$$F_f(v):=\sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty}\chi(f)g_f^{-s}.$$

Note that $F_f(v)=F_f(v+k)$ for all v:

$$\begin{aligned}F_f(v+k)=\sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty}\frac{\chi(f)}{g_f(v+k)^s}&=\sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty}\frac{\chi(f(x,y))}{(a((x+ky)+vy)^2+dy^2/4a)^s}\\&=\sum_{y=1}^{\infty}\sum_{X=-\infty}^{\infty}\frac{\chi(f(X-ky,y))}{(a(X+vy)^2+dy^2/4a)^s}=F_f(v),\end{aligned}$$

since χ is k-periodic and $k\mid f(X-vk,y)-f(X,y)$.
We now take the Fourier series of the F_f on $[0,k]$ to obtain

$$\hat{F}_f(\omega)=\sum_{r=-\infty}^{\infty}A_r(s)\exp(2\pi i\omega r/k),$$

where the Fourier coefficients are by definition

$$A_r(s)=\frac{1}{k}\int_0^k\sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty}\chi(f)g_f^{-s}\exp(-2\pi ivr/k)\mathrm{d}v,$$

and hence the Fourier series of the second term in (2) is

$$\sum_{f\in\mathcal{F}} \hat{F}_f(b/2a) = \sum_{f\in\mathcal{F}} \sum_{r=-\infty}^{\infty} A_r(s)\exp(\pi irb/ka).$$

We proceed by introducing some more substitutions. First, making the substitution $x + vy = uy\sqrt{d}/2a$ in (3) gives

$$g(u) = \left(\frac{\sqrt{d}}{2a}\right)^2 a(u^2+y^2),$$

so

$$A_r(s) = k^{-1}a^{-s}\left(\frac{\sqrt{d}}{2a}\right)^{1-2s} \int_0^k \sum_{y=1}^{\infty}\sum_{x=-\infty}^{\infty} \frac{\chi(f)\exp(-\pi iur\sqrt{d}/ka)}{(u^2+y^2)^s}\mathrm{d}u.$$

For any y, we can divide x by ky with remainder to write $x = m + kyn$. Introducing this change of variables and simplifying further, and writing $m = j + kl$ with $1 \le j \le k$ in the expression for σ, we find finally that

$$A_r(s) = k^{-1}a^{-s}\left(\frac{\sqrt{d}}{2a}\right)^{1-2s} I_r(s)\sum_{y=1}^{\infty}\sigma(y)y^{-2s},$$

where

$$I_r(s) = \int_{-\infty}^{\infty} \frac{\exp(-\pi iur\sqrt{d}/ka)}{(u^2+1)^s}\mathrm{d}u, \qquad \text{and} \qquad \sigma(y) = \begin{cases} y\sum_{j=1}^{k}\chi(f(j,y))\exp(2\pi irj/ky) & y \mid r; \\ 0 & \text{o/w.} \end{cases}$$

So $\sigma(y)$ is non-zero for only finitely many values of y for non-zero r. For $r = 0$, however, we have to do some work to show this. Following Baker's notation, we write $A_r := A_r(1)$ for non-zero r, and $A_0 := \lim_{s\to 1} A_0(s)$. Using our previously obtained expression, we get

$$L(1,\chi)L(1,\chi\chi') = \frac{\pi^2}{6}\prod_{p\mid k}(1-p^{-2})\sum_{f\in\mathcal{F}}\frac{\chi(a)}{a} + \sum_{f\in\mathcal{F}}\sum_{r=-\infty}^{\infty} A_r\exp(\pi irb/ka).$$

We want to bound this sum. More precisely:

Theorem 3.1. For non-zero r, we have

$$|A_r| \le \frac{2\pi}{\sqrt{d}}|r|\exp(-\pi|r|\sqrt{d}/ka), \tag{4}$$

and we have

$$A_0 = \begin{cases} \frac{-2\pi}{k\sqrt{d}}\chi(a)\log p & k \text{ is a power of the prime } p; \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Before we start the proof, we briefly recall the Möbius function: for p a prime number, it is defined as

$$\mu(p^k) = \begin{cases} 1 & k = 0; \\ -1 & k = 1; \\ 0 & \text{otherwise,} \end{cases}$$

and it is multiplicative on coprime integers. If $f(n) = \sum_{d\mid n} g(d)$, then by Möbius inversion, we have $g(n) = \sum_{d\mid n}\mu(n/d)f(d)$.
We now prove the theorem.

Proof. First consider the case $r \neq 0$. Simply substituting $s = 1$ everywhere in the expression for $A_r(s)$ gives

$$A_r = (k\sqrt{d}/2)^{-1} I_r(1) \sum_y \sum_{j=1}^{k} y^{-1} \chi(f(j,y)) \exp(2\pi i r j/ky).$$

Fact 2 now says that $I_r(1) = \pi \exp(-\pi|r|\sqrt{d}/ka)$. Since the sum over y runs only over positive divisors of r, it has absolute value at most $k|r|$, so (4) follows.
So let now $r = 0$. By definition, we get

$$A_0(s) = k^{-1} a^{s-1} (\sqrt{d}/2)^{1-2s} I_0(s) \sum_{y=1}^{\infty} y^{1-2s} \sum_{j=1}^{k} \chi(f(j,y)). \tag{6}$$

Fact 2 again says that $I_0(s) = \sqrt{\pi}\Gamma(s-1/2)/\Gamma(s)$, so it remains to estimate the sum over y. First by Fact 3, we have that

$$\sum_{j=1}^{k} \chi(f(j,y)) = \chi(a) \sum_{j=1}^{k} \chi(j^2) \exp(2\pi i j y/k).$$

This is a Ramanujan sum, which we can simplify: firstly,

$$\sum_{j=1}^{k} \chi(j^2) \exp(2\pi i j y/k) = \sum_{(j,k)=1} \exp(2\pi i j y/k). \tag{7}$$

Let $F(x) = \exp(2\pi i x y)$, $f(n) = \sum_{(j,n)=1} F(j/n)$, and $g(n) = \sum_1^n F(j/n)$. Then $g(n) = \sum_{d|n} f(d)$ (any fraction can be expressed uniquely in lowest terms), and Möbius inversion gives

$$(7) = f(k) = \sum_{d|k} \mu\left(\frac{k}{d}\right) g(d) = \sum_{d|k} \mu\left(\frac{k}{d}\right) \sum_{j=1}^{d} \exp(2\pi i j y/k) = \sum_{d|(y,k)} d\mu\left(\frac{k}{d}\right),$$

where the last equality follows because the sum of exponentials is d if $k|y$ and zero otherwise. Thus, returning to equation (6), we have

$$\begin{aligned}
\sum_{y=1}^{\infty} y^{1-2s} \sum_{j=1}^{k} \chi(f(j,y)) &= \chi(a) \sum_{d|k} d\mu\left(\frac{k}{d}\right) \sum_{d|y} y^{1-2s} \\
&= \chi(a) \sum_{d|k} \frac{k\mu(d)}{d} \sum_{\frac{k}{d}|y} y^{1-2s} \\
&= \chi(a) \sum_{d|k} \frac{k^{2s-2}\mu(d)}{d^{2s-2}} \zeta(2s-1) \\
&= \chi(a) k^{2-2s} \zeta(2s-1) \sum_{d|k} \frac{\mu(d)}{d^{2-2s}} \\
&= \chi(a) \zeta(2s-1) k^{2-2s} \prod_{p|k} (1 - p^{2s-2}),
\end{aligned}$$

where we used that d is square-free in the last equality.
This essentially shows that A_0 exists: the zeta function has a simple pole at $s = 1$, and if k is

divisible by more than one prime, the product gives a zero of order greater than one, giving the second case of (5). We only get a non-zero limit if k is a prime power, namely $-\log p$ by our previous lemma.
In this case, we plug everything we obtained into (6), and get

$$A_0 = \lim_{s \to 1} A_0(s) = \frac{2}{k\sqrt{d}} \sqrt{\pi} \Gamma(1/2) \chi(a)(-\log p),$$

and since $\Gamma(1/2) = \sqrt{\pi}$, this is what we wanted. □

Bibliography

[1] A. Baker. *Transcendental number theory.* Cambridge University Press, 1975.

[2] A. Baker. *A concise introduction to the theory of numbers.* Cambridge University Press, 1984.

[3] D. A. Buell. *Binary Quadratic Forms.* Springer-Verlag, first edition, 1989.

[4] D. Goldfeld. Gauss' class number problem for imaginary quadratic fields. *Bulletin of the American Mathematical Society*, 13:23 – 37, 1985.

[5] D. Zagier. A kronecker limit formula for real quadratic fields. *Mathematische Annalen*, 213:153–184, 1975.