Michael Straka

Class Groups for Cryptographic Accumulators

Posted Mar 31, 2019

Late last year Benedikt Bunz and Ben Fisch, both PhD students at Stanford University, released a paper along with Dan Boneh titled "Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains". In it they use some basic group theory to build a dynamic accumulator, which allows for storing and deleting elements in addition to the use of both membership and non-membership proofs. It can be used to create a vector commitment data structure analogous to Merkle trees, with the main difference being that it allows for *constant-sized* inclusion proofs, where a Merkle tree has $O(\log n)$ sized inclusion proofs where n is the number of elements being stored. If the stored set is big enough, this can be a pretty big deal.

One of the main security assumptions their construction uses is that it relies on a group of unknown order. In particular the *strong RSA assumption* must hold, meaning it is hard to compute a chosen root of a random group element. There are two good candidates for such a group. The simpler of the two is known as an *RSA group*, or a multiplicative group of order N where $N = pq$ for some unknown factorization. This however requires a trusted setup, as whoever generates the modulus N must be trusted to discard p and q. The alternative is known as a *class group of imaginary quadratic order*, which eliminates the need for a trusted setup and which we will be exploring in this post.

Class groups come from a long line of mathematical research, and were originally discovered by Gauss in his *Disquisitiones Arithmeticae* in 1801. The math that's been developed on top of his work in the past two centuries involves some decently complex algebra. I'll explain most of the concepts used but will expect that you know what groups, rings, fields, homomorphisms, and isomorphisms are in an algebraic context. Feel free to look them up if not.

This post is meant to be an introduction to what a class group is and to summarize the most important results to consider when implementing them as a group of unknown order;

detailed proofs can be found in the list of further readings below.

What is a class group?

There are two equivalent ways to understand the class group which are isomorphic to one another. One coming from a subfield of mathematics known as algebraic number theory is known as the *ideal class group*, which is the quotient of fractional ideals by fractional principal ideals J_K/P_K of a ring of integers O_K of a quadratic extension $K = \mathbb{Q}(\sqrt{d})$ of the rational numbers. Later we'll walk through what this means step-by-step. The other way to look at the class group is known as the *form class group* and comes from the study of *binary quadratic forms*, or equations of the form

$$ax^2 + bxy + xy^2 = n$$

by working with an equivalence relation over forms which all have the same discriminant $b^2 - 4ac$.

These two views are actually pretty different; it's not at all obvious that they represent the same object! Either is paramaterized by its integer *discriminant* Δ, as there is a one-to-one correspondence between class groups and valid discriminants. When using the group for cryptographic purposes as a group of unknown order there are three main choices to be made:

-What discriminant should be chosen

-How to represent the group in a numerical setting

-What algorithms should be used when performing the group operation

The ideal class group makes it easier to understand how and why a particular form of discriminant should be chosen. As we will see, we want the discriminant to be the negation of a prime congruent to 3 mod 4, or $-p$ where $p \equiv 3 \pmod 4$. On the other hand, the form class group is easier to represent and perform operations on numerically. With this in mind, we will start with the ideal class group and move on to the form class group from there.

Ideal Class Group

In basic field theory there is the concept of a *field extension*, or a field containing another field as a subfield. The *degree* of an extension is the size of the larger field's basis over the smaller *base field*. An example of this is the complex numbers $\mathbb{C}$, which extend the real numbers $\mathbb{R}$ by adding in $\sqrt{-1} = i$, so that $\mathbb{C} = \mathbb{R}(i)$. This is known as a *degree 2* or *quadratic* extension, because the basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$ is of size 2, and is given by $(1, i)$.

Similarly, we can construct generalizations of the rational numbers by adding in $\sqrt{d}$ to $\mathbb{Q}$, for some square-free number d. In this case a basis for $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ is also size 2 and is given by $(1, \sqrt{d})$, making $\mathbb{Q}(\sqrt{d})$ a quadratic extension of $\mathbb{Q}$. More formally, $\mathbb{Q}(\sqrt{d})$ is the smallest field containing both $\mathbb{Q}$ and $\sqrt{d}$.

Once we have our quadratic extension $K = \mathbb{Q}(\sqrt{d})$, we can also get a corresponding generalization of the integers known as the *ring of integers* of K, denoted O_K. To obtain O_K, we look at K and take all of its elements which are the roots of some monic polynomial with integer coefficients, also known as an *integral* polynomial, i.e. the set of all $\alpha \in K$ such that there exists some polynomial

$$p(x) = x^n + b_{n-1}x^{n-1} + ...b_1 x + b_0$$

where $b_{n-1}, \dots, b_0 \in \mathbb{Z}$ and $p(\alpha) = 0$. It turns out that $O_{\mathbb{Q}} = \mathbb{Z}$, so that the ring of integers of the rational numbers is simply the integers. In fact, for any finite-degree extension K of $\mathbb{Q}$, O_K contains $\mathbb{Z}$. As its name suggests, O_K forms a ring under addition and multiplication.

Something that would help us to understand O_K would be to find some analogue of a basis over a vector space for it. We are helped here by the concept of a *module*, which is a generalization of vector spaces for rings. As an example, a $\mathbb{Z}$-module M consists of the integers $\mathbb{Z}$, which form a ring, acting on some abelian group $(M, +)$. In other words, the ring of integers acts like a set of scalars and the abelian group like a set of vectors. Modules do not have as many guarantees as vector spaces; for example, a module may not have a basis.

Because every ring is an abelian group under addition, every ring is a $\mathbb{Z}$-module. This implies we can act on any ring of integers O_K by the integers $\mathbb{Z}$ in a way analogous to acting on vectors by scalars. While not every module has a basis as a $\mathbb{Z}$-module (a "$\mathbb{Z}$-basis"), it is true that every ring of integers O_K has a $\mathbb{Z}$-basis. More specifically, if K is a degree n extension of $\mathbb{Q}$, then there is some $b_1, \ldots, b_n \in O_K$ such that any $x \in O_K$ can be uniquely written as

$$x = \sum_{i=1}^{n} a_i b_i$$

where $a_1, \ldots, a_n \in \mathbb{Z}$.

What are the possible $\mathbb{Z}$-bases for a ring of integers of a quadratic extension? This turns out to be pretty simple. We know $\sqrt{d} \in O_K$ since $\sqrt{d} \in K = \mathbb{Q}(\sqrt{d})$ and it is the root of the integral polynomial $x^2 - d$. It also happens to be the case that if $d \equiv 1 \pmod 4$ then for any $x + y\sqrt{d} \in O_K$ where $x, y \in \mathbb{Z}$ we can write

$$x + y\sqrt{d} = a + b\frac{1 + \sqrt{d}}{2}$$

for some $a, b \in \mathbb{Z}$. It can be shown that no other elements are in O_K, giving us two possible $\mathbb{Z}$-basis depending on d. If $d \equiv 2, 3 \pmod 4$ then we have a $\mathbb{Z}$-basis of $(1, \sqrt{d})$, and if $d \equiv 1 \pmod 4$ we have a $\mathbb{Z}$-basis of $(1, \frac{1+\sqrt{d}}{2})$. Another way of phrasing this is to say that if $d \equiv 1 \pmod 4$, then $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and $O_K = \mathbb{Z}[\sqrt{d}]$ otherwise.

To define the discriminant of a finite extension K of $\mathbb{Q}$, we first need the concept of an embedding of K into some field $\mathbb{F}$, which is simply an injective ring homomorphism from K into $\mathbb{F}$. If we have n embeddings $\sigma_1, \ldots, \sigma_n$ from K into the complex numbers $\mathbb{C}$ and a basis $b_1, \ldots, b_n$ of O_K as a $\mathbb{Z}$-module, then the discriminant of K is given by

$$\Delta_K = \begin{vmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \ldots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \sigma_2(b_n) \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \ldots & \ldots & \sigma_n(b_n) \end{vmatrix}^2$$

where the notation above means we take the square of the determinant of the given matrix.

For our case where $K = \mathbb{Q}(\sqrt{d})$, we have two embeddings of K into $\mathbb{C}$. Letting $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, one is given by $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ and the other by $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$. If $d > 0$ then we can consider these to be embeddings of K into $\mathbb{R}$. In practice we want $d < 0$. As we'll see later this gives us a nicer structure by letting us take a unique "reduced" form for any element when using the form class group as a numerical representation. It also makes it less likely that the class group will be trivial and contain only one element.

Given these embeddings and the $\mathbb{Z}$-bases above it is easy to check that if $d \equiv 1 \pmod 4$ then $\Delta_K = d$ and if $d \equiv 2, 3 \pmod 4$ then $\Delta_K = 4d$. When choosing a discriminant, this makes it more convenient to pick some square-free value $\Delta \equiv 1 \pmod 4$, as otherwise we need to ensure that $\Delta/4$ is square-free.

We're almost ready to construct the class group itself! To do so we'll need the concept of an *ideal*, which is an additive subgroup of a ring with an additional multiplicative "absorption" property. Specifically if we have an ideal $I \subset O_K$ of a ring of integers then for any $r \in R$ and $x \in I$, $rx \in I$.

For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal.

We can generalize the concept of an ideal of a ring to get the idea of a *fractional ideal*. Intuitively a fractional ideal J of a ring O_K is a subset of the ring's enclosing field K such that we can "clear the denominators" of J. More formally J is a nonzero subset of K such that for some $r \neq 0 \in O_K$, $rJ \subset O_K$ is an ideal of O_K.

As an example $\frac{5}{4}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$, since it is a subset of the smallest field $\mathbb{Q}$ containing $\mathbb{Z}$ and has the property that $4(\frac{5}{4}\mathbb{Z}) = 5\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

For any two ideals or fractional ideals $I, J \subset O_K$ we can define a form of multiplication on them:

$$IJ = \{\sum a_i b_i | a_i \in I, b_i \in J\}$$

Since ideals are closed under addition, this gives the smallest ideal containing every element of both I and J.

A fractional ideal I of O_K is called *principal* if there is some $r \in O_K$ such that $rO_K = I$. In other words, I is generated by a single element of O_K.

Finally we need one more concept from group theory known as a *quotient group*. While I won't define it formally here, a basic example is given by $\mathbb{Z}/3\mathbb{Z}$ which has the structure of arithmetic mod 3. It can be formed by taking every element $n \in \mathbb{Z}$, computing $n3\mathbb{Z}$, then forming a group operation having the same structure as $(\mathbb{Z}, +)$ over the 3 resulting distinct sets of integers.

Let J_K denote the set of fractional ideals of O_K and P_K the set of principal fractional ideals of O_K. Both form abelian groups under ideal multiplication defined above. This means it makes sense to take the quotient group J_K/P_K. This quotient group is the ideal class group.

There are two extreme cases we can consider here. If $J_K = P_K$, then J_K/P_K is the trivial group with one element. On the other hand, if no fractional ideals are principal then $J_K/P_K = J_K$. The order of J_K/P_K can be interpreted as a measurement of the extent to which O_K fails to be a *principal ideal domain*, or to have all of its ideals be principal. We can even take this a bit further, since for any ring of integers O_K being a principal ideal domain is equivalent to every element of O_K having a unique factorization. In other words, the order of a class group of K is a measurement of how much its ring of integers O_K fails to give each element a unique factorization! Given that O_K is effectively a generalization of the integers, it's pretty neat that we can define this rigorously.

The order or number of elements of J_K/P_K is known as its *class number*, and is known to be hard to compute for large discriminants. As with all cryptographic assumptions, this has not been proven but is assumed to be true because no one has broken it efficiently. At the moment it is generally accepted that, within the context of solving discrete logarithms, a discriminant of 687 bits provides as much security as a 1024-bit RSA key, and a discriminant of 1208 bits about as much security as a 2048-bit RSA key.

Form Class Group

Next we will discuss the form class group, and see how it is related to the ideal class group. The form class group was originally discovered in the study of *binary quadratic forms*, or functions of the form

$$f(x, y) = ax^2 + bxy + cy^2$$

where $a, b, c \in \mathbb{R}$. For convenience we will write $f = (a, b, c)$ and call f a *form*. In practice we want to restrict ourselves to the case where $a, b, c \in \mathbb{Z}$, as our end goal is to use forms to represent the class group in a computer and being able to store forms as integer triples rather than triples of floating point values simplifies things.

All binary quadratic forms in a given form class group have the same *discriminant*, given by $\Delta_f = b^2 - 4ac$. This is identical to the discriminant of the corresponding ideal class group.

A form *represents* an integer n if $f(x, y) = n$ for some $x, y \in \mathbb{Z}$.

The form class group is made up of equivalence classes of forms, or sets of forms considered to be equivalent. This is similar to how, when doing arithmetic mod 3, the symbol 1 represents the set of all integers congruent to 1 (mod 3). We say that two forms f_1, f_2 are *equivalent* if they represent the same set of integers.

In order to be a valid group, we need a group operation $*$ that will give us some representative f_3 of an appropriate equivalence class given forms f_1, f_2 so that $f_1 * f_2 = f_3$. We also need an identity form g so that $f * g = f$ for all forms f, and for any form f we need an inverse f^{-1} so that $f * f^{-1} = g$.

We mentioned above the the ideal class group with discriminant $\Delta \in \mathbb{Z}$ is isomorphic to the form class group with the same discriminant Δ. In fact, this is only true when $\Delta < 0$, and all forms $f = (a, b, c)$ in the group are positive definite, meaning $f(x, y) > 0$ for all possible $x, y \in \mathbb{Z}$. This is equivalent to having both $\Delta_f < 0$ and $a > 0$. From now on, we will assume that any form is positive definite.

As the form class group is composed of equivalence classes of forms, it would also be good if we could reduce any form of an equivalence class down to one unique element. Since we also want to represent elements $f = (a, b, c)$ in terms of bits, it would also be good if this

reduced element was reasonably small. It turns out that we can define a reduction operation that gives us both of these desirable properties.

We can break down the reduction operation into two pieces; a "normalization" operation and a "reduction" operation, with the requirement that a form must be normalized before it is reduced.

A form $f = (a, b, c)$ is *normal* if $-a < b \leq a$. We can define a normalization operation by

$$\eta(a, b, c) := (a, b + 2ra, ar^2 + br + c)$$

where $r = \lfloor \frac{a-b}{2a} \rfloor$.

When we normalize a form f, we want the resulting normalized form f' to be equivalent to f. How do we know this is actually the case? It turns out we can understand equivalence of forms using actions by a certain class of matrices known as SL_2, or the "special linear group" of invertible matrices with determinant equal to 1.

Two forms f_1, f_2 are in fact equivalent if there exists $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that

$$f_1(\alpha x + \beta y, \gamma x + \delta y) = f_2(x, y)$$

$$\alpha\delta - \beta\gamma = 1$$

This is actually only partially true, as we can relax the second requirement to be $\alpha\delta - \beta\gamma = \pm 1$. However, this won't actually give us a valid equivalence relation, i.e. if we let $\equiv$ denote equivalence then $f_1 \equiv f_2$ and $f_2 \equiv f_3$ wouldn't necessarily imply $f_1 \equiv f_2 \equiv f_3$.

The "correct" form of equivalence mentioned above gives us an action of SL_2 on forms, so that if f_1, f_2 are equivalent then there is some invertible

$$A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

with $\det(A) = 1$ such that $f_1 = Af_2$.

With this is mind, we can show that f and its normalized form $f' = \eta(f)$ are equivalent by the matrix

$$A = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix}$$

Once we've normalized a form, we can then reduce it to obtain its unique reduced equivalent form. A form $f = (a, b, c)$ is *reduced* if it is normal and $a < c$ or $a = c$ and $b \geq 0$.

We can define a reduction operation as

$$\rho(a, b, c) := (c, -b + 2sc, cs^2 - bs + a)$$

where $s = \lfloor \frac{c+b}{2c} \rfloor$. Unlike the normalization operation η, it may need multiple iterations before our form is reduced. To reduce a form f, we can compute $f \leftarrow \eta(f)$ then repeatedly compute $f \leftarrow \rho(f)$ until f is reduced.

Similar to normalized forms, we can see that a reduced form f' of f is equivalent to f using the matrix

$$A = \begin{bmatrix} 0 & -1 \\ 1 & r \end{bmatrix}$$

How do we know reduced elements are relatively small? If $\Delta_f < 0$ then for a reduced form $f = (a, b, c)$ we have that

$$a \leq \sqrt{\frac{|\Delta_f|}{3}}$$

Because in a reduced form $|b| \leq a$ and $c = \frac{b^2 - \Delta_f}{4a}$, the above upper bound on the size of a implies that reduce elements as a whole tend to be small, having a bit representation at least as small as that of Δ_f. This makes the group operation on reduced elements relatively efficient.

There is also a reasonable upper bound on the number of reduction steps required, given by $\log_2(\frac{a}{\sqrt{|\Delta|}}) + 2$.

The group operation itself, known as "form composition", is a bit complicated. The basic idea is that, given two forms f_1, f_2 with the same discirminant Δ, we can multiply them together and use a change of variables to obtain a third form f_3 such that $f_1 f_2 = f_3$. More exactly, the game is to find integers $p, q, r, s, p', q', r', s', \alpha, \beta, \gamma$ so that

$$\begin{aligned} X &= px_1x_2 + qx_1y_2 + ry_1x_2 + sy_1y_2 \\ Y &= p'x_1x_2 + q'x_1y_2 + r'y_1x_2 + s'y_1y_2 \\ f_3(x,y) &= \alpha x^2 + \beta xy + \gamma y^2 \\ f_3(X,Y) &= f_1(x,y)f_2(x,y) \end{aligned}$$

Let LinCong(a, b, m) be an algorithm which solves a linear congruence of the form $ax \equiv b \pmod m$ by finding some $x = \mu + \nu n$ where $n \in \mathbb{Z}$ and outputs (μ, ν). Given two forms $f_1 = (a, b, c)$ and $f_2 = (\alpha, \beta, \gamma)$, we can define a group operation on them as follows:

1. Set $g \leftarrow \frac{1}{2}(b + \beta)$, $h \leftarrow -\frac{1}{2}(b - \beta)$, $w \leftarrow \gcd(a, \alpha, g)$
2. Set $j \leftarrow w$, $s \leftarrow \frac{a}{w}$, $t \leftarrow \frac{\alpha}{w}$, $u \leftarrow \frac{g}{w}$
3. Set $(\mu, \nu) \leftarrow$ LinCong$(tu, hu + sc, st)$
4. Set $(\lambda, \rho) \leftarrow$ LinCong$(tv, h - t\mu, s)$
5. Set $k \leftarrow \mu + \nu\lambda$, $l \leftarrow \frac{kt-h}{s}$, $m \leftarrow \frac{tuk-hu-cs}{st}$.
6. Return $f_3 = (st, ju - (kt + ls), kl - jm)$.

In practice it's best to always reduce the result f_3 after performing composition. This way we are guaranteed that the multiplication of two forms takes $O(\log^2 |\Delta|)$ bit operations where Δ is the discriminant of the group being used. This is not guaranteed if the two inputs forms are not reduced.

In order to be a group operation forms under composition must have an identity element. If $\Delta < 0$ this turns out to be $f = (1, k, \frac{k^2-\Delta}{4})$ where $k = \Delta \pmod 2$.

For any form $f = (a, b, c)$, its inverse under form composition is given by $f^{-1} = (a, -b, c)$.

We're now done constructing the form class group! We have a group operation, a way to get a unique representative element from each equivalence class of forms, an identity, and inverses.

There is one very important optimization we can do. Above we mentioned that we want to choose the negation of a prime p as our discriminant. It turns out that this lets us simplify our composition algorithm when $f_1 = f_2$, since using $\Delta = -p$ implies that $\gcd(a, b) = 1$ for any form $f = (a, b, c)$. Unlike much of the math discussed in this post, this is pretty easy to see. If $\gcd(a, b) = n \neq 1$ then for some $a', b' \in \mathbb{Z}$ we have that ana' and $b = nb'$, implying $\Delta = b^2 - 4ac = n(b'b - 4a'c)$ which is impossible because $-p$ can't be divisible by n.

This, in addition to the fact that $a = \alpha, b = \beta, c = \gamma$ gives us the simplified squaring algorithm below:

1. Set $(\mu, \nu) \leftarrow \text{LinCong}(b, c, a)$
2. Return $f^2 = (a^2, b - 2\alpha\mu, \mu^2 - \frac{b\mu - c}{a})$.

This is a big deal for efficiency, since we can compute exponentiation using repeated squaring.

Isomorphism

Going back to the ideal class group, there is another construction equivalent to the quotient group J_K/P_K. Similar to equivalence of forms, we can define an equivalence of ideals in J_K by saying that two fractional ideals I, J of J_K are equivalent if there is some $\alpha \neq 0 \in K$ such that $\alpha I = J$. The equivalence classes formed by this relation are exactly the elements of J_K/P_K. We can similarly represent fractional ideals by their at most 2 generating elements, so that if I is generated by α, β we can represent it by (α, β). We can also get a unique "reduced" ideal from each equivalence class.

Ideal and form class groups are isomorphic when the discriminant $\Delta \in \mathbb{Z}$ being used is negative. In some sense this means multiplication of fractional ideals in the ideal setting and form composition in the form class group are really the same operation, since we can

move back and forth between corresponding equivalence classes of fractional ideals and of forms.

We need just a few more tools before defining the isomorphism itself. If K is a finite field extension of $\mathbb{F}$, so that K is a finite-dimensional vector space over $\mathbb{F}$, then for any $\alpha \in K$ the map $m_\alpha(x) = \alpha x$ is an $\mathbb{F}$-linear transformation from K into itself. The *field norm* $N(\alpha)$ is the determinant of the matrix of this linear transformation. The trace Tr of α is the trace of this matrix.

In our case where $K = \mathbb{Q}(\sqrt{d})$, for any $x = a + b\sqrt{d} \in K$ we have $N(x) = a^2 - db^2$, implying $N(x)$ is positive when $d < 0$.

Next, if I is a non-zero fractional ideal of O_K, the *absolute norm* of I is given by the mapping $N(I) = |O_K/I|$, or the order of the quotient of O_K by its ideal I.

As their names and notation suggests, the field and absolute norms are related. If an ideal I of ring of integers O_K is principal so that there is some $\alpha \in O_K$ such that $\alpha O_K = I$, then $N(I) = |N(\alpha)|$.

The isomorphism between ideal and form class groups is as follows. If $f = (a, b, c)$ where $a, b, c \in \mathbb{Z}$ and $\Delta_f < 0$, then we can map f to a fractional ideal of the ideal class group with same discriminant by

$$\Phi(a, b, c) := (a\mathbb{Z} + \frac{-b + \sqrt{\Delta_f}}{2}\mathbb{Z})$$

with inverse

$$\Phi^{-1}(I) := \frac{N(\alpha x - \beta y)}{N(I)}$$

where (α, β) is some $\mathbb{Z}$-basis of the fractional ideal I. We can see that the inverse maps a fractional ideal to a binary quadratic form using the following identity:

$$N(\alpha x + \beta y) = N(\alpha)x^2 + Tr(\alpha\beta')xy + N(\beta)y^2$$

where for some element of a ring of integers $x = a + b\sqrt{d}$ we denote its conjugate by $x' = a - b\sqrt{d}$.

If $\Delta < 0$ then the coefficient of x^2 given by $N(\alpha)/N(I)$ will be positive, meaning the resulting form $f = (a, b, c)$ will be positive definite as $\Delta_f < 0$ and $a > 0$. It can be shown that when $\Delta < 0$, Φ is a bijection which preserves the group structure of binary quadratic forms under form composition in mapping to fractional ideals of a ring of integers under ideal multiplication. In other words, Φ is an isomorphism.

Solved and Open Conjectures

We'll conclude with a handful of conjectures made in some form by Gauss in 1801 which show further why we want to use a negative discriminant:

1. The class number of the ideal class group of $\mathbb{Q}(\sqrt{d})$ converges to infinity as $d \to -\infty$.
2. There are exactly 13 negative discriminants having a class number of 1, in particular -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.
3. There are infinitely many positive discriminants associated with class groups having a class number of 1.

The first was proven in 1934 by Hans Heilbronn, the second in 1967 by Heegner, Stark and Baker. The third remains open.

Further Reading

The Chia VDF Competition exposition of class groups is an excellent overview on how to implement the group numerically. The form class group algorithms above on normalization, reduction, and composition in particular were taken from here.

A Survey on IQ Cryptography by Johannes Buchmann and Safuat Hamdy is a great survey from 2001 of cryptography using class groups of imaginary quadratic order.

A Course in Computational Algebraic Number Theory by Henry Cohen is a well-written and comprehensive textbook on algorithms fundamental to algebraic number theory.

The Structure of the Class Group of Imaginary Quadratic Fields by Nicole Miller and The Correspondence Between Binary Quadratic Forms and Quadratic Fields by Corentin Perret-Gentil are both good proof-focused introductions to the ideal and form class groups and their correspondence.

About

Hi! I'm Michael Straka. I'm currently finishing my Master's degree in Computer Science at Stanford University with a focus in cryptography and experience working with various fintech, blockchain, and private cryptography lab companies. I've had experience implementing cutting-edge cryptographic accumulators and user-authenication services in industry, in addition to having done circuit construction for general-purpose zero-knowledge proofs. In my spare time I enjoy kickboxing, photography, and writing short stories. The unifying factor between my interests is a passion for distilling complex ideas and topics down to their essence; this blog is an attempt to share that.

Posted May 1, 1995

Home