Binary quadratic forms

Lipa Long

Chik Network

1 Introduction

Chik's underlying verifiable delay function (VDF) performs squaring computations within class groups of binary quadratic forms. This paper provides an introduction to binary quadratic forms and to their properties relevant to application in the Chik VDF, and an efficient algorithm for their composition is introduced.

A VDF is a sequential operation that takes a prescribed amount of time to compute (and which cannot be accelerated by parallelism) and which produces an accompanying proof by which the result may be quickly verified. The best known method for achieving a non-parallelizable sequential operation is repeated squaring in a group of unknown order. The unknown order requirement is due to the divisibility of the order of a finite group by the order of any element in the group; if the group order is known then the repeated squaring operation could be reduced modulo the order of the group, shortcutting the computation.

When using an RSA group in a VDF, the group is a multiplicative group $\mathbb{Z}/N$, where $N = pq$ such that p and q are primes, $p, q \neq 2$, and p and q are both unknown. $\mathbb{Z}/N$ is considered a group of unknown order because the difficulty of computing the group order is on par with the difficulty of computing the factors of N. To guarantee that the factors — and therefore the group order — are indeed unknown, a trusted setup may be used which ensures that the factors used to generate the group are not revealed.[1] However, a trusted setup requires that the party generating the trusted parameters destroys the keys once N is created. If such a party were malicious and otherwise fails the destroy the keys, the VDF's sequentiality requirement could be broken.

In contrast, using class groups of binary quadratic forms omits the trusted setup because the order of the class group of a negative prime discriminant d, where $|d| \equiv 3 \bmod 4$, is believed to be difficult to compute when $|d|$ is sufficiently large, making the order of the class group effectively unknown. Therefore, a suitable discriminant — and its associated class group — can be chosen without the need for a trusted setup, which is a major advantage for using class groups in applications requiring groups of unknown order.

The study of class groups is typically presented either in the context of binary quadratic forms or in the context of fractional ideals of algebraic number fields.[2] The ideal class group of an algebraic number field K is the quotient group J_K/P_K, where J_K is the group of fractional ideals of the ring of integers, O_K, of K, and P_K is its subgroup of principal fractional ideals. While many feel that this provides a more conceptually intuitive introduction to class groups, the representation of elements

[1] Alternatively, RSA keys may be generated by multi-party protocols or by using an RSA modulus for which the prime factors are believed to be lost.

[2] See Appendix 7.3 for definitions of the following terms appearing in this paragraph: algebraic number field, quotient group, fractional ideal, ring of integers, and principal fractional ideal.

of a class group and the implementation of the group operation are best carried out through binary quadratic forms, so in this paper I limit the scope of my discussion to form class groups.

The theorems here will often be presented without proof. Please see the References section for resources containing proofs of the theorems and for additional information about class groups and binary quadratic forms.

2 Background

Throughout this paper, recall that $\mathbb{R}$ represents the set of real numbers, $\mathbb{Z}$ represents the set of integers, and $\mathbb{Q}$ represents the set of rational numbers.

Definition 2.1 (Binary quadratic form)**.** A binary quadratic form is

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

where $a, b, c \in \mathbb{R}$ and a, b, c are not all equal to zero.

We write $f = (a, b, c)$ and call f a *form*. These are the objects that we will be working with throughout this paper.

Definition 2.2 (Integral form)**.** An integral form is a binary quadratic form where $a, b, c \in \mathbb{Z}$.

Integral binary quadratic forms are of key importance in algebraic number theory, and they are the relevant forms to the Chik VDF. The remainder of this handout will focus solely on integral forms.

Definition 2.3 (Content of a form)**.** Denoted by $\text{cont}(f)$, the content of a form is

$$\text{cont}(f) = \gcd(a, b, c)$$

Definition 2.4 (Primitive form)**.** A form f is called primitive if $\text{cont}(f) = 1$.

2.1 Discriminant

Definition 2.5 (Discriminant)**.** The discriminant of a form f is $\Delta(f) = b^2 - 4ac$.

One can easily check that if $f = (a, b, c)$ is an integral form, then b and $\Delta(f)$ always share the same parity, i.e. $b \equiv \Delta(f) \bmod 2$.

Note that because the square of an integer is always congruent to 0 or 1 mod 4, the discriminant of an integral binary quadratic form is always congruent to 0 or 1 mod 4.[3]

Further, any integer which is congruent to 0 or 1 mod 4 is the discriminant of a binary quadratic form. This is easy to see by considering the form

[3]Every integer is congruent to 0, 1, 2, or 3 mod 4. Therefore, every square of an integer is congruent to 0, 1, 4, or 9 mod 4, but because 4 and 9 are congruent to 0 and 1 mod 4 respectively, every square is therefore congruent to 0 or 1 mod 4.

$$\left(1,\ d \bmod 4, \frac{(d \bmod 4)-d}{4}\right)$$

For $d \equiv 0$ or $1 \bmod 4$, observe that this form will always be integral, and its discriminant, $\Delta(f)$, is equal to d. We then have the following theorem.

Theorem 2.1. *Given $\Delta \in \mathbb{Z}$, there is at least one integer binary quadratic form with discriminant Δ if and only if $\Delta \equiv 0$ or $1 \bmod 4$.*

Definition 2.6 (Fundamental discriminant)**.** For $\Delta \in \mathbb{Z}$, Δ is a fundamental discriminant if and only if:

1. $\Delta \equiv 1 \bmod 4$ and Δ is square-free,[4] or
2. $\Delta \equiv 0 \bmod 4$, $\frac{\Delta}{4} \equiv 2, 3 \bmod 4$, and $\frac{\Delta}{4}$ is square-free

Fundamental discriminants are exactly those values which are discriminants of quadratic fields.[5]

Definition 2.7 (Positive semi-definite binary quadratic form)**.** A binary form is called positive semi-definite if for any $(x, y) \in \mathbb{R}^2$ with $(x, y) \neq (0, 0)$, the value $f(x, y)$ is non-negative, i.e. $f(x, y) \geq 0$.

Definition 2.8 (Negative semi-definite binary quadratic form)**.** A binary form is called negative semi-definite if for any $(x, y) \in \mathbb{R}^2$ with $(x, y) \neq (0, 0)$, the value $f(x, y)$ is non-positive, i.e. $f(x, y) \leq 0$.

Definition 2.9 (Positive definite binary quadratic form)**.** A binary form is called positive definite if for any $(x, y) \in \mathbb{R}^2$ with $(x, y) \neq (0, 0)$, the value $f(x, y)$ is positive, i.e. $f(x, y) > 0$.

Definition 2.10 (Negative definite binary quadratic form)**.** A binary form is called negative definite if for any $(x, y) \in \mathbb{R}^2$ with $(x, y) \neq (0, 0)$, the value $f(x, y)$ is negative, i.e. $f(x, y) < 0$.

Definition 2.11 (Indefinite binary quadratic form)**.** A binary form is called indefinite if for any $(x, y) \in \mathbb{R}^2$ with $(x, y) \neq (0, 0)$, the value $f(x, y)$ takes on both positive and negative values.

The forms relevant to the Chik VDF are positive definite forms. Therefore we take note of the following theorem.

Theorem 2.2. *A form f is positive definite if and only if $\Delta(f) < 0$ and $a > 0$.*

[4] A square-free integer is one which is not divisible by any perfect squares, i.e. there are no repeated factors in its prime decomposition.

[5] See Appendix 7.3 for the definition of quadratic field.

2.1.1 A brief detour to build intuition about discriminants

The quantity $b^2 - 4ac$ should look familiar. You likely first saw it as the content under the square root in the quadratic formula,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Recall that the quadratic formula helps us solve single-variable quadratic equations that are too difficult to factor, giving the two roots of the associated single-variable quadratic expression. If we set the expression equal to y and consider the represented curve, the roots are the points in the plane where the curve touches the x-axis.

In the quadratic formula, what happens when $b^2 - 4ac = 0$? The square root reduces to zero, and we are left with $x = \frac{-b}{2a}$. Hence, there is only one (repeated) root. Graphically, this is the case in which the curve grazes the x-axis at a single point. Relative to binary quadratic forms, these discriminants correspond to those semi-definite binary quadratic forms for which $f(x, y) = 0$ for some $(x, y) \neq (0, 0)$. (See definitions 2.7 and 2.8 and Figure 1.)

When $b^2 - 4ac < 0$, the quantity under the square root is negative and the roots are complex. Therefore, the curve has no roots on the real x-axis and the x-axis is never crossed. This gives a curve which is entirely positive or entirely negative. These cases analogously correspond to the definite binary quadratic forms. (See definitions 2.9 and 2.10 and Figure 1.)

Finally, when $b^2 - 4ac > 0$, two real roots exist, and the curve crosses the x-axis at two points, leading to at least one positive and at least one negative value along the curve. These cases analogously correspond to indefinite binary quadratic forms. (See definition 2.11 and Figure 1.)

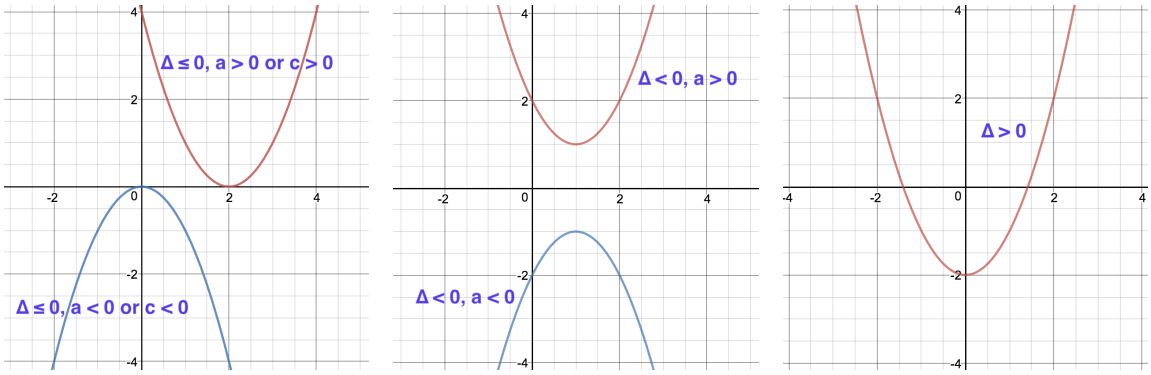


Figure 1: Analogous correspondences between binary quadratic forms (purple text) and single-variable quadratic curves (blue and red curves).

2.2 Matrix representations of forms

Definition 2.12 (Matrix of a form)**.** The matrix of a form $f = (a, b, c)$ is

$$M(f) = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

with $\det(M(f)) = ac - \frac{b^2}{4}$.

Using its matrix form, and defining

$$X = \begin{pmatrix} x & y \end{pmatrix}$$

$f(x, y)$ can be written as

$$\begin{aligned} f(x,y) &= X\ M(f)X^\top \\ &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= ax^2 + bxy + cy^2 \end{aligned}$$

The discriminant of f is given by

$$\begin{aligned} \Delta(f) &= -4\ \det(M(f)) \\ &= b^2 - 4ac \end{aligned}$$

2.3 Representation of integers

Consider the equation

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

where $n \in \mathbb{Z}$ and $f = (a, b, c)$ is an integral binary quadratic form.

Definition 2.13 (A representation of n by f)**.** For a given f and n, a solution $(x, y) \in \mathbb{Z}^2$ to the above equation is called a representation of n by f.

Definition 2.14 (A proper representation of n by f)**.** For a given f and n, a solution $(x, y) \in \mathbb{Z}^2$ to the above equation, such that $\gcd(x, y) = 1$, is called a proper representation of n by f.

Notice that we can restrict our representation considerations to primitive forms. This is because if the content of f is $k \neq 1$, i.e. $gcd(a, b, c) = k$ for some $k \neq 1$ such that, say, $a = kA$, $b = kB$, and $c = kC$, then we could factor out k from the lefthand side of the equation, which would mean that n, on the righthand side, is also divisible by k.

Theorem 2.3. *If $\Delta(f) < 0$ and if $n \in \mathbb{Z}$, then the equation $ax^2 + bxy + cy^2 = n$ has only finitely many solutions, and x and y are bounded by*

$$x^2 \leq \tfrac{4cn}{|\Delta|} \qquad \text{and} \qquad y^2 \leq \tfrac{4an}{|\Delta|}$$

To find all of the solutions to such an equation where $\Delta(f) < 0$ and $n \in \mathbb{Z}$, one could test for each solution (x, y) which obeys the constraints given above.

Example 2.1. *Solve the equation*

$$2x^2 + xy + 3y^2 = 18.$$

Notice that

$$\begin{aligned}\Delta(f) &= b^2 - 4ac \\ &= 1^2 - 4(2)(3) \\ &= -23\end{aligned}$$

Therefore

$$x^2 \leq \tfrac{4(3)(18)}{|-23|} = \tfrac{216}{23} \approx 9.391... \qquad \textit{and} \qquad y^2 \leq \tfrac{4(2)(18)}{|-23|} = \tfrac{144}{23} \approx 6.261...$$

And so

$$|x| \leq 3 \qquad \textit{and} \qquad |y| \leq 2$$

Testing all pairs of (x, y) which satisfy those constraints, we find that the representations of 18 by $f = (2, 1, 3)$ are $(-3, 0)$, $(-3, 1)$, $(3, -1)$, and $(3, 0)$. □

3 Equivalence

This section covers equivalence between forms. If two forms are equivalent then they represent the same integers, although the inverse is not necessarily true. There are two types of equivalence: wide equivalence and proper equivalence.

Definition 3.1 (Wide equivalence)**.** Two forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are widely equivalent if there is an invertible change of variables

$$x' = rx + sy, \quad y' = tx + uy$$

with $r, s, t, u \in \mathbb{Z}$ and $ru - st = \pm 1$, such that

$$a(x')^2 + bx'y' + c(y')^2 = Ax^2 + Bxy + Cy^2$$

or, in other words, $g(x, y) = f(rx + sy, tx + uy)$.

Definition 3.2 (Proper equivalence)**.** Two forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are properly equivalent if the wide equivalence conditions hold and also $ru - st = +1$.

Given these definitions, a change of variables of a wide equivalence relation can be represented by a matrix[6]

[6]See Appendix 7.1 for definitions of $GL(2, \mathbb{Z})$ and $SL(2, \mathbb{Z})$.

$$T = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL(2, \mathbb{Z})$$

and a change of variables of a proper equivalence relation can be represented by the matrix

$$U = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL(2, \mathbb{Z})$$

In either case, we can write

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

to describe the change of variables. The invertibility requirement of the change of variables is what imposes the constraint that $ru - st = \pm 1$ (in the case of wide equivalence, or $ru - st = +1$ in the case of proper equivalence) because only those 2×2 matrices whose determinant is equal to ± 1 are invertible.

We will restrict our discussion to proper equivalence. What follows does not necessarily generalize to wide equivalence, and in particular to cases where the matrix is in $GL(2, \mathbb{Z}) \setminus SL(2, \mathbb{Z})$.

We can express form equivalence and the change of variables using the matrix representation of forms, i.e. $M(f) = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$.

Suppose that two forms $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = Ax^2 + Bxy + Cy^2$ are properly equivalent. Then we have

$$\begin{aligned} g(x, y) &= \begin{pmatrix} x & y \end{pmatrix} M(g) \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} \; U^\top \; M(f) \; U \begin{pmatrix} x \\ y \end{pmatrix} \end{aligned}$$

Therefore, $M(g) = U^\top \; M(f) \; U$.

Further, observe that

$$\begin{aligned} f\left(\begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right) &= f(rx + sy, tx + uy) \\ &= a(rx + sy)^2 + b(rx + sy)(tx + uy) + c(tx + uy)^2 \end{aligned}$$

For ease of notation, define $(fU)(x, y) = f\left(\begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right)$, and note that

$$M(fU) = U^\top \; M(f) \; U$$

We can then state a second definition for proper equivalence as the following.

Definition 3.3 (Proper equivalence)**.** Two forms f and g are properly equivalent if $g = fU$ for some $U \in SL(2,\mathbb{Z})$. The $SL(2,\mathbb{Z})$-orbit of a form is called the proper equivalence class of that form.[7]

Notice that because $SL(2,\mathbb{Z})$ is a group (and associative under matrix multiplication), equivalence is transitive. To see this, consider three forms $f(x,y)$, $g(x,y)$, and $h(x,y)$, and let $g = fU$ and $h = gV$, where $U, V \in SL(2,\mathbb{Z})$. Then

$$\begin{aligned} M(h) &= V^\top \; M(g) \; V \\ &= V^\top \; U^\top \; M(f) \; U \; V \\ &= W^\top \; M(f) \; W \end{aligned}$$

where $W = UV \in SL(2,\mathbb{Z})$ and $W^\top = V^\top U^\top \in SL(2,\mathbb{Z})$. Therefore $h = fW$, where $W \in SL(2,\mathbb{Z})$.

4 The class group

We can now say a bit more about the connection between ideal class groups and form class groups.

Take a negative discriminant Δ and let $F(\Delta)$ be the set of primitive positive definite binary quadratic forms $ax^2 + bxy + cy^2$ whose discriminant is Δ. Define a proper equivalence relation $\sim$ on $F(\Delta)$ such that $f \sim g$ when $g = fU$ for $U \in SL(2,\mathbb{Z})$. This breaks up $F(\Delta)$ into a set of equivalence classes, $C(\Delta) = F(\Delta)/\sim$.

Now consider a quadratic extension field $K = \mathbb{Q}(\sqrt{d})$, where d is square-free.[8] If $d \equiv 1 \bmod 4$, then the discriminant of K is $\Delta = d$. Otherwise, the discriminant of K is $\Delta = 4d$. Let O_K be the ring of integers of K, and let J_K be the group of fractional ideals of the ring of integers O_K. P_K is the subgroup of J_K consisting of principal fractional ideals. We define the ideal class group of K as the quotient group $Cl(K) = J_K/P_K$.

The connection between these two types of class groups — and therefore between binary quadratic forms and ideals in quadratic fields — involves bijections between special versions of each type of class group, the details of which depend upon whether the discriminant in question is positive or negative.[9] For a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ with discriminant $\Delta_K > 0$, there is a bijection between the narrow ideal class group of K and the form class group of primitive integral binary quadratic forms of discriminant Δ_K.[10] And for an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with discriminant $\Delta_K < 0$, there is a bijection between the ideal class group of K and the form class group of primitive positive-definite integral binary quadratic forms of discriminant Δ_K.

[7] See Appendix 7.2 for discussion on orbits. Essentially, this statement means that the proper equivalence class of a form is the set of all forms given by computing $U^\top M(f)\; U$ for all of the $U \in SL(2,\mathbb{Z})$.

[8] See Appendix 7.3 for definitions of the following terms in this paragraph: quadratic extension field, ring of integers, fractional ideal, principal fractional ideal, quotient group.

[9] A bijection is a mapping that is both injective and surjective; in other words, every element in the mapping's codomain is mapped to by exactly one element in the mapping's domain.

[10] The narrow ideal class group is such that P_K^+, the group of totally positive principal fractional ideals of K, is used instead of P_K in the class group quotient group.

5 Reduction

This section introduces normal forms and reduced forms and give algorithms for normalization and reduction.

5.1 Normal forms

Definition 5.1 (Normal form)**.** A form $f = (a, b, c)$ is called normal if $-a < b \leq a$.

Definition 5.2 (Normalization operator)**.** We define the normalization operator $\eta(f)$ as

$$\begin{aligned}\eta(f) &= \eta(a, b, c) \\ &= (a, b + 2ra, ar^2 + br + c)\end{aligned}$$

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

For $f = (a, b, c)$ with $\Delta(f) < 0$ and $a > 0$, let $f_{\text{norm}} = (a', b', c')$ be the normalized form of f. Then $f_{\text{norm}} = \eta(f)$.

Notice that $f = (a, b, c)$ and $f_{\text{norm}} = (a', b', c')$ are in the same proper equivalence class by Definition 3.3 with matrix

$$U = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$$

5.1.1 Normalization algorithm

Given a primitive positive definite form $f = (a, b, c)$, such that $\Delta < 0$ and $a > 0$, the normalization algorithm is:

1. Compute $r = \left\lfloor \frac{a-b}{2a} \right\rfloor$.
2. Set $\eta(f) = (a, b + 2ra, ar^2 + br + c)$, and update $f = \eta(f)$.
3. Return f, which is now normalized.

Example 5.1. *Normalize the form $f = (11, 49, 55)$. Note that it is not normal because $b > a$.*

First compute r:

$$
\begin{aligned}
r &= \left\lfloor \frac{a-b}{2a} \right\rfloor \\
&= \left\lfloor \frac{11-49}{2(11)} \right\rfloor \\
&= \left\lfloor -1.\overline{72} \right\rfloor \\
&= -2
\end{aligned}
$$

Then compute $\eta(f)$:

$$
\begin{aligned}
\eta(f) &= \eta(a,b,c) \\
&= (a, b+2ra, ar^2+br+c) \\
&= (11, 49+2(-2)(11), 11(-2)^2+49(-2)+55) \\
&= (11,5,1)
\end{aligned}
$$

And so the normalization of $f=(11,49,55)$ is $f_{norm}=(11,5,1)$. $\square$

Note that in Example 5.1 the discriminant of both f and f_{norm} is -19. Normalizing a form does not change its discriminant.

5.2 Reduced forms

Definition 5.3 (Reduced form)**.** A positive definite form $f=(a,b,c)$ is called reduced if it is normal and $a \leq c$, and if $a=c$ then $b \geq 0$.

Reduction of forms is important to the Chik VDF because frequently reducing $f(a,\ b,\ c)$ as f is repeatedly squared keeps a, b, and c from growing too large and because reduction identifies a canonical group element for each equivalence class.

For any given $\Delta < 0$, each proper equivalence class of binary quadratic forms of that discriminant contains a unique reduced representative. We can therefore know certain properties of a discriminant, such as its class number, by studying only the reduced forms in the class group of that discriminant.

Given a reduced form with $\Delta < 0$, we have

$$
\begin{aligned}
|\Delta| &= 4ac - |b|^2 && (\Delta < 0) \\
&\geq 4a(a) - a^2 && (-a < b \leq a,\ a \leq c) \\
&\geq 3a^2
\end{aligned}
$$

and so

$$
a \leq \sqrt{\tfrac{|\Delta|}{3}}
$$

Therefore, for a given $\Delta < 0$, there are finitely many a, and consequently there are finitely many b and c.[11] This means that negative discriminants have a finite number of reduced forms and therefore have a finite number of equivalence classes.

Theorem 5.1. *Each primitive positive definite form f is properly equivalent to a unique reduced form.*

Definition 5.4 (Principal form of discriminant Δ)**.** Let Δ be a negative integer such that $\Delta \equiv 0, 1 \bmod 4$, i.e. Δ is a negative discriminant. Let $k = \Delta \bmod 2$. Then

$$f = \left(1, k, \tfrac{k^2-\Delta}{4}\right)$$

is the unique reduced form $(1, b, c)$ of discriminant Δ. This particular reduced form is called the principal form of discriminant Δ.

Example 5.2. *Here are examples of principal forms of several discriminants.*

$$\begin{array}{llll} \Delta = -3 & (1,1,1) & \Delta = -4 & (1,0,1) \\ \Delta = -7 & (1,1,2) & \Delta = -8 & (1,0,2) \\ \Delta = -11 & (1,1,3) & \Delta = -15 & (1,1,4) \\ \Delta = -19 & (1,1,5) & \Delta = -20 & (1,0,5) \end{array} \qquad \square$$

Definition 5.5 (Principal class of discriminant Δ)**.** The equivalence class of the principal form of discriminant Δ is called the principal class of discriminant Δ.

The principal class of a discriminant Δ is the identity element of the form class group of Δ with respect to form composition.[12]

Example 5.3. *Consider the discriminant $\Delta = -23$. This discriminant has a total of three equivalence classes of positive definite binary quadratic forms. Therefore its class number is 3. In particular, the three unique reduced representatives of the equivalence classes are*

$$(1,1,6), \quad (2,-1,3), \quad \textit{and} \quad (2,1,3).$$

The principal form is $(1,1,6)$, and therefore this form (as a representative of the principal equivalence class) acts as the identity when composed with other forms with $\Delta = -23$. Every primitive positive definite binary quadratic form with $\Delta = -23$ is properly equivalent to one of the three forms above, and composition in the group boils down to composition between these three forms. $\square$

Definition 5.6 (Reduction operator)**.** Given a form $f = (a, b, c)$, the reduction operator $\rho(f)$ is defined as

$$\begin{aligned} \rho(f) &= \rho(a, b, c) \\ &= (c, -b + 2sc, cs^2 - bs + a) \end{aligned}$$

[11] Because $|b| \leq a$ and $c = \left(\frac{b^2-\Delta}{4a}\right)$.

[12] Form composition is defined in Section 6.

where $s = \left\lfloor \frac{c+b}{2c} \right\rfloor$.

For $f = (a, b, c)$ with $\Delta(f) < 0$ and $a > 0$, let $f_{\text{red}} = (a', b', c')$ be the reduced form of f. Then $f_{\text{red}} = \rho(f)$.

Notice that $\rho(a, b, c)$ is equivalent to $\eta(c, -b, a)$, the normalization of $(c, -b, a)$. Notice, too, that $f = (a, b, c)$ and $f_{\text{red}} = (a', b', c')$ are in the same proper equivalence class by Definition 3.3 with matrix

$$U = \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}$$

5.2.1 Reduction algorithm

Given a form $f = (a, b, c)$ such that $\Delta < 0$ and $a > 0$, the reduction algorithm is:

1. Normalize f and update $f = f_{\text{norm}}$.
2. If f is reduced, return f. If f is not reduced, compute $s = \left\lfloor \frac{c+b}{2c} \right\rfloor$; set $\rho(f) = (c, -b + 2sc, cs^2 - bs + a)$; and update $f = \rho(f)$.
3. Repeat step 2 until a reduced form is produced.

Example 5.4. *Reduce the form $f = (11, 49, 55)$. We first normalize it, which we did in Example 5.1, finding that $f_{norm} = (11, 5, 1)$. Solving Example 5.1 is equivalent to performing step 1 of the reduction algorithm.*

But $f = f_{norm}$ is not yet reduced because $a > c$. We implement the reduction step until we reach a reduced form.

Compute s:

$$\begin{aligned} s &= \left\lfloor \frac{c+b}{2c} \right\rfloor \\ &= \left\lfloor \frac{1+5}{2(1)} \right\rfloor \\ &= \lfloor 3 \rfloor \\ &= 3 \end{aligned}$$

Compute $\rho(f)$:

$$\begin{aligned} \rho(f) &= (c, -b + 2sc, cs^2 - bs + a) \\ &= (1, -5 + 2(3)(1), 1(3)^2 - 5(3) + 11)) \\ &= (1, 1, 5) \end{aligned}$$

This form is reduced and so $(1, 1, 5)$ is the reduced form of $(11, 49, 55)$. Notice that, of course, the discriminant of all three forms, f, f_{norm}, and f_{red}, is -19. □

5.2.2 An upper bound on the number of reduction steps

In considering implementation of the reduction algorithm in the Chik VDF, it is helpful to get a sense of how many steps of the reduction algorithm will be required to produce a reduced form. Here we set an upper bound on that number. This discussion addresses three cases: (i) $a < \frac{\sqrt{|\Delta|}}{2}$, (ii) $\frac{\sqrt{|\Delta|}}{2} \leq a < \sqrt{|\Delta|}$, and (iii) $a \geq \sqrt{|\Delta|}$. At the end of this section is a summary of the results.

Let $f = (a, b, c)$ be a normalized form. By $\Delta(f) = b^2 - 4ac$,

$$c = \frac{b^2 - \Delta(f)}{4a} = \frac{b^2 + |\Delta(f)|}{4a}.$$

If $a < \frac{\sqrt{|\Delta|}}{2}$, then

$$c = \frac{b^2 - \Delta(f)}{4a} = \frac{b^2 + |\Delta(f)|}{4a} \geq \frac{|\Delta(f)|}{4a} > \frac{a^2}{a} = a$$

and so $c > a$ and f is reduced.

Assume that $\frac{\sqrt{|\Delta|}}{2} \leq a < \sqrt{|\Delta|}$ and that f is not reduced. Then either $a > c$, or $a = c$ and $b < 0$.

If $a = c$ and $b < 0$, then by $a = c$ and f is normal, $-c < b < 0$. Therefore

$$0 < c + b < c \Rightarrow 0 < \frac{c+b}{2c} < 1 \Rightarrow \left\lfloor \frac{c+b}{2c} \right\rfloor = 0$$

and so $s = \left\lfloor \frac{c+b}{2c} \right\rfloor = 0$ and a single step of the reduction algorithm will produce the form

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

which is reduced.

Assume instead that $a > c$. Then if $c < \frac{\sqrt{|\Delta|}}{2}$, $\rho(f) = (a', b', c') = (c, -b + 2sc, cs^2 - bs + a)$ is reduced because $a' = c < \frac{\sqrt{|\Delta|}}{2}$ and, as noted above, given a form $f = (a, b, c)$, $a < \frac{\sqrt{|\Delta|}}{2}$ guarantees a reduced form.

So assume now that $a > c$ and $c \geq \frac{\sqrt{|\Delta|}}{2}$. Then $2c \geq \sqrt{|\Delta|}$. Because f is normalized, $|b| \leq a$ and therefore $|b| < \sqrt{|\Delta|}$. Then $-1 < \frac{b}{2c} < 1$, and, noting that $\frac{c+b}{2c} = \frac{1}{2} + \frac{b}{2c}$, we find that $-\frac{1}{2} < \frac{c+b}{2c} < \frac{3}{2}$. Therefore $s = \left\lfloor \frac{c+b}{2c} \right\rfloor$ has one of three possible values: $0, \pm 1$. (Note that in the case of $s = \pm 1$, s has the same sign as b.) Let $\rho(f) = (a', b', c') = (c, -b + 2sc, c - |b| + a)$. If $s = 0$, then $\rho(f) = (c, -b, a)$ which is reduced. In the case of $s = \pm 1$, $\rho(f) = (c, -b + 2sc, c - |b| + a)$. Because f is normalized, it is either the case that $|b| < a$ or $b = a$. If $|b| < a$, then $c - |b| + a > c \Rightarrow c' > a'$ and so $\rho(f)$ is reduced. If $b = a$, then $s = 1$ and $\rho(f) = (c, -a + 2c, c)$. We have assumed here that $c \geq \frac{\sqrt{|\Delta|}}{2}$ and $\sqrt{|\Delta|} > a$, and so $-a + 2c > 0$. Therefore $a' = c'$ and $b' > 0$, and $\rho(f)$ is reduced.

We now find an upper bound on the number of reduction steps needed for the reduction algorithm to produce a reduced form, given an input form $f = (a, b, c)$ with $a \geq \sqrt{|\Delta|}$.

Assume that $a \geq \sqrt{|\Delta|}$. Then, noting that $b^2 \leq a^2$ because f is normalized,

$$c = \frac{b^2 - \Delta(f)}{4a} = \frac{b^2 + |\Delta(f)|}{4a} \leq \frac{a^2 + a^2}{4a} = \frac{a}{2}$$

and so $c \leq \frac{a}{2}$. Therefore, where $\rho(f) = (a', b', c') = (c, -b+2sc, cs^2 - bs + a)$, we find that $a' = c \leq \frac{a}{2}$. If $a' \geq \sqrt{|\Delta|}$, then a second step of the reduction algorithm will find that for $\rho(\rho(f)) = (a'', b'', c'')$, $a'' = c' \leq \frac{a'}{2} \leq \frac{a}{4}$. If $a'' \geq \sqrt{|\Delta|}$, then a third application yields $a''' = c'' \leq \frac{a''}{2} \leq \frac{a'}{4} \leq \frac{a}{8}$. And so on. This gives an upper bound of $\log_2\left(\frac{a}{\sqrt{|\Delta|}}\right) + 1$ reduction algorithm steps needed to produce a form such that its a term is less than $\sqrt{|\Delta|}$. Then, as shown above, one additional step of the reduction algorithm will yield a reduced form. Therefore, given a form $f = (a, b, c)$, a maximum number of $\log_2\left(\frac{a}{\sqrt{|\Delta|}}\right) + 2$ steps will be required to produce a reduced form.

In summary, if $f = (a, b, c)$ is a normalized form, then

- If $a < \frac{\sqrt{|\Delta|}}{2}$, then f is reduced.
- If $\frac{\sqrt{|\Delta|}}{2} \leq a < \sqrt{|\Delta|}$, then $\rho(f)$ is reduced.
- If $a \geq \sqrt{|\Delta|}$, then a maximum of $\log_2\left(\frac{a}{\sqrt{|\Delta|}}\right) + 2$ steps will be required to produce a reduced form.

6 Composition

Originally developed by Gauss, composition of binary quadratic forms is a commutative operation on the class group. Others, such as Arndt, Dirichlet, and Bhargava, have contributed to the topic, and various algorithms have been developed for its implementation. In this section I motivate and outline the details of composition, and then I lay out the basic structure of the algorithm.

6.1 Explaining composition

To begin, note that we only perform composition between forms which have the same discriminant. This should make sense because we are operating within the class group of a particular discriminant, and although the objects we are operating on are integer 3-tuples, (a, b, c), which represent binary quadratic forms, the more abstract objects being operated upon are the equivalence classes of the class group. Analogously, when we add the rational numbers $\frac{20}{12}$ and $\frac{5}{35}$, what we are fundamentally working with are the fraction equivalence classes whose "reduced representatives" are $\frac{5}{3}$ and $\frac{1}{7}$.

To understand the basic idea behind composition, consider two binary quadratic forms

$$f_1 = ax_1^2 + bx_1y_1 + cy_1^2 \quad \text{and} \quad f_2 = \alpha x_2^2 + \beta x_2y_2 + \gamma y_2^2$$

Note that we consider (x_1, y_1) and (x_2, y_2) as independent sets of variables.

We then would like to find a form f_3 such that

$$f_1 f_2 = f_3$$

Multiplying f_1 and f_2, we find that

$$f_1 f_2 = a\alpha x_1^2 x_2^2 + a\beta x_1^2 x_2 y_2 + a\gamma x_1^2 y_2^2 + b\alpha x_1 y_1 x_2^2 + b\beta x_1 y_1 x_2 y_2 + b\gamma x_1 y_1 y_2^2 + c\alpha y_1^2 x_2^2 + c\beta y_1^2 x_2 y_2 + c\gamma y_1^2 y_2^2$$

We want the righthand side of the equation to resemble a binary quadratic form such that

$$f_1 f_2 = AX^2 + BXY + CY^2 = f_3$$

for some A, B, $C \in \mathbb{Z}$.

We do this by using a change of variables such that X and Y are linear combinations of x_1x_2, x_1y_2, y_1x_2, and y_1y_2:

$$X = jx_1x_2 + kx_1y_2 + ly_1x_2 + my_1y_2, \quad Y = rx_1x_2 + sx_1y_2 + ty_1x_2 + uy_1y_2$$

for some $j, k, l, m, r, s, t, u \in \mathbb{Z}$. The goal of our algorithm is to find A, B, and C by finding appropriate integer values for j, k, l, m, r, s, t, u.

We find j, k, l, m, r, s, t, u as follows. Define $g = \frac{1}{2}(b+\beta)$ and $h = -\frac{1}{2}(b-\beta)$. Define $w = \gcd(a, \alpha, g)$. Then define the matrix

$$M = \begin{pmatrix} j & k & l & m \\ r & s & t & u \end{pmatrix}$$

with submatrices

$$M_1 = \begin{pmatrix} j & k \\ r & s \end{pmatrix}, \quad M_2 = \begin{pmatrix} j & l \\ r & t \end{pmatrix}, \quad M_3 = \begin{pmatrix} j & m \\ r & u \end{pmatrix},$$

$$\mathrm{M}_4 = \begin{pmatrix} k & l \\ s & t \end{pmatrix}, \quad M_5 = \begin{pmatrix} k & m \\ s & u \end{pmatrix}, \quad M_6 = \begin{pmatrix} l & m \\ t & u \end{pmatrix}$$

Set the values j, r, s, t, and u to be

$$j = w, \quad r = 0, \quad s = \tfrac{a}{w}, \quad t = \tfrac{\alpha}{w}, \quad u = \tfrac{g}{w}$$

and find k, l, and m using the following set of conditions:

1. $\det(M_4) = kt - ls = h$
2. $\det(M_5) = ku - ms = \gamma$
3. $\det(M_6) = lu - mt = c$

To solve this set of equations, we create an augmented matrix and row reduce.

$$\left(\begin{array}{ccc|c} t & -s & 0 & h \\ u & 0 & -s & \gamma \\ 0 & u & -t & c \end{array}\right) \leftarrow\!\!\lrcorner \quad \Rightarrow \quad \left(\begin{array}{ccc|c} t & -s & 0 & h \\ 0 & u & -t & c \\ u & 0 & -s & \gamma \end{array}\right) \begin{array}{l} \\ \\ \end{array} \begin{array}{l} \cdot 1/t \\ \cdot 1/u \\ \end{array}$$

$$\Rightarrow \left(\begin{array}{ccc|c} 1 & -s/t & 0 & h/t \\ 0 & 1 & -t/u & c/u \\ u & 0 & -s & \gamma \end{array}\right) \begin{array}{l} \leftarrow\!\!\lrcorner^{+} \\ \lrcorner_{s/t} \\ \end{array} \quad \Rightarrow \quad \left(\begin{array}{ccc|c} 1 & 0 & -s/u & (hu+cs)/tu \\ 0 & 1 & -t/u & c/u \\ u & 0 & -s & \gamma \end{array}\right) \begin{array}{l} \lrcorner^{-u} \\ \\ \leftarrow\!\!\lrcorner_{+} \end{array}$$

$$\Rightarrow \left(\begin{array}{ccc|c} 1 & 0 & -s/u & (hu+cs)/tu \\ 0 & 1 & -t/u & c/u \\ 0 & 0 & 0 & \gamma - (hu+cs)/t \end{array}\right)$$

In order for this matrix to have solutions, it must be the case that $\gamma-(hu+cs)/t=0$.[13] Let's check to see if $\gamma-\frac{hu+cs}{t}\stackrel{?}{=}0$:

$$\begin{aligned}
\gamma-\frac{hu+cs}{t} &= \gamma-\frac{h\frac{g}{w}+c\frac{a}{w}}{\frac{\alpha}{w}} \\
&= \gamma-\frac{gh+ac}{\alpha} \\
&= \gamma-\frac{\left(\frac{1}{2}(b+\beta)\right)\left(-\frac{1}{2}(b-\beta)\right)+ac}{\alpha} \\
&= \gamma-\frac{\left(-\frac{1}{4}b^2+\frac{1}{4}\beta^2\right)+ac}{\alpha} \\
&= \frac{1}{\alpha}\left(\alpha\gamma+\frac{1}{4}b^2-\frac{1}{4}\beta^2-ac\right) \\
&= \frac{1}{4\alpha}\left(4\alpha\gamma+b^2-\beta^2-4ac\right) \\
&= \frac{1}{4\alpha}\left(\left(b^2-4ac\right)-\left(\beta^2-4\alpha\gamma\right)\right) \\
&= \frac{1}{4\alpha}(0) \qquad [\text{ because } \Delta(f_1)=\Delta(f_2)\ ] \\
&= 0 \quad \checkmark
\end{aligned}$$

Therefore, our row-reduced matrix is

$$\left(\begin{array}{ccc|c} 1 & 0 & -s/u & (hu+cs)/tu \\ 0 & 1 & -t/u & c/u \\ 0 & 0 & 0 & 0 \end{array}\right)$$

This matrix corresponds to the following system of equations:

1. $k-\frac{s}{u}m=\frac{hu+cs}{tu}$
2. $l-\frac{t}{u}m=\frac{c}{u}$
3. $0=0$

We can parameterize the system, with ξ as the parameter, and we find that the system has infinite solutions of the following form:

$$k=\tfrac{s}{u}\xi+\tfrac{hu+cs}{tu}, \qquad l=\tfrac{t}{u}\xi+\tfrac{c}{u}, \qquad \text{and} \qquad m=\xi$$

We need to choose a form of ξ such that k, l, and m are integers.

Putting ξ in terms of k, we have

$$\xi=\tfrac{tuk-hu-cs}{st}$$

To ensure that the fraction on the righthand side is an integer, we solve the congruence[14]

[13] Note that because the reduced binary quadratic forms relevant to Chik are positive definite forms, $a>0$, and so $t\neq 0$.

[14] See Appendix 7.4 for one method of solving a congruence of this form.

$$(tu)k \equiv hu + sc \mod st$$

which produces a set of solutions of the form $k = \mu + \nu n$, where $\mu, \nu \in \mathbb{Z}$ and n ranges over all of $\mathbb{Z}$. Any choice of n will yield integer values for k and m, but some n values may produce a non-integer value for l, so we now find an appropriate n value which guarantees $l \in \mathbb{Z}$. Putting l in terms of n, we have

$$\begin{aligned} l &= \frac{t}{u}\xi + \frac{c}{u} \\ &= \frac{tk - h}{s} \\ &= \frac{t(\mu + \nu n) - h}{s} \\ &= \frac{(t\nu)n + (t\mu - h)}{s} \end{aligned}$$

We want the fraction on the righthand side to equal an integer, so we solve the congruence

$$(t\nu)n \equiv h - t\mu \mod s$$

which gives a set of solutions of the form $n = \lambda + \sigma n'$, where $\lambda, \sigma \in \mathbb{Z}$ and n' ranges over all of $\mathbb{Z}$. We choose $n' = 0$ and let $n = \lambda$.

We can now find k, l, and m by

$$k = \mu + \nu\lambda, \qquad l = \tfrac{kt-h}{s}, \qquad \text{and} \qquad m = \tfrac{tuk-hu-cs}{st}$$

and these values are guaranteed to be integers. Notice that because $s = \frac{a}{w}$ and $t = \frac{\alpha}{w}$, and because a and α are never equal to 0, it will always be the case that $s, t \neq 0$, and so k, l, and m will always be defined.

Finally, $f_3 = AX^2 + BXY + CY^2$ is given by[15]

$$A = st - ru, \qquad B = (ju + mr) - (kt + ls), \qquad C = kl - jm$$

To verify that f_3 indeed equals $f_1 f_2$, expand f_3 using $X = jx_1x_2 + kx_1y_2 + ly_1x_2 + my_1y_2$ and $Y = rx_1x_2 + sx_1y_2 + ty_1x_2 + uy_1y_2$. After grouping together common terms, we end up with:

$$\begin{aligned} f_3 = {} & (Aj^2 + Bjr + Cr^2)x_1^2x_2^2 + (2Ajk + B(js + kr) + 2Crs)x_1^2x_2y_2 \\ & + (Ak^2 + Bks + Cs^2)x_1^2y_2^2 + (2Ajl + B(jt + lr) + 2Crt)x_1y_1x_2^2 \\ & + (2A(jm + kl) + B(ju + kt + ls + mr) + 2C(ru + st))x_1y_1x_2y_2 \\ & + (2Akm + B(ku + ms) + 2Csu)x_1y_1y_2^2 + (Al^2 + Blt + Ct^2)y_1^2x_2^2 \\ & + (2Alm + B(lu + mt) + 2Ctu)y_1^2x_2y_2 + (Am^2 + Bmu + Cu^2)y_1^2y_2^2 \end{aligned}$$

We then wish to check that the above expansion of f_3 is equal to

$$\begin{aligned} f_1f_2 = {} & a\alpha x_1^2x_2^2 + a\beta x_1^2x_2y_2 + a\gamma x_1^2y_2^2 + b\alpha x_1y_1x_2^2 + b\beta x_1y_1x_2y_2 \\ & + b\gamma x_1y_1y_2^2 + c\alpha y_1^2x_2^2 + c\beta y_1^2x_2y_2 + c\gamma y_1^2y_2^2 \end{aligned}$$

The reader may check for coefficient equality for all terms, but here I will confirm coefficient equality for two of the terms:

[15] Although $r = 0$, I present these formulae with the r terms to gesture to their inherent symmetry. In the composition algorithm given in Section 6.1.1. instances of r are removed for efficiency.

1. $(Aj^2 + Bjr + Cr^2)x_1^2x_2^2 \stackrel{?}{=} a\alpha x_1^2x_2^2$
   $\Rightarrow Aj^2 + Bjr + Cr^2 \stackrel{?}{=} a\alpha$
2. $(2Alm + B(lu + mt) + 2Ctu)y_1^2x_2y_2 \stackrel{?}{=} c\beta y_1^2x_2y_2$
   $\Rightarrow 2Alm + B(lu + mt) + 2Ctu \stackrel{?}{=} c\beta$

We draw from the definitions for A, B, C, g, h, w, j, r, s, t, and u, and from the identities defined by the three conditions on k, l, and m.

To check the first equality, $Aj^2 + Bjr + Cr^2 \stackrel{?}{=} a\alpha$:

$$\begin{aligned}
Aj^2 + Bjr + Cr^2 &= (st - ru)j^2 + ((ju + mr) - (kt + ls))jr + (kl - jm)r^2 \\
&= (st - 0)j^2 + ((ju + mr) - (kt + ls))0 + (kl - jm)0 \\
&= stj^2 \\
&= \frac{a}{w}\frac{\alpha}{w}w^2 \\
&= a\alpha \quad \checkmark
\end{aligned}$$

To check the second equality, $2Alm + B(lu + mt) + 2Ctu \stackrel{?}{=} c\beta$:

$$\begin{aligned}
2Alm + B(lu + mt) + 2Ctu &= 2(st - ru)lm + ((ju + mr) - (kt + ls))(lu + mt) + 2(kl - jm)tu \\
&= 2lmst - 2lmru + jlu^2 + jmtu + lmru + m^2rt - kltu - kmt^2 \\
&\quad - l^2su - lmst + 2kltu - 2jmtu \\
&= lmst - lmru + jlu^2 + lmru + m^2rt - kmt^2 - l^2su + kltu - jmtu \\
&= lmst - 0 + jlu^2 + 0 + 0 - kmt^2 - l^2su + kltu - jmtu \\
&= lmst + jlu^2 - kmt^2 - l^2su + kltu - jmtu \\
&= (kltu - kmt^2 - l^2su + lmst) + jlu^2 - jmtu \\
&= (kt - ls)(lu - mt) + jlu^2 - jmtu \\
&= (kt - ls)(lu - mt) + ju(lu - mt) \\
&= (kt - ls)c + juc \\
&= hc + juc \\
&= hc + w\frac{g}{w}c \\
&= c(h + g) \\
&= c\left(\frac{1}{2}(b + \beta) - \frac{1}{2}(b - \beta)\right) \\
&= c\beta \quad \checkmark
\end{aligned}$$

The reader may similarly verify the equality of the other coefficients, and therefore we confirm that $f_3 = f_1f_2$.

There are several notes to make about this construction.

The first, and most important, is that the system of equations defining $k, l,$ and m has infinite solutions. However, all of the solutions are in the same equivalence class, and they will each reduce to the same binary quadratic form.

Second, we have the observation that if we wish to reconstruct f_1 and f_2 from g, h, w, j, k, l, m, r, s, t, and u, we note that $\det(M_1)$ and $\det(M_2)$ recover a and α respectively, $\det(M_3) - \det(M_4)$ and $\det(M_3) + \det(M_4)$ recover b and β respectively, and $\det(M_6)$ and $\det(M_5)$ recover c and γ respectively.[16] So f_1 and f_2 can be represented using the determinants of the six submatrices of M:

$$\begin{aligned}
f_1 &= ax_1^2 + bx_1y_1 + cy_1^2 \\
&= (js - kr)x_1^2 + ((ju - mr) - (kt - ls))x_1y_1 + (lu - mt)y_1^2 \\
&= \det(M_1)\, x_1^2 + (\det(M_3) - \det(M_4))\, x_1y_1 + \det(M_6)\, y_1^2 \\
f_2 &= \alpha x_2^2 + \beta x_2y_2 + \gamma y_2^2 \\
&= (jt - lr)x_2^2 + ((ju - mr) + (kt - ls))x_2y_2 + (ku - ms)y_2^2 \\
&= \det(M_2)\, x_2^2 + (\det(M_3) + \det(M_4))\, x_2y_2 + \det(M_5)\, y_2^2
\end{aligned}$$

6.1.1 The composition algorithm

Given $f_1 = (a, b, c)$ and $f_2 = (\alpha, \beta, \gamma)$, the composition algorithm for $f_1 f_2 = f_3$ is as follows[a]:

1. Set $g = \frac{1}{2}(b + \beta)$, $h = -\frac{1}{2}(b - \beta)$, and $w = \gcd(a, \alpha, g)$.
2. Set $j = w$, $s = \frac{a}{w}$, $t = \frac{\alpha}{w}$, and $u = \frac{g}{w}$.
3. Solve $(tu)k \equiv hu + sc \bmod st$, the solutions to which have the form $k = \mu + \nu n$ for all $n \in \mathbb{Z}$.[b] Store μ and ν.
4. Solve $(t\nu)n \equiv h - t\mu \bmod s$, the solutions to which have the form $n = \lambda + \sigma n'$ for all $n' \in \mathbb{Z}$. Store λ.
5. Set $k = \mu + \nu\lambda$, $l = \frac{kt - h}{s}$, and $m = \frac{tuk - hu - cs}{st}$.
6. Set $A = st$, $B = ju - (kt + ls)$, and $C = kl - jm$.
7. Set $f_3 = (A, B, C)$, and return f_3.

[a] Note that because $r = 0$, the variable r does not appear in this algorithm, despite appearing in the explanation of composition in Section 6.1.

[b] See Appendix 7.4 for one method of solving such an equation.

6.2 Composition and representation of integers

Consider a composition

$$f_1 f_2 = f_3$$

[16] Note that recovering b, β, c, and γ uses the three conditions on k, l, and m.

where

$$f_1 = ax_1^2 + bx_1y_1 + cy_1^2, \qquad f_2 = \alpha x_2^2 + \beta x_2y_2 + \gamma y_2^2, \qquad \text{and} \qquad f_3 = AX^2 + BXY + CY^2$$

In Section 2.3, we saw that a binary quadratic form represents certain integers, and a representation of an integer n by a form f is a solution $(x, y) \in \mathbb{Z}^2$ to the equation

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

Recall that if two forms are equivalent then they represent the same integers. If $f_{3,nr}$ is the non-reduced form found by composing f_1 and f_2 using the algorithm in section 6.1, and if, for a given (x_1, y_1) and (x_2, y_2), $f_1(x_1, y_1) = n_1$ and $f_2(x_2, y_2) = n_2$, and if X, Y are defined as they were in section 6.1, then $f_{3,nr}(X, Y) = n_1n_2$. Note that this is not necessarily true for the reduced form $f_{3,r}$, which is found by submitting $f_{3,nr}$ to the reduction algorithm. However, n_1n_2 will be representable by $f_{3,r}$ under some different set of integers (X', Y') because $f_{3,nr}$ and $f_{3,r}$ are in the same equivalence class and therefore represent the same set of integers.

6.3 Squaring

Section 6.1 laid out the general case for composing two primitive positive definite binary quadratic forms. When composing a form with itself, however, many of the steps in the composition algorithm simplify. This is further the case when squaring a form whose discriminant is the negative of a prime number. The Chik VDF restricts its discriminants to negative primes, so in this section I derive the simplified squaring algorithm (assuming a negative prime discriminant) as a special case of the composition algorithm.

Let $f = (a, b, c)$. Applying the composition algorithm, $f = f_1 = (a, b, c)$ and $f = f_2 = (\alpha, \beta, \gamma)$ such that $\alpha = a$, $\beta = b$, and $\gamma = c$.

Step 1 (from the composition algorithm):

1. Set $g = \frac{1}{2}(b + \beta)$, $h = -\frac{1}{2}(b - \beta)$, and $w = \gcd(a, \alpha, g)$.

Because $b = \beta$ and $a = \alpha$, this simplifies to:

1. Set $g = b$, $h = 0$, and $w = \gcd(a, b)$.

In Chia's VDF, $\gcd(a, b) = 1$ in all cases due to the generation method of the discriminant. This is because the discriminant is chosen as the negative of a prime number. We therefore note the following: Let $\Delta = -p$, where p is prime, and $\Delta = b^2 - 4ac$. Let a and b have a common factor n. Then $a = na'$ and $b = nb'$ for some $a', b' \in \mathbb{Z}$, and $\Delta = n(b'b - 4a'c)$. Therefore Δ is divisible by n. But the only factors of Δ are ± 1 and $\pm p$. Because $a, b < |\Delta|$, $a, b < p$. Therefore $n = \pm 1$, and $\gcd(a, b) = 1$. The first composition step thus becomes:

1. Set $g = b$, $h = 0$, and $w = 1$.

Step 2 (from the composition algorithm):

2. Set $j = w$, $s = \frac{a}{w}$, $t = \frac{\alpha}{w}$, and $u = \frac{g}{w}$.

This simplifies to

2. Set $j = 1$, $s = a$, $t = a$, and $u = b$.

Step 3 (from the composition algorithm):

3. Solve $(tu)k \equiv hu + sc \bmod st$, the solutions to which have the form $k = \mu + \nu n$ for all $n \in \mathbb{Z}$. Store μ and ν.

This simplifies to

3. Solve $(ab)k \equiv ac \bmod a^2$, the solutions to which have the form $k = \mu + \nu n$ for all $n \in \mathbb{Z}$. Store μ and ν.

This linear congruence simplifies further because a may be factored out of all three terms. Observe the following proof: Let $ax \equiv b \bmod m$. Let n be a factor of a, b, and m. Then $na'x \equiv nb' \bmod nm'$ for some $a', b', m' \in \mathbb{Z}$, and so nm' divides $na'x - nb'$ and $nm'k = na'x - nb'$ for some $k \in \mathbb{Z}$. Dividing by n, $m'k = a'x - b'$. Therefore m' divides $a'x - b'$ and $a'x \equiv b' \bmod m'$. The third composition step thus becomes:

3. Solve $bk \equiv c \bmod a$, the solutions to which have the form $k = \mu + \nu n$ for all $n \in \mathbb{Z}$. Store μ and ν.

Finally, although the linear congruence has infinite solutions of the form $k = \mu + \nu n$, ranging through all $n \in \mathbb{Z}$, we will see in Step 5 that the term νn is not needed in this algorithm, and therefore we only store μ.

3. Solve $bk \equiv c \bmod a$, the solutions to which have the form $k = \mu + \nu n$ for all $n \in \mathbb{Z}$.[17] Store μ.

Step 4 (from the composition algorithm):

4. Solve $(t\nu)n \equiv h - t\mu \bmod s$, the solutions to which have the form $n = \lambda + \sigma n'$ for all $n' \in \mathbb{Z}$. Store λ.

This simplifies to

4. Solve $(a\nu)n \equiv -a\mu \bmod a$, the solutions to which have the form $n = \lambda + \sigma n'$ for all $n' \in \mathbb{Z}$. Store λ.

As in Step 3, we factor out a, giving

4. Solve $\nu n \equiv -\mu \bmod 1$, the solutions to which have the form $n = \lambda + \sigma n'$ for all $n' \in \mathbb{Z}$. Store λ.

But any two integers are equivalent modulo 1. To see this, let $a, b \in \mathbb{Z}$. Then $a - b \in \mathbb{Z}$ and so 1 divides $a - b$, and the remainder of $a - b$ divided by 1 is 0. Therefore, there is only one equivalence class modulo 1: $[0] = \mathbb{Z}$. Therefore we apply the solution $\{\lambda = 0, \sigma = 0\}$. The fourth composition step thus becomes:

[17] See Appendix 7.4 for one method of solving such an equation.

4. Set $\lambda = 0$.

Step 5 (from the composition algorithm)

5. Set $k = \mu + \nu\lambda$, $l = \frac{kt-h}{s}$, and $m = \frac{tuk-hu-cs}{st}$.

Because $\lambda = 0$, $\nu\lambda = 0$ and $k = \mu$. This is why we did not store ν in Step 3. The expressions for l and m also simplify, giving

5. Set $k = \mu$, $l = \mu$, and $m = \frac{b\mu-c}{a}$.

Step 6 (from the composition algorithm)

6. Set $A = st$, $B = ju - (kt + ls)$, and $C = kl - jm$.

These become

6. Set $A = a^2$, $B = b - 2a\mu$, and $C = \mu^2 - \frac{b\mu-c}{a}$.

Step 7 (from the composition algorithm)

7. Set $f_3 = (A, B, C)$, and return f_3.

Here we simply return f_3, the square of f:

7. Set $f_3 = (A, B, C)$, and return f_3.

Notice that in the interest of efficiency, we may omit steps 1, 2, 4, and 5, which are superfluous. In the following algorithm, we apply these changes.

6.3.1 The squaring algorithm

Here is the completed squaring algorithm, as derived above.[18] This algorithm assumes a discriminant which is the negative of a prime number.

Given a primitive positive definite form $f = (a, b, c)$, the squaring algorithm to find f^2 is as follows:

1. Solve $bk \equiv c \bmod a$, the solutions to which have the form $k = \mu + \nu n$ for all $n \in \mathbb{Z}$.[a] Store μ.
2. Set $A = a^2$, $B = b - 2a\mu$, and $C = \mu^2 - \frac{b\mu-c}{a}$.
3. Return (A, B, C), which is the square of f.

[a] See Appendix 7.4 for one method of solving such an equation.

[18] Notice that here we omit steps 1, 2, 4, and 5 from above. And so step 3 above has become step 1 in the below algorithm, and steps 6 and 7 above have become steps 2 and 3 in the below algorithm.

7 Appendix

7.1 Special matrices

Definition 7.1 ($GL(2,\mathbb{Z})$)**.** $GL(2,\mathbb{Z})$ is the set of all invertible 2×2 matrices with integer entries whose determinants are equal to ± 1.

Definition 7.2 ($SL(2,\mathbb{Z})$)**.** $SL(2,\mathbb{Z})$ is a subgroup of $GL(2,\mathbb{Z})$ defined as the set of all 2×2 matrices with integer entries whose determinants are equal to 1. The two generating matrices of $SL(2,\mathbb{Z})$ are

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

7.2 Orbits

Let S be a non-empty set and let G be a group. A *left action* of G on S is a mapping

$$G \times S \to S, \quad (g, s) \mapsto gs \in S$$

which has the following properties:

- $1_G s = s$ for all $s \in S$
- for $g, h \in G$ and $s \in S$, $g(hs) = (gh)s$

Given a left action of G on S, two elements s and t in S are equivalent if there is an element $g \in G$ such that $t = gs$. This is an equivalence relation on S, and the equivalence class $\{gs : g \in G\}$ is called the G-orbit of s.

We have an analogous definition for a *right action* of a group G on a set S. Given a right action of G on S we define the G-orbit of s in the same way as with left actions.

Orbits should bring to mind ring ideals, gesturing toward the deep connection between ideal class groups and form class groups.

7.3 Ideal class group definitions

Here are various definitions relating to the content about ideal class groups in Section 4. This information is included to acknowledge the relationship between ideal class groups and form class groups, and to satisfy those curious about the topic, but an understanding of this material is not necessary for implementing class group composition of binary quadratic forms.

Definition 7.3 (Algebraic number field)**.** An algebraic number field is a finite extension $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ of $\mathbb{Q}$, where $\alpha_1, ..., \alpha_n$ are algebraic numbers.

Definition 7.4 (Quadratic extension field)**.** A quadratic extension field is an algebraic number field $Q(\sqrt{z})$ of degree 2 over $\mathbb{Q}$, such that $\sqrt{z}$ is the root of some irreducible quadratic equation whose coefficients are in $\mathbb{Z}$.

Definition 7.5 (Ring of integers)**.** The ring of integers of an algebraic number field K is the set of elements in K which are roots of monic polynomials with integer coefficients.

Examples of rings of integers:

- For $K = \mathbb{Q}(i)$, where $i = \sqrt{-1}$, the ring of integers of K is $O_K = \{a + bi \mid a, b \in \mathbb{Z}\}$.
- In general, for $K = \mathbb{Q}(\sqrt{d})$, if $d \equiv 1 \mod 4$, then $O_K = \{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\}$, and if $d \equiv 2, 3 \mod 4$, then $O_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

Definition 7.6 (Ideal)**.** An ideal I of a ring R is an additive subgroup of R which multiplicatively absorbs all elements in R which are outside of I. In other words, for every $x \in R$ and $y \in I$, $xy \in I$ and $yx \in I$.

Examples of ideals:

- In the ring $\mathbb{Z}$, the ideals of $\mathbb{Z}$ have the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$.
- In $\mathbb{Z}_6$ (i.e. the integers modulo 6), the set $I = \{0, 2, 4\}$ is an ideal.

Definition 7.7 (Principal ideal)**.** An ideal I of a ring R is called a (right) principal ideal if there is an element $a \in R$ such that $I = aR = \{ar \mid r \in R\}$. In other words, the ideal is generated by the element a. If R is non-commutative, then R can have left principal ideals, right principal ideals, or two-sided principal ideals, given by (respectively):

- $Ra = \{ra \mid r \in R\}$
- $aR = \{ar \mid r \in R\}$
- $RaR = \{r_1as_1 + ... + r_nas_n \mid r_1, s_1, ..., r_n, s_n \in R\}$

If R is commutative then the three above definitions are equivalent. All rings have principal ideals.

Examples of principal ideals:

- The set of even integers, $2\mathbb{Z}$, is a principal ideal of $\mathbb{Z}$ generated by ± 2.
- In fact, every ideal of the ring of integers $\mathbb{Z}$ is a principal ideal.
- In the ring $\mathbb{Z}(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$, the ideal generated by $\sqrt{-3}$ is a principal ideal.

To define fractional ideals, I first explain modules.

Definition 7.8 (Module)**.** A module M over a ring R is a generalization of a vector space over a field, with the ring elements playing the role of the field scalars. A left R-module, M, is an abelian group $(M, +)$ with a scalar multiplication operation $* : R \times M \to M$ which satisfies the following conditions for all $r, s \in R$ and $m, n \in M$:

- $r * (m + n) = r * m + r * n$
- $(r + s) * m = r * m + s * m$
- $(rs) * m = r * (s * m)$
- $1_R * m = m$

A right R-module is the same as above except the ring R acts on the righthand side of the module instead of on the lefthand side. If R is commutative, then the left and right R-modules are the same and the module is simply called an R-module.

Examples of modules:

- For a field F, the concepts of a vector space over F and an F-module are identical.
- Any ideal I of a ring R is an R-module.

Definition 7.9 (Submodule)**.** If M is a module of a ring R, and S is a subgroup of M, then S is an R-submodule if for any $s \in S$ and any $r \in R$, the product $r * s$ is in S (for a left R-submodule) or the product $s * r$ is in S (for a right R-submodule).

Definition 7.10 (Fractional ideal)**.** Let K be an algebraic number field with ring of integers O_K, and let T_K be some subset of K. T_K is a fractional ideal of O_K if it is a finitely-generated O_K-module such that there exists some nonzero $r \in O_K$ where for all $t \in T_K$, $rt \in O_K$. Moreover, the set $T'_K = rT_K$ is an ideal of O_K, and $T_K = r^{-1}T'_K$.

The element r can be thought of as "clearing the denominator" of all elements in T_K to produce elements in O_K.

Examples of fractional ideals:

- Consider the algebraic number field $\mathbb{Q}$ with ring of integers $\mathbb{Z}$. The subset of $\mathbb{Q}$ defined by $I = \{..., -\frac{15}{7}, -\frac{10}{7}, -\frac{5}{7}, 0, \frac{5}{7}, \frac{10}{7}, \frac{15}{7}, ...\}$ is a fractional ideal of $\mathbb{Z}$, with $\pm 7 \in \mathbb{Z}$ being the element which clears the denominator such that for all $t \in T_K$, $7t \in \mathbb{Z}$.
- In general, fractional ideals in $\mathbb{Q}$ have the form $\{r\mathbb{Z} \mid r \in \mathbb{Q}\}$.
- The set $\mathbb{Q}$ is not a fractional ideal because its elements can have arbitrarily large denominators.

Definition 7.11 (Principal fractional ideal)**.** Given an algebraic number field K and its ring of integers O_K, a principal fractional ideal is a fractional ideal generated by a single element $k \in K$ such that the principal fractional ideal is the set $\{ka \mid a \in O_K\}$.

Given an algebraic number field, K, the set of principal fractional ideals, P_K, is a subgroup of the group of fractional ideals, J_K.

To define quotient groups, I first explain cosets.

Definition 7.12 (Right coset of a subgroup in a group)**.** Let S be a subgroup of a group G. Let $s \in S$, and $g \in G$. The congruence class of g modulo S, i.e. $Sg = \{sg \mid s \in S\}$, is the right coset of S in G.

Definition 7.13 (Left coset of a subgroup in a group)**.** Let S be a subgroup of a group G. Let $s \in S$, and $g \in G$. $gS = \{gs \mid s \in S\}$ is the left coset of S in G.

Definition 7.14 (Quotient group)**.** Let N be a normal subgroup of a group G. Then G/N is the quotient group of G by N, and it denotes the set of all right cosets of N in G. The operation on the group is defined as $(Na)(Nb) = Nab$.[19]

One can think of quotient groups as grouping together similar elements of a larger group into equivalence classes.

Examples of quotient groups:

- Let G be the integers modulo 6 under addition, i.e. $G = \{0, 1, 2, 3, 4, 5\}$, and let N be the subgroup $\{0, 3\}$, noting that N is normal because G is abelian. $G/N = \{g + N \mid g \in G\} = \{\{0, 3\}, \{1, 4\}, \{2, 5\}\} = \{0 + N, 1 + N, 2 + N\}$.
- Let $G = \mathbb{Z}$ and $N = 2\mathbb{Z}$, i.e. G is the set of integers and N is the set of even integers. N is a normal subgroup because G is abelian. $G/N = \{2\mathbb{Z}, 2\mathbb{Z} + 1\}$, with the two cosets being the even and odd integers, respectively.

7.4 Solving linear congruences

In this section, I outline one way of solving linear congruences of the form $ax \equiv b \bmod m$.

First, using the extended Euclidean algorithm, we may find integers d, e, and g such that

$$g = \gcd(a, m) \qquad \text{and} \qquad da + em = g$$

Then note the following theorem:

Theorem 7.1. *The congruence $ax \equiv b \bmod m$ has a solution if and only if $\gcd(a, m)$ divides b.*

If the linear congruence $ax \equiv b \bmod m$ has a solution, then by Theorem 7.1 there exists some $q \in \mathbb{Z}$ such that $qg = b$. Therefore we have

[19] Note that because N is normal, we could have equivalently defined G/N to be the set of all left cosets of N in G.

$$da + em = g \quad \Rightarrow \quad qda + qem = qg \quad \Rightarrow \quad qda + qem = b$$

Taking the last equation mod m, we have

$$aqd \equiv b \bmod m$$

Therefore qd is one solution to the congruence relation. However, the congruence $ax \equiv b \bmod m$ has an infinite set of solutions — these solutions have the form $k = \mu + \nu n$, where μ is $qd \bmod m$, $\nu = \frac{m}{g}$, and n ranges over all of $\mathbb{Z}$. To check these solutions, first note that because $g = \gcd(a, m)$, g divides a and so there exists some $w \in \mathbb{Z}$ such that $a = wg$. Then

$$\begin{aligned} ax &= a(qd + \frac{m}{g}n) \\ &= aqd + a\frac{m}{g}n \\ &= aqd + wmn \\ &\equiv b \bmod m \quad \checkmark \end{aligned}$$

7.4.1 Linear congruence algorithm

The following is an example algorithm for solving a linear congruence of the form $ax \equiv b \bmod m$:

1. Use the extended Euclidean algorithm to find g, d, e, where $g = \gcd(a, m)$ and $da+em = g$.
2. Compute $q = \left\lfloor \frac{b}{g} \right\rfloor$, and set $r = b \ \% \ g$.
3. If $r \neq 0$, return "The congruence has no solution." End algorithm.
4. Else set $\mu = qd \ \% \ m$, and set $\nu = \frac{m}{g}$. Return μ, ν.

The set of solutions of the linear congruence then have the form $x = \mu + \nu n$, where n ranges over all of $\mathbb{Z}$.

References

Boneh, D., Bünz, B., and Fisch, B. A survey of two verifiable delay functions. *Cryptology ePrint Archive*, Report 2018/712, 2018. https://eprint.iacr.org/2018/712.

Buchmann, J. and Vollmer, U. (2007). *Binary quadratic forms: An algorithmic approach.* (Vol. 20, Algorithms and computation in mathematics). Berlin: Springer-Verlag.

Cohen, H. (1993). A course in computational algebraic number theory. (Vol. 138, Graduate texts in mathematics). Berlin: Springer-Verlag.

Granville, A. (2014). Composing quadratic forms: Gauss, Dirichlet and Bhargava. *Pi in the Sky*, **18**, 3-6.

Jacobson, M. J. and van der Poorten, A. J. (2002). Computational aspects of NUCOMP. *Lecture notes in computer science*, *Algorithmic number theory - ANTS-V*, vol. 2369, 120-133. doi:10.1007/3-540-45455-1_10

Jenkins, E. D. (1935). On the composition of quadratic forms. *Bulletin of the American Mathematical Society*, vol. 41, number 10, 719-726.