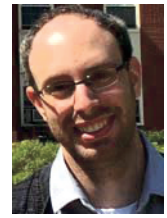
Composition of Binary Quadratic Forms*

Understanding the Approaches of Gauss, Dirichlet and Bhargava

François Séguin

In 2004, Bhargava introduced a new way to understand the composition law of integral binary quadratic forms through what he calls the 'cubes of integers'. The goal of this article is to introduce the reader to Bhargava's cubes and this new composition law, as well as to relate it to the composition law as it is known classically. We will present a historical exposition of the subject, from Gauss to Bhargava, and see how the different formulations of the composition laws are equivalent.



François Séguin received his PhD from Queen's University in 2018. His research interests are in analytic number theory, specifically concerning questions of algebraic nature.

1. Introduction

Binary quadratic forms were already studied in the seventeenth and eighteenth centuries. Originally, the main questions formulated in terms of binary quadratic forms were about the representation of numbers. Given a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$, we can ask which integers n can be written as $n = f(x_0, y_0)$ for some x_0, y_0, in which case f is said to represent n. Given an integer n, we can also ask which binary quadratic forms could represent n. Finally, given such a representation, how many other representations can we find. It is interesting to note that these very questions will eventually come to play a role in subjects such as Diophantine equations, quadratic reciprocity and even class field theory. Mathematicians like Fermat and Euler tried to classify all the possible binary quadratic forms, but the biggest results came from Carl Friedrich Gauss in 1801 in his *Disquisitiones Arithmeticae*. Gauss spells out the underlying structure that those binary quadratic forms have – a structure that

Keywords
Cubes of integers, binary quadratic forms, composition laws.

*DOI: https://doi.org/10.1007/s12045-019-0822-4

In this article, we explore how the composition law came to be understood by Gauss, Dirichlet and finally Bhargava, as well as, see how these different formulations are really equivalent.

later came to be known as a group. What is now known as Gauss composition law for binary quadratic forms has been modernized using algebraic number theory through the works of Dirichlet amongst others. This construction plays a critical role in number theory. In particular, it is one of the primary tools to understand class groups of quadratic number fields.

Recently, Manjul Bhargava formulated a brand new way to approach the composition law for binary quadratic forms. In his thesis [1] and then a series of articles [2–5], Bhargava uses a geometric approach to describe the composition law, giving insight into a new possible way to understand it. Bhargava also generalizes the composition law to other objects, establishing a correspondence with structures in higher degree number fields.

In this article, we will explore how the composition law came to be understood by Gauss, Dirichlet and finally Bhargava, as well as, see how these different formulations are really equivalent. The proofs for most of the propositions we will be presenting are easy exercises, accessible to undergraduate students. We encourage the reader to take them as exercises when possible.

2. Preliminaries

Recently, Manjul Bhargava formulated a brand new way to approach the composition law for binary quadratic forms. Bhargava uses a geometric approach to describe the composition law, giving insight into a new possible way to understand it.

We define a (integral) binary quadratic form as a homogenous degree 2 polynomial in two variables, i.e., of the form:

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

where $a, b, c \in \mathbb{Z}$. Since any binary quadratic form is completely determined by its three coefficients a, b and c, we sometimes denote the above polynomial by (a, b, c).

The *discriminant* of a binary quadratic form (a, b, c) is defined as:

$$\text{Disc}(a, b, c) = b^2 - 4ac.$$

Also, we say that a binary quadratic form is *primitive* if the three coefficients are coprime, i.e., $\gcd(a, b, c) = 1$, and *positive definite* if the binary quadratic form takes only positive values, i.e., $ax^2 + bxy + cy^2 > 0$ for all $x, y \neq 0$.

Proposition 2.1 *The binary quadratic form* (a, b, c) *is positive definite if and only if* $\mathrm{Disc}(a, b, c) < 0$ *and* $a > 0$.

Proof. If $f(x, y) = ax^2 + bxy + cy^2$ is of discriminant D, then

$$4af(x, y) = (2ax + by)^2 - Dy^2.$$

□

From now on, we will use the term binary quadratic forms to mean integral primitive positive definite binary quadratic forms.

Recall that the group $\mathrm{SL}_2(\mathbb{Z})$ is defined as:

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

We define the action of $\mathrm{SL}_2(\mathbb{Z})$ on a binary quadratic form as:

$$(ax^2 + bxy + cy^2) * \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2.$$

Note that this is simply a change of variable. An alternative way of expressing this action is, for $Q(x, y)$ a binary quadratic form and $M \in \mathrm{SL}_2(\mathbb{Z})$,

$$Q(x, y) * M = Q(x', y'),$$

where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}.$$

Example 2.1 The result of the action of the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ on the binary quadratic form (a, b, c) is

$$(a, b, c) * \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = ay^2 - bxy + cx^2 = (c, -b, a).$$

Proposition 2.2 *For any matrix M,*

$$\mathrm{Disc}\,((a,b,c) * M) = \det(M)^2\,\mathrm{Disc}(a,b,c).$$

Proof. Note that for $f(x,y) = ax^2 + bxy + cy^2$ of discriminant D,

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

and

$$\mathrm{Disc}(f(x,y)) = -4 \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix}.$$

Therefore,

$$f(x,y) * M = \begin{pmatrix} x & y \end{pmatrix} M^{\mathrm{T}} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M \begin{pmatrix} x \\ y \end{pmatrix}.$$

and computing the determinant we are done. □

From this Proposition, we can conclude that the action of $\mathrm{SL}_2(\mathbb{Z})$ preserves the discriminant.

We now fix a certain integer D and consider all the possible binary quadratic forms of discriminant D. On this set, we define the following equivalence relation. If Q_1 and Q_2 are binary quadratic forms of discriminant D, then

$$Q_1 \sim Q_2 \quad \text{if and only if} \quad Q_1 * M = Q_2$$

for some $M \in \mathrm{SL}_2(\mathbb{Z})$. We call the set of equivalence classes under this relation G_D, i.e.,

$$G_D = \{(a,b,c) : a,b,c \in \mathbb{Z}, \mathrm{Disc}(a,b,c) = D\} / \sim .$$

We denote $[a,b,c]$ the equivalence class containing (a,b,c) in G_D.

Proposition 2.3 *Any binary quadratic form that is equivalent to a primitive binary quadratic form is primitive.*

Proof. Consider the set of integers that can be written as $Q(x, y)$ for a binary quadratic form Q and $x, y \in \mathbb{Z}$. Q is non-primitive if and only if those integers are all multiple of some N (consider $(x, y) = (1, 0), (0, 1)$ and $(1, 1)$ for the reverse implication).

However, since equivalence of binary quadratic forms is given by a simple invertible change of variables, any equivalent binary quadratic forms represent the same integers. □

We say that a binary quadratic form (a, b, c) is *reduced* if

$$|b| \leq a \leq c.$$

Proposition 2.4 *There are finitely many reduced binary quadratic forms of a fixed discriminant D.*

Furthermore, every binary quadratic form is equivalent to a unique reduced binary quadratic form, with the exception of

$$(a, b, a) \sim (a, -b, a) \quad \text{and} \quad (a, a, c) \sim (a, -a, c)$$

where the reduced form is not unique.

Finally, we conclude that $|G_D|$ is finite for any discriminant D.

Proof. Recall that two generators for $\mathrm{SL}_2(\mathbb{Z})$ are

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{2.1}$$

Using T^n, we can show that

$$(a, b, c) \sim (a, b + 2an, c') \tag{2.2}$$

Note that c' is uniquely determined from the first two entries by the fact that the discriminant is fixed. Here, $c' = an^2 + bn + c$. Using S, we have

$$(a, b, c) \sim (c, -b, a). \tag{2.3}$$

Using (2.2) we can find a representative with $|b| \leq |a|$, and using (2.3) we can insure that $|a| \leq |c|$. Uniqueness follows from the fact that T and S are generators for $\mathrm{SL}_2(\mathbb{Z})$, and any transformation can be expressed in terms of these two.

The last statement is an obvious consequence of the first two. □

3. Gauss's Composition Law

Numbers of the form $x^2 + Dy^2$ are closed under multiplication. Gauss asked whether it was possible to generalize this result to numbers of a more general form. He comes up with the answer: Yes!

We recall the following identity attributed to 7th century Indian mathematician Brahmagupta (see [6]).

Proposition 3.1 *For any integers x_1, y_1, x_2, y_2, D,*

$$\left(x_1^2 + Dy_1^2\right)\left(x_2^2 + Dy_2^2\right) = (x_1x_2 - Dy_1y_2)^2 + D\,(x_1y_2 + x_2y_1)^2\,.$$

Proof. Note that $\mathrm{N}(x + y\sqrt{-D}) = x^2 + Dy^2$. Therefore,

$$\begin{aligned}&\left(x_1^2 + Dy_1^2\right)\left(x_2^2 + Dy_2^2\right)\\ &= \mathrm{N}\left(x_1 + y_1\sqrt{-D}\right)\mathrm{N}\left(x_2 + y_2\sqrt{-D}\right)\\ &= \mathrm{N}\left(x_1x_2 - Dy_1y_2 + (x_1y_2 + x_2y_1)\sqrt{-D}\right)\end{aligned}$$

by the multiplicativity of the norm, and so

$$= (x_1x_2 - Dy_1y_2)^2 + D\,(x_1y_2 + x_2y_1)^2\,.$$

□

We can summarize this previous identity by saying that the numbers of the form $x^2 + Dy^2$ are closed under multiplication. In 1801, Gauss asked in his *Disquisitiones Arithmeticae* whether it was possible to generalize this to numbers of a more general form, namely $ax^2 + bxy + cy^2$. He comes up with the answer: Yes!

Theorem 3.2 (Gauss) *Let $a_1x_1^2+b_1x_1y_1+c_1y_1^2$ and $a_2x_2^2+b_2x_2y_2+c_2y_2^2$ be binary quadratic forms of discriminant D. Then, there exists an (explicit) transformation (change of variables)*:

$$\begin{pmatrix}X\\ Y\end{pmatrix} = \begin{pmatrix}p_0 & p_1 & p_2 & p_3\\ q_0 & q_1 & q_2 & q_3\end{pmatrix}\begin{pmatrix}x_1\,x_2\\ x_1\,y_2\\ y_1\,x_2\\ y_1\,y_2\end{pmatrix},$$

and integers A, B and C, such that

$$\begin{aligned}&\left(a_1x_1^2 + b_1x_1y_1 + c_1y_1^2\right)\left(a_2x_2^2 + b_2x_2y_2 + c_2y_2^2\right)\\ &\qquad = AX^2 + BXY + CY^2.\end{aligned}$$

Moreover, $B^2 - 4AC = D$.

From this, it is easy to conclude the following.

Proposition 3.3 *The set G_D forms a finite abelian group.*

Proof. We need to show that the composition law defined this way is well-defined on G_D. Indeed, the two changes of variables $\begin{pmatrix} x_1' \\ y_1' \end{pmatrix} = M_1 \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ and $\begin{pmatrix} x_2' \\ y_2' \end{pmatrix} = M_2 \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$ correspond to the change of variable

$$\begin{pmatrix} x_1'x_2' \\ x_1'y_2' \\ y_1'x_2' \\ y_1'y_2' \end{pmatrix} = (M_1 \otimes M_2) \begin{pmatrix} x_1\, x_2 \\ x_1\, y_2 \\ y_1\, x_2 \\ y_1\, y_2 \end{pmatrix}$$

so the matrix

$$\begin{pmatrix} p_0' & p_1' & p_2' & p_3' \\ q_0' & q_1' & q_2' & q_3' \end{pmatrix} = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} (M_1 \otimes M_2)$$

will yield the correct change of variable for the multiplication of $Q_1(x_1', y_1')$ and $Q_2(x_2', y_2')$.

□

It is worth noting that the modern notion of a group did not exist when Gauss wrote his *Disquisitiones*. However, it is clear that, without using our modern terms, this is really what he was after.

It is worth noting that the modern notion of a group did not exist when Gauss wrote his *Disquisitiones*. However, it is clear that, without using our modern terms, this is really what he was after.

4. Dirichlet's United Forms

Gustav Lejeune Dirichlet was a student of Gauss, and apparently spent a considerable amount of time studying Gauss's *Disquisitiones Arithmeticae*. During his private study of Gauss's work, Dirichlet established a way to realize Gauss's composition law in a much simpler way. This approach was so successful that it gave the basis for the modern understanding of this composition law.

Dirichlet established a way to realize Gauss's composition law in a much simpler way. This approach was so successful that it gave the basis for the modern understanding of this composition law.

We say that two binary quadratic forms (a_1, b_1, c_1) and (a_2, b_2, c_2) of discriminant D are *united* if

$$\gcd\left(a_1, a_2, \frac{b_1 + b_2}{2}\right) = 1.$$

Remark 1 The quantity $b_1 + b_2$ is always even. Indeed, $D = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$ and so $b_1^2 \equiv b_2^2 \pmod 4$ and $b_1 \equiv b_2 \pmod 2$.

Proposition 4.1 *If (a_1, b_1, c_1) and (a_2, b_2, c_2) are united forms, then there exist integers B and C such that*

$$(a_1, b_1, c_1) \sim (a_1, B, a_2C)$$

and

$$(a_2, b_2, c_2) \sim (a_2, B, a_1C).$$

See [7, Prop.4.5] for the proof.

Corollary 4.2 *If (a_1, b_1, c_1) and (a_2, b_2, c_2) are united forms, then in the group G_D,*

$$[a_1, b_1, c_1] \cdot [a_2, b_2, c_2] = [a_1a_2, B, C].$$

Proof. Consider the matrix

$$\begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix}$$

in Theorem 3.2, where B and C are as in Proposition 4.1. □

Corollary 4.2 allows us to compute some group operations in a more efficient way than what is given by Theorem 3.2. Also, we now have a way to explicitly describe the identity of G_D, as well as inverses.

Proposition 4.3 *In G_D,*

1)
$$1_{G_D} = \begin{cases} \left[1, 0, \frac{D}{4}\right] & \text{if } D \equiv 0 \pmod 4 \\ \left[1, 1, \frac{1-D}{4}\right] & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

2)
$$[a, b, c]^{-1} = [a, -b, c] = [c, b, a].$$

Proof. 1) We consider the case $D \equiv 0 \pmod 4$. Consider (a, b, c) of discriminant D, we want to compute $[a, b, c] \cdot \left[1, 0, \frac{D}{4}\right]$. Note that b is even, say $b = 2n$. Using notation from the solution of Proposition 2.4, we can use T^n to have $\left[1, 0, \frac{D}{4}\right] = [1, 2n, c'] = [1, b, c']$. The last coefficient c' is entirely determined by the first two entries, and here $c' = \frac{b^2-D}{4}$. Also, by the same reasoning $c = \frac{b^2-D}{4a}$ and so $c' = ac$. So we have

$$[a, b, c] \cdot \left[1, 0, \frac{D}{4}\right] = [a, b, c] \cdot [1, b, ac] = [a, b, c]$$

by Corollary 4.2. The case $D \equiv 1 \pmod 4$ is similar.

2) We want to compute $[a, b, c][c, b, a]$. By Corollary 4.2 with $B = b$ and $C = 1$, we get

$$[a, b, c] \cdot [c, b, a] = [ac, b, 1] = [1, -b, ac]\,,$$

and applying T^n for a suitable n will retrieve the identity from the previous part.

□

Dirichlet went on to use the notion of ideals in quadratic number fields to obtain the 'modern' formulation of the composition law. To understand this formulation, one must first understand the concepts of ideals and ideal class groups. For the benefit of the reader, we include here a short summary. We recommend [7, Ch.6] for a more in-depth exposition.

Let K be a number field. An ideal I of the ring of integer of K, $\mathcal{O}_K$, is called an integral ideal of K. Additionally, we say that the ideal I is *principal* if there exists a single element $\alpha \in \mathcal{O}_K$ generating it, i.e., such that

$$I = \{\alpha x : x \in \mathcal{O}_K\}.$$

For our application, we only consider quadratic numbers fields, i.e., fields $K = \mathbb{Q}(\sqrt{D})$, where D is a fundamental discriminant. It is a well-known fact that for any integral ideal $\mathfrak{A}$ of a quadratic

Dirichlet went on to use the notion of ideals in quadratic number fields to obtain the 'modern' formulation of the composition law. To understand this formulation, one must first understand the concepts of ideals and ideal class groups.

number field K, there exists at most two algebraic integers a, b in O_K such that

$$\mathfrak{A} = \langle \alpha, \beta \rangle = \{\alpha x + \beta y : x, y \in \mathbb{Z}\}.$$

We call $\langle \alpha, \beta \rangle$ the $\mathbb{Z}$-*basis* of $\mathfrak{A}$.

Given a quadratic number field $K = \mathbb{Q}(\sqrt{D})$, the set of all its integral ideals forms an abelian group, where the operation is given by multiplication. Specifically, if $\mathfrak{A}$ and $\mathfrak{B}$ are integral ideals, then

$$\mathfrak{AB} = \{ab : a \in \mathfrak{A} \text{ and } b \in \mathfrak{B}\}$$

is also an integral ideal. The set of all principal integral ideals forms a subgroup of this group. The quotient of all the integral ideals by the principal ideals is called the *ideal class group*.

Here, we actually need to refine this concept slightly and introduce the *narrow class group*. Given an algebraic integer $\alpha \in O_K$, we define its norm to be $N(\alpha) = \alpha\overline{\alpha}$, where conjugation is defined by sending $\sqrt{D}$ to $-\sqrt{D}$. Then, the set of all principal integral ideals (α) with $N(\alpha) > 0$ also form a subgroup of the group of all integral ideals. The quotient of all ideals by this new subgroup is called the narrow class group of K, denoted $C\ell^+(K)$.

In the narrow class group, two integral ideals $\mathfrak{A}$ and $\mathfrak{B}$ are 'the same' (narrowly equivalent) if they differ by a principal ideal generated by an element of positive norm.

In the narrow class group, two integral ideals $\mathfrak{A}$ and $\mathfrak{B}$ are 'the same' (narrowly equivalent) if they differ by a principal ideal generated by an element of positive norm.

$$\mathfrak{A} = (\alpha)\mathfrak{B}$$

with $N(\alpha) > 0$.

Finally, let $\mathfrak{A} = \langle \alpha, \beta \rangle$ be an integral ideal of $K = \mathbb{Q}(\sqrt{D})$. We define the norm of $\mathfrak{A}$ as $\mathrm{N}(\mathfrak{A}) = \left|\alpha\overline{\beta} - \overline{\alpha}\beta\right| / \sqrt{D}$. Note that this norm is independent of the choice of basis for $\mathfrak{A}$.

The modern formulation of the composition law relies on the following theorem.

Theorem 4.4 *The group G_D is isomorphic to the narrow class group of $K = \mathbb{Q}(\sqrt{D})$.*

More specifically, there is an explicit isomorphism that allows us to compute compositions of binary quadratic forms. To each binary quadratic form, we associate an ideal of O_K in the following way:

$$(a, b, c) \overset{\Phi}{\longmapsto} a\mathbb{Z} + \left(\frac{b - \sqrt{D}}{2}\right)\mathbb{Z}.$$

Conversely, for every ideal of O_K, we associate a binary quadratic form:

$$\frac{(\alpha x + \beta y)(\overline{\alpha} x + \overline{\beta} y)}{|\mathrm{N}(\mathfrak{A})|} \overset{\Psi}{\longleftarrow} \alpha\mathbb{Z} + \beta\mathbb{Z} = \mathfrak{A}.$$

Theorem 4.5 *1) The map Φ sends equivalent binary quadratic forms in G_D to (narrowly) equivalent ideals in $C\ell^+(K)$.*

2) The map Ψ sends (narrowly) equivalent ideals in $C\ell^+(K)$ to equivalent binary quadratic forms in G_D.

3) The maps Φ and Ψ are inverses of each other.

See [7, Theorem 6.20] for the proof of this theorem.

Under this correspondence above, the composition of binary quadratic forms in G_D corresponds to the multiplication of ideals in $C\ell^+(K)$. Therefore, given two binary quadratic forms of discriminant D, say Q_1 and Q_2, we can compute $Q_1 \cdot Q_2$ by

1. Finding $\Phi(Q_1)$ and $\Phi(Q_2)$,
2. Finding a 2 elements $\mathbb{Z}$-basis for the ideal $\Phi(Q_1)\Phi(Q_2)$, say $\langle \alpha, \beta \rangle$ (one always exists since O_K is a Dedekind domain),
3. Computing $\Psi(\langle \alpha, \beta \rangle)$, and finding a reduced representative if necessary.

Proposition 4.6 *The algorithm described above is equivalent to the composition law defined in Corollary 4.2. That is, if (a_1, b_1, c_1) and (a_2, b_2, c_2) are united forms, then*

$$\left[\Psi\Big(\Phi\left([a_1, b_1, c_1]\right)\Phi\left([a_2, b_2, c_2]\right)\Big)\right] = [a_1 a_2, B, C],$$

where B and C are the integers from Proposition 4.1.

Proof. From Proposition 4.1, $(a_1, b_1, c_1) \sim (a_1, B, a_2C)$ and $(a_2, b_2, c_2) \sim (a_2, B, a_1C)$ for some B and C. Clearly $\gcd(a_1, a_2, B) = 1$ (see Proposition 2.3). Then, we compute

$$\begin{aligned}\mathfrak{A} &= \Phi((a_1, B, a_2C))\,\Phi((a_2, B, a_1C)) \\ &= \left\langle a_1a_2, a_1\left(\tfrac{B-\sqrt{D}}{2}\right), a_2\left(\tfrac{B-\sqrt{D}}{2}\right), \right. \\ &\qquad \left. \tfrac{B^2+D-2B\sqrt{D}}{4}\right\rangle\end{aligned}$$

as a $\mathbb{Z}$-basis. Also, writing $D = B^2 - 4a_1a_2C$, the last generator can be replaced by $B\left(\frac{B-\sqrt{D}}{2}\right)$.

Finally, since $\gcd(a_1, a_2, B) = 1$, we can find a linear combination of them that equals 1. As such, we can easily see

$$\begin{aligned}\left\langle a_1a_2, \frac{B-\sqrt{D}}{2}\right\rangle \subseteq \left\langle a_1a_2, a_1\left(\frac{B-\sqrt{D}}{2}\right),\right. \\ \left. a_2\left(\frac{B-\sqrt{D}}{2}\right), B\left(\frac{B-\sqrt{D}}{2}\right)\right\rangle,\end{aligned}$$

and since the reverse inclusion is trivial, we have

$$\begin{aligned}[a_1, B, a_2C][a_2, B, a_1C] &= \Psi\left(\left\langle a_1a_2, \tfrac{B-\sqrt{D}}{2}\right\rangle\right) \\ &= [a_1a_2, B, C].\end{aligned}$$

□

5. Bhargava's Cube

Consider the following *cube of integers*, that is a cube with an integer at every corner. In *Figure* 1, a, b, c, d, e, f, g, h are all integers. We can *cut* the cube to obtain two squares in three ways.

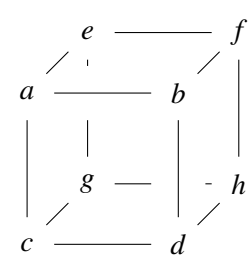
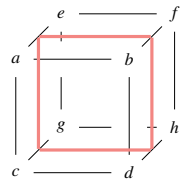


Figure 1. Bhargava's cube of integers.

1) Front–Back:

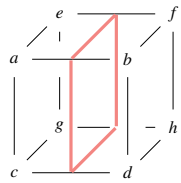


We then define the following two matrices using the two squares we get.

$$M_1 := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad N_1 := \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

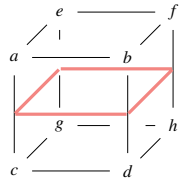
We do the same for the next two cuts, rotating the whole cube so that a is always the top left entry of the first matrix.

2) Left–Right:



$$M_2 := \begin{pmatrix} a & c \\ e & g \end{pmatrix} \quad N_2 := \begin{pmatrix} b & d \\ f & h \end{pmatrix}.$$

3) Up–Down:



$$M_3 := \begin{pmatrix} a & e \\ b & f \end{pmatrix} \quad N_3 := \begin{pmatrix} c & g \\ d & h \end{pmatrix}.$$

Now, we define an action of the group

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$$

on the space C of all cubes of integers.

If $\gamma \in \Gamma$ and $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ is its ith factor, $1 \le i \le 3$, then the action of γ on a cube replaces (M_i, N_i) with $(rM_i + sN_i, tM_i + uN_i)$. In other

words, each factor of γ performs a 'face operation' on the cube, similar to what we would do on a matrix with row and column operations. The first factor performs a face operation on the front and back faces, the second factor on the left and right faces, and the last on the up and down faces.

Proposition 5.1 *The action of each factor of* $\gamma \in \Gamma$ *commutes with each other.*

Proof. This can be viewed simply as the analogue of row and column operation on matrices commuting with each other. A moment's reflection should make this clear. □

Given a cube C, we define three binary quadratic forms as:

$$Q_i^C = -\det(M_i x - N_i y) \ ,$$

for $1 \leq i \leq 3$.

Example 5.1 If we take C to be the cube of *Figure* 1, then

$$Q_1^C = -\det\begin{pmatrix} ax - ey & bx - fy \\ cx - gy & dx - hy \end{pmatrix},$$

which indeed gives a binary quadratic form.

We say that a cube C is *projective* if Q_1^C, Q_2^C, Q_3^C are primitive binary quadratic forms.

Proposition 5.2 *For any cube C,*

$$\mathrm{Disc}\left(Q_1^C\right) = \mathrm{Disc}\left(Q_2^C\right) = \mathrm{Disc}\left(Q_3^C\right).$$

Proof. From Example 5.1, we can find a formula for the discriminant of Q_1^C as:

$$\begin{aligned}\mathrm{Disc}(Q_1^C) \quad &= (cf)^2 + (ed)^2 + (bg)^2 + (ah)^2 - 2ah(de + cf + bg) \\ &\quad -2(bcfg + cdef + bdeg + bcfg)\,.\end{aligned}$$

Then, we notice that we can retrieve M_2 and N_2 from M_1 and N_1 by permuting the elements a, b, c, d, e, f, g, h as follows:

$$\begin{pmatrix} a & b & c & d & e & f & g & h \\ a & c & e & g & b & d & f & h \end{pmatrix}$$

or in cycle notation $(a)(b\ c\ e)(d\ g\ f)(h)$. Actually, we notice that we can also retrieve M_3 and N_3 from M_2 and N_2 using the same permutation.

Finally, note that the formula above for the discriminant is invariant under this permutation.

□

It, therefore, makes sense to define $\mathrm{Disc}(C)$ for a cube C as the discriminant of its associated binary quadratic forms.

We now examine the action of Γ on these newly defined binary quadratic forms.

Proposition 5.3 *Any element of* $\{1\} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ *acts trivially on* Q_1^C.

Proof. Let $\gamma \in \{1\} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ act on the cube C. Suppose G_2 is the second factor of γ and G_3 the third. Then note that G_2 acts on M_1 and N_1 by column operation. Specifically, M_1 and N_1 become M_1G_2 and N_1G_2 respectively. On the other hand, G_3 act on M_1G_2 and N_1G_2 by row operations, and they become $G_3M_1G_2$ and $G_3N_1G_2$ respectively. Therefore, we have that

$$\begin{aligned} Q_1^{C*\gamma} &= -\det\left(G_3M_1G_2x - G_3N_1G_2y\right) = -\det(G_3) \\ &\quad \det\left(M_1x - N_1y\right)\det(G_2) = Q_1^C. \end{aligned}$$

□

Proposition 5.4 *The element* $\gamma = M \times 1 \times 1 \in \Gamma$ *acts on* Q_1^C *in the usual way. Specifically,*

$$Q_1^{C*\gamma} = Q_1^C * \tilde{M},$$

where

$$\tilde{\begin{pmatrix} r & s \\ t & u \end{pmatrix}} = \begin{pmatrix} r & -t \\ -s & u \end{pmatrix}.$$

Proof. This time, let $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \times 1 \times 1$ act on C. Then,

$$\begin{aligned} Q_1^{C*\gamma}(x,y) &= -\det((rM_1 + sN_1)x - (tM_1 + uN_1)y) \\ &= -\det(M_1(rx - ty) - N_1(uy - sx)) \\ &= Q_1^C(rx - ty, uy - sx) \\ &= Q_1^C * \begin{pmatrix} r & -t \\ -s & u \end{pmatrix}. \end{aligned}$$

□

By symmetry, the above two Propositions hold for the i-th factor of Γ and Q_i^C, $1 \leq i \leq 3$. In particular, note that we can conclude the following corollary.

Corollary 5.5 $\mathrm{Disc}(C)$ *is invariant under the action of* Γ.

From there, we can impose a group structure on the set of primitive binary quadratic forms of discriminant D by declaring that for any triplet Q_1^A, Q_2^A, Q_3^A arising from a cube A of discriminant D,

$$Q_1^A + Q_2^A + Q_3^A = 0.$$

In other words, we mod out this relation on the free abelian group generated by all binary quadratic forms of discriminant D. Note that we obtain the $\mathrm{SL}_2(\mathbb{Z})$ equivalence of binary quadratic forms for free from this definition. Indeed, if $\gamma = M \times 1 \times 1 \in \Gamma$,

$$\begin{aligned} Q_1^A + Q_2^A + Q_3^A = 0 &= Q_1^{A*\gamma} + Q_2^{A*\gamma} + Q_3^{A*\gamma} \\ &= Q_1^A * \tilde{M} + Q_2^A + Q_3^A \\ \Rightarrow Q_1^A &= Q_1^A * \tilde{M}. \end{aligned}$$

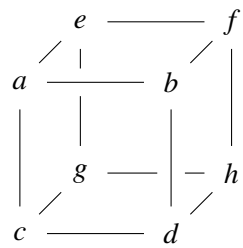
As it turns out, this is exactly equivalent to the previously defined composition law. Indeed, Bhargava proved the following theorem

Theorem 5.6 ([2, Thm 1]) *There exists a projective cube A of discriminant D with Q_1^A, Q_2^A, Q_3^A if and only if*

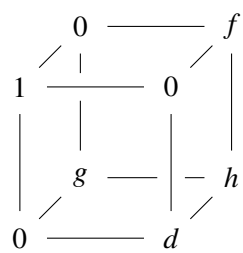
$$\left[Q_1^A\right] \cdot \left[Q_2^A\right] \cdot \left[Q_3^A\right] = 1_{G_D},$$

and that cube is unique up to Γ*-equivalence.*

There is a way to easily see that this composition law agrees with our previously defined composition. Start with a projective cube C.



Since C is projective, we can show that $\gcd(a, b, c, d, e, f, g, h) = 1$. As such, we can find a Γ-equivalent cube such that $a = 1$. We then use this entry to clear entries b, c and e using face operations again. We, therefore, have the equivalent cube $\tilde{C}$ as follows.



The three binary quadratic forms associated to $\tilde{C}$ are:

$$Q_1 = -dx^2 + hxy + fgy^2,$$
$$Q_2 = -gx^2 + hxy + dfy^2,$$
$$Q_3 = -fx^2 + hxy + dgy^2.$$

The cube law tells us that

$$[Q_1] \cdot [Q_2] = [Q_3]^{-1}.$$

Let us now use Dirichlet's united form to arrive at the same conclusion. Recall that from Proposition 4.3,

$$[Q_3]^{-1} = [dg, h, -f].$$

Also, from Corollary 4.2, we get,

$$[Q_1] \cdot [Q_2] = [-d, h, gf] \cdot [-g, h, df] = [dg, h, -f] = [Q_3]^{-1}$$

by letting $a_1 = -d$, $a_2 = -g$, $B = h$ and $C = -f$. Thus, we conclude that the two composition laws are equivalent.

6. Concluding Remarks

One of the most remarkable and surprising aspect of this new approach to the composition law might be how it generalizes to 'higher' compositions.

One of the most remarkable and surprising aspects of this new approach to the composition law might be how it generalizes to 'higher' compositions. Although it was only briefly mentioned in the rest of this article, Bhargava describes in [2] how he generalizes the cube law presented here to retrieve some algebraic structure in higher degree number fields. The correspondence between binary quadratic forms and the narrow class group of quadratic fields was already well-known, but getting a handle on other types of algebraic structures for higher degree is very important in algebraic number theory. In particular, see [2–5] for generalizations. For a more involved introduction to the topic, we refer the reader to [8], while [9] also provides a good introduction to the results arising from this new theory of higher compositions.

Acknowledgment

I would like to thank Professor M. Ram Murty, Siddhi Pathak, as well as the referee for their helpful comments and suggestions on a previous version of this article.

Suggested Reading

[1] Manjul Bhargava, *Higher Composition Laws*, PhD Thesis, Princeton University, June 2001.

[2] Manjul Bhargava, Higher Composition Laws I: A New View on Gauss Composition and Quadratic Generalizations, *Annals of Mathematics*, Vol.159, pp.217–250, 2004.

[3] Manjul Bhargava, Higher Composition Laws II: On Cubic Analogues of Gauss Composition, *Annals of Mathematics*, Vol.159, pp.865–886, 2004.

[4] Manjul Bhargava, Higher Composition Laws III: The Parametrization of Quartic Rings, *Annals of Mathematics*, Vol.159, pp.1329–1360, 2004.

[5] Manjul Bhargava, Higher Composition Laws IV: The Parametrization of Quintic Rings, *Annals of Mathematics*, Vol.167, pp.53–94, 2008.

[6] André Weil, *Number Theory: An Approach Through History from Hammurapi to Legendre*, Basel:Birkhäuser, 2001.

[7] D A Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, New York: Springer–Verlag, 1989.

[8] Karim Belabas, Paramétrisation de structures algébriques et densité de discriminants [d'aprés Bhargava], *Astérisque*, No.299 (2005) Exp.No.935, ix, pp.267–299, Seminaire Bourbaki Vol.2003–2004.

[9] Arul Shankar and Xiaoheng Wang, Laws of Composition and Arithmetic Statistics: From Gauss to Bhargava, *The Mathematics Student*, Vol.84, Nos.3–4, pp.159–171, 2015.

[10] Johannes Buchmann and Ulrich Vollmer, *Binary Quadratic Forms: An Algorithmic Approach*, Berlin: Springer–Verlag, 2007.

Address for Correspondence
François Séguin
Department of Mathematics
Queen's University, Kingston
Ontario K7L 3N6, Canada.
Email:
francois.seguin@queensu.ca