COMPOSING QUADRATIC FORMS: GAUSS, DIRICHLET AND BHARGAVA

ANDREW GRANVILLE

0.1. **Introduction.** One of the basic problems of mathematics is to find all of the solutions of a given equation. Some equations are easy, like $x + y = z$, and others can be difficult, like $x^{101} + y^{101} = z^{101}$, though the level of difficulty depends largely on what kind of solutions one is looking for. If we are simply asked for complex numbers that one can take any complex numbers x and y, and let z be any of the 101st roots of $x^{101} + y^{101}$. If we are asked for integer solutions then this is a problem of much greater subtlety and depth, and is the focus of number theory.

One particular, but important, problem is the question of which integers are *represented* by a given polynomial. For example, what integers are represented by $x + 2y$, as x and y run through all the integers? Or by $u^2 + v^2$ as u and v run through all of the integers? Or even by $x^{101} + y^{101} - z^{101}$ as x, y and z run through all the integers?

In this article we will focus on quadratic equations, those of degree two. We know a lot about this question, but by no means all that we would like to understand: there are many unsolved problems about representations by quadratic equations still today, some quite evidently of sublime interest. Our objective is to explain the importance of a beautiful new construction by Manjul Bhargava, allowing us a new perspective on which integers are indeed represented by binary quadratic forms. But before we proceed with quadratic equations, we will review representation by linear equations, and particularly those aspects that will be relevant to our discussion of quadratic equations.

0.2. **Representation by linear equations in integers.** Fix non-zero integers a and b. We wish to determine which integers n can be represented as

$$n = ax + by$$

where x and y are integers. One way to start is to subtract by from both sides and divide by a so that if we are given an integer y then

$$x = \frac{n - by}{a}.$$

However, we have no guarantee that the quantity on the right-hand side here will be an integer. Not only for a specific value of y but perhaps for any value of y. So we have not really made any headway on the question of whether or not there are any solutions. It is not difficult to construct examples for which there are no solutions:

$$2x + 4y = 1$$

1991 *Mathematics Subject Classification.* 11P32.

can have no solutions since, no matter what the choice of integers x and y, the left hand side will always be *even*, while the right hand side will always be *odd*. The reason the left hand side is always even is that 2 divides both terms on the left hand side, because 2 divides both 2 and 4, the coefficients a and b. In fact, 2 is the *greatest common divisor* (gcd) of 2 and 4, written $2 = (2, 4)$.

One can generalize this argument: If there are solutions in integers x, y to $ax + by = n$ then $\gcd(a, b)$ divides both a and b, hence both ax and by, and therefore must divide $ax + by = n$. Since $g = \gcd(a, b)$ divides a, b and n, we can divide this common factor out from each. To do this we write $a = Ag, b = Bg$ and $n = Ng$ for some integers A, B and N. Then

$$Ng = n = ax + by = Agx + Bgy = (Ax + By)g,$$

and dividing through by g, leaves us with

$$N = Ax + By.$$

So we have proved that if n is represented by $ax + by$ then $n = Ng$ for some integer N, and N can be represented by $Ax + By$. For example if n can be represented by $2x + 4y$ then $n = 2N$ for some integer N, that is, n is even, and N can be represented by $x + 2y$. Evidently every integer N can be represented by $x + 2y$ (simply take $x = N$ and $y = 0$), so every even integer $N = 2n$ can be represented by $2x + 4y$.

This is not the whole story for if we ask what is represented by $2x - 3y$ we cannot so easily find the representation, since neither coefficient is 1 yet their gcd is 1. The trick here is to find a representation of 1, for example $2 \cdot 2 - 3 \cdot 1$ and then $n = 2 \cdot (2n) - 3 \cdot n$; that is we multiply the representation of 1 through by n. Therefore, for a more general linear form $ax + by$, our question boils down to finding a representation of 1, and this is supplied by the *Euclidean algorithm*. We will not spell this out in detail here but its consequence is that if we are given integers a and b with gcd 1, then the Euclidean algorithm supplies us with integers u and v for which

$$au + bv = 1;$$

and therefore

$$n = ax + by \text{ where } x = nu \text{ and } y = nv.$$

0.3. **Representation by quadratic equations in integers.** Let a, b and c be given integers. The polynomial

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

is a *binary quadratic form* ("binary" as in **two** variable, and "quadratic" as in degree **two**. The degree of bxy is also two, since the degree of a term like this is given by the degree of x, plus the degree of y). We are interested in what integers can be represented by a given binary quadratic form f. As in the linear case, we can immediately reduce our considerations to the case that $\gcd(a, b, c) = 1$.

The first important result of this type was given by Fermat near the beginning of the Renaissance. He considered the particular example $f(x, y) = x^2 + y^2$, asking which integers can be written as the sum of two squares of integers. He proved two things. Firstly that an odd prime p can be written as the sum of two squares if and only if $p \equiv 1$

(mod 4) (so that $2, 5, 13, 17, 29, 37, 41, \ldots$ can be written as the sum of two squares of integers, whereas $3, 7, 11, 19, 23, 31, 43, 47, \ldots$ cannot). Secondly that the product of two integers that can be written as the sum of two squares, can also be written as the sum of two squares, a consequence of the identity

$$(u^2 + v^2)(r^2 + s^2) = (ur + vs)^2 + (us - vr)^2; \tag{1}$$ Comp1

that is, $x^2 + y^2$ where $x = ur + vs$ and $y = us - vr$. One can combine these two facts to classify exactly which integers are represented by the binary quadratic form $x^2 + y^2$.

At first sight it looks like it might be difficult to work with the example $f(x, y) = x^2 + 20xy + 101y^2$. However, this can be rewritten as $(x + 10y)^2 + y^2$, and so represents exactly the same integers as $g(x, y) = x^2 + y^2$. To see this we remark that if

$$n = f(u, v) \text{ then } n = g(u + 10v, v)$$

and if

$$n = g(r, s) \text{ then } n = f(r - 10s, s).$$

Thus every representation of n by f corresponds to one by g, and vice-versa. This is known as a *1-to-1 correspondence*. It is obtained using the *linear transformation* $u, v \to u + 10v, v$, which is *invertible* via the inverse linear transformation $r, s \to r - 10s, s$. Such a pair of quadratic forms, f and g, are said to be *equivalent*; and we have just seen how equivalent binary quadratic forms represent exactly the same integers.

It would take a whole book to fully describe the theory of binary quadratic forms. Our objective here is to study generalizations of the identity (1).Comp1

0.4. **Composition and Gauss.** In (1)Comp1 we see that the product of two integers represented by the binary quadratic form $x^2 + y^2$ is also an integer represented by that binary quadratic form; we are now looking for further such identities. One easy generalization is given by

$$(u^2 + dv^2)(r^2 + ds^2) = x^2 + dy^2 \text{ where } x = ur + dvs \text{ and } y = us - vr. \tag{2}$$ Comp2

Therefore the product of two integers represented by the binary quadratic form $x^2 + dy^2$ is also an integer represented by that binary quadratic form. For general *diagonal* binary quadratic forms (that is, having no "cross-term" bxy) we have

$$(au^2 + cv^2)(ar^2 + cs^2) = x^2 + acy^2 \text{ where } x = aur + cvs \text{ and } y = us - vr. \tag{3}$$ Comp3

Notice here that the quadratic form on the right hand side is different from those on the left; that is the product of two integers represented by the binary quadratic form $ax^2 + cy^2$ is an integer represented by the binary quadratic form $x^2 + acy^2$.

One can come up with a similar identity no matter what the quadratic form, though one proceeds slightly differently depending on whether the coefficient b is odd or even. In the even case we have (with $b = 2B$)

$$(au^2 + 2Buv + cv^2)(ar^2 + 2Brs + cs^2) = x^2 + (ac - B^2)y^2 \tag{4}$$ Comp4

$$\text{where } x = aur + B(vr + us) + cvs \text{ and } y = us - vr. \tag{5}$$

What is the connection between the quadratic form on the left and that on the right? The most important thing to notice is that their discriminants are the same (the *discriminant* of $ax^2+bxy+cy^2$ is b^2-4ac and one can show that equivalent binary quadratic forms have the same discriminant). Notice that $ac - B^2 = -\frac{1}{4}(b^2 - 4ac)$ in (4).

What about two different binary quadratic forms. Can one multiply together their values? For example,

$$(4u^2 + 3uv + 5v^2)(3r^2 + rs + 6s^2) = 2x^2 + xy + 9y^2$$

by taking $x = ur - 3us - 2vr - 3vs$ and $y = ur + us + vr - vs$. These are three different (that is, inequivalent) binary quadratic forms of discriminant -71. Gauss called this *composition*, that is, finding, for given binary quadratic forms f and g of the same discriminant, a third binary quadratic form h of the same discriminant for which

$$f(u, v)g(r, s) = h(x, y),$$

where x and y are quadratic polynomials in u, v, r, s. Gauss proved that this can always be done. The formulas above can mislead one in to guessing that this is simply a question of finding the right generalization, but that is far from the truth. (1), (2), (3) and (4) are so explicit only because they are very special cases in the theory. In Gauss's proof he had to prove that various other equations could be solved in integers in order to find h and the quadratic polynomials x and y. This was so complicated that some of the intermediate formulas took two pages to write down, and are very difficult to make sense of. See article 234 and beyond in Gauss's book *Disquisitiones Arithmeticae* (1804).

0.5. **Dirichlet Composition.** Dirichlet claimed that when he was a student, working with Gauss, he slept with a copy of *Disquisitiones* under his pillow, every night for three years. It worked as Dirichlet found a way to better understand Gauss's proof of composition,which amounted to a straightforward algorithm to determine the composition of two given binary quadratic forms f and g of the same discriminant. The key was to prove that there exist quadratic forms $F(x, y) = ax^2 + bxy + cy^2$, equivalent to f, and $G(x, y) = Ax^2 + bxy + Cy^2$, equivalent to g, for which $(a, A) = 1$. Notice that the middle coefficients of F and G are the same. Since these have the same discriminant we deduce that $ac = AC$ and so there exists an integer h for which

$$F(x, y) = ax^2 + bxy + Ahy^2 \text{ and } G(x, y) = Ax^2 + bxy + ahy^2.$$

Then

$$H(ur - hvs, aus + Avr + bvs) = F(u, v)G(r, s) \text{ where } H(x, y) = aAx^2 + bxy + hy^2.$$

Dirichlet went on to interpret this in terms of what we would today call *ideals*; and this in turn led to the birth of modern algebra by Dedekind. In this theory one is typically not so much interested in the identity, writing H as a product of f and g (which is typically very complicated and none too enlightening), but rather in determining H from f and g (which has an important interpretation in terms of group theory that will take us too far afield for this article).

0.6. **Bhargava Composition.** [1] Let us begin with one further explicit composition, a tiny variant on (4) (letting $s \to -s$ there):

$$(au^2 + 2Buv + cv^2)(ar^2 - 2Brs + cs^2) = x^2 + (ac - B^2)y^2$$
$$\text{where } x = aur + B(vr - us) - cvs \text{ and } y = us + vr.$$

Combining this with the results of the previous section suggests that if the discriminant d is divisible by 4 (which is equivalent to b being even) then

$$F(u, v)G(r, s)H(m, n) = P(x, y) \tag{6}$$

where $P(x, y) = x^2 - \frac{d}{4}y^2$ and x and y are cubic polynomials in m, n, r, s, u, v. Analogous remarks can be made if the discriminant is odd.

In 2004 Bhargava came up with an entirely new way to find all of the triples F, G, H of binary quadratic forms of the same discriminant for which (6) holds: We begin with a 2-by-2-by-2 cube, the corners of which are labeled with the integers a, b, c, d, e, f, g, h. There are six faces of a cube, and these can be split into three parallel pairs. To each such parallel pair consider the pair of 2-by-2 matrices given by taking the entries in each face, those entries corresponding to opposite corners of the cube, always starting with a. Hence we get the pairs

$$M_1(x, y) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} x + \begin{pmatrix} e & f \\ g & h \end{pmatrix} y = \begin{pmatrix} ax + ey & bx + fy \\ cx + gy & dx + hy \end{pmatrix},$$
$$M_2(x, y) := \begin{pmatrix} a & c \\ e & g \end{pmatrix} x + \begin{pmatrix} b & d \\ f & h \end{pmatrix} y = \begin{pmatrix} ax + by & cx + dy \\ ex + fy & gx + hy \end{pmatrix},$$
$$M_3(x, y) := \begin{pmatrix} a & b \\ e & f \end{pmatrix} x + \begin{pmatrix} c & d \\ g & h \end{pmatrix} y = \begin{pmatrix} ax + cy & bx + dy \\ ex + gy & fx + hy \end{pmatrix},$$

where we have, in each, appended the variables, x, y, to create matrix function of x and y. The determinant, $-Q_j(x, y)$, of each $M_j(x, y)$, is a quadratic form in x and y. (The *determinant* of a 2-by-2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by $ad - bc$.) Incredibly Q_1, Q_2 and Q_3 all have the same discriminant and their composition equals P, just as in (6). Let's work though an example: Plot the cube in 3-dimensions and label each corner with its Cartesian co-ordinates (each 0 or 1), and then label the corner with this as a binary number, $4x + 2y + z$, squared. Hence

$$a, b, c, d, e, f, g, h = 2^2, 6^2, 0^2, 4^2, 3^2, 7^2, 1^2, 5^2,$$

leading to three binary quadratic forms of discriminant $-7 \cdot 4^4$:

$$Q_1 = -4^2(4x^2 + 13xy + 11y^2),\ Q_2 = -2^2(x^2 - 2xy + 29y^2),\ \text{and } Q_3 = 4^2(8x^2 + 5xy + y^2).$$

[1] There is no Nobel prize in mathematics; the nearest equivalent is the *Fields' medal.* though this is only given to people 40 years of age or younger. They are awarded every four years, up to four each time, the most recent being last Wednesday (August 13th, 2014) in Korea. One of the laureates was Manjul Bhargava for a body of work which begins with his version of composition, as discussed here, and allows him to much better understand many classes of equations, especially cubic. Bhargava was born in Hamilton, Ontario, and was the first Canadian to receive this most prestigous award in mathematics.

After some work one can verify that

$$Q_1(m,n)Q_2(r,s)Q_3(u,v) = 4(x^2 + 4^3 \cdot 7y^2),$$

where x and y are the following cubic polynomials in m, n, r, s, u, v:

$$x = 8(-11mru - 3mrv + 25msu + 17msv - 17nru - 4nrv + 59nsu + 32nsv)$$

$$\text{and} \quad y = mru + mrv + 21msu + 5msv + 3nru + 2nrv + 31nsu + 6nsv.$$

Bhargava proves his theorem, inspired by a 2-by-2-by-2 Rubik's cube. The idea is to apply an invertible linear transformation simultaneously to a pair of opposite sides. For example, if one applies an invertible linear transformation to the first pair of sides, then the binary quadratic form Q_1 is transformed in the usual way, whereas Q_2 and Q_3 remain the same. One can do this with any pair of sides.This allows one to proceed in "reducing" the three binary quadratic forms to equivalent forms that are easy to work with (rather like in Dirichlet's proof). This brings to mind the twists of the Rubik's cube, though in that case one has only finitely many possible transformations, whereas here there are infinitely many possibilities!

References

[1] Manjul Bhargava, *Higher Composition Laws I: A New View on Gauss Composition, and Quadratic Generalizations*, Annals of Mathematics **159** (2004), 217?250.
[2] Karl Frederich Gauss, *Disquisitiones Arithmeticae* (1804).

Département de mathématiques et de statistiques, Université de Montréal, Montréal QC H3C 3J7, Canada.

E-mail address: andrew@dms.umontreal.ca