

# On Integers and Quadratics

Joshua Zucker, Berkeley Math Circle, November 12, 2000

One interesting quadratic to solve over the integers is familiar even to the average high school geometry student:  $x^2 + y^2 = z^2$ . I assume you all know the proof that the only primitive integer solutions are  $x = a^2 - b^2$ ,  $y = 2ab$ ,  $z = a^2 + b^2$ , with  $a > b$ , relatively prime and not both odd. Here's a problem that might keep you busy for a minute or two in case the rest of this talk is old hat to you, too.

1. For prime  $p$ , find all primitive solutions to  $x^2 + py^2 = z^2$ . [Hint: there are two cases,  $a$  and  $b$  both odd, or exactly one of them odd]

Another interesting quadratic is  $x^2 - dy^2 = N$ , with  $d$  and  $N$  integers, usually called Pell's equation even though he never did any work on it. For big fans of continued fractions like me, this equation is lots of fun. It's also of some importance in the overall theory of quadratics.

2. Show that the equation  $ax^2 + bxy + cy^2 + dx + ey + f = 0$  can be reduced to an equation of the Pell form, and thus that knowing an integer solution to Pell's equation always produces a rational solution of the general quadratic. [Why not an integer solution?]

This talk is not about continued fractions, though perhaps some digression into them is justified. Still, you might enjoy trying your hand at the following problems.

3. a) Find the minimum positive solution of  $x^2 - 94y^2 = 1$ .  
b) Find the minimum positive solution of  $x^2 - 95y^2 = 1$ .
4. What if the 1 on the right side of the previous problem were changed to  $-1$ ?
5. For what values of  $N$  with  $|N| < 10$  is there a solution of each of those equations?

Now let's turn to finding integer solutions of another type of quadratic equation. In particular, we'll look at the possible values of a binary quadratic form. The "binary" means that there are two variables, and the "quadratic form" means that every term has degree 2, so the general binary quadratic form is  $ax^2 + hxy + by^2$ , and for today we'll be assuming that  $a$ ,  $h$ , and  $b$  are integers. The question is, what possible values can this expression take when  $x$  and  $y$  are integers?

6. Some quadratic forms are easier to manage than others. By a clever substitution, show that  $2x^2 - 4xy + 3y^2$  is nonnegative (this is thus called a "positive semidefinite" quadratic form). Also find all possible values that it can take on (mod 8).
7. It's fairly easy to see by guessing that it's possible for  $3x^2 + 6xy - 5y^2$  to equal 3, 4, or -5. Can it equal 7? 17? 30? 40?

We can think of these quadratic forms as functions  $f(x, y)$  or simply as a function  $f(\mathbf{v})$ , where  $\mathbf{v}$  is a vector in the plane lattice with basis vectors  $\mathbf{e}_1$  and  $\mathbf{e}_2$ ,  $\mathbf{v} = x\mathbf{e}_1 + y\mathbf{e}_2$ . Certainly  $f$  is quadratic under scalar multiplication,  $f(a\mathbf{v}) = a^2 f(\mathbf{v})$ . More intriguingly,  $f$  is "linear" in the sense that it has a corresponding matrix,

$$ax^2 + hxy + by^2 = ax^2 + \frac{h}{2}xy + \frac{h}{2}yx + by^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & \frac{h}{2} \\ \frac{h}{2} & b \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Let's call that 2 by 2 matrix  $F$ .

8. Show that the substitution you found in problem 6 corresponds to a matrix  $M$  that transforms  $F$  by  $M^T F M$ .
9. Show that any invertible substitution that converts integer quadratic forms into integer quadratic forms must correspond to some such matrix  $M$  with integer entries and integer entries in its inverse (or equivalently that  $M$  has integer entries and  $\det M = \pm 1$ ).

Even more intriguingly, you can make  $f$  seem really linear by studying the corresponding symmetric bilinear form  $B$ , as follows:

$$B(\mathbf{v}, \mathbf{w}) = f(\mathbf{v} + \mathbf{w}) - f(\mathbf{v}) - f(\mathbf{w}).$$

10. Prove that  $B$ , defined as above, is symmetric in  $\mathbf{v}$  and  $\mathbf{w}$ . Sorry, that was too trivial.
11. Prove that  $B$  is linear:  $B(\alpha\mathbf{u} + \beta\mathbf{v}, \mathbf{w}) = \alpha B(\mathbf{u}, \mathbf{w}) + \beta B(\mathbf{v}, \mathbf{w})$ .

Following John Conway, from *The Sensual Quadratic Form*, we'll extend the basis  $\{\mathbf{e}_1, \mathbf{e}_2\}$  to a "superbase"  $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$  where  $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 = \mathbf{0}$ . Why? Hopefully you'll appreciate their use by the end of the talk.

The first step in making a superbase useful is to note that each superbase consists of three different bases, and each basis is in exactly two superbases (well, up to sign, but from now on we'll pretend that  $\mathbf{v}$  and  $-\mathbf{v}$  are the same vector). Since each basis is in exactly two superbases, the bases can be edges of a graph, and the superbases can be vertices, all of degree 3. And now, by arranging the location of new nodes, we can make the faces correspond to vectors, such that each vertex and edge adjacent to the face contains that vector!

[Insert nicely drawn pictures here]

12. Prove the "Arithmetic Progression Rule":  $f(\mathbf{v} + \mathbf{w}) + f(\mathbf{v} - \mathbf{w}) = 2[f(\mathbf{v}) + f(\mathbf{w})]$ .

Why is that called the "Arithmetic Progression Rule"? In our nice picture, if

$$a = f(\mathbf{v}_1), \quad b = f(\mathbf{v}_2), \quad c = f(\mathbf{v}_1 + \mathbf{v}_2), \quad d = f(\mathbf{v}_1 - \mathbf{v}_2)$$

which are the values of  $f$  in the faces around one edge of our graph, then the rule proves that  $d, a + b, c$  is an arithmetic progression. Let's call the (positive) common difference  $h$ , and label the edge with an arrow to show in which direction the arithmetic progression increases.

13. Why did we call the difference  $h$ ?

14. Prove that there exists a quadratic form with any given values of  $a, b$ , and  $c$  in the three faces surrounding a particular node. [Note that I re-use the letters  $a$  and  $b$ ]

15. Given  $a, b$ , and  $c$  as in the previous problem, is the quadratic form unique? Is it unique up to substitution?

16. Prove the "Climbing Lemma": if the two values  $a$  and  $b$  along edge  $PQ$  are positive, and  $h$  is positive in the direction from  $P$  to  $Q$ , then there can be no cycle starting at  $P$ .

17. Note that the structure of the picture we drew only had to do with properties of the vectors themselves and not of the particular function  $f$  we chose. Use that, and the climbing lemma, to prove that the graph we drew is actually a tree.

Now let's look a little bit more closely at some of the simpler examples of quadratic forms and their related graphs. The simplest type to study is *positive definite*, where the values are always positive. Let's pick three (positive!) values as our starting superbase, and work backwards down the arrows (since we know working forwards will just give larger and larger values, because of the climbing lemma). Eventually we get to a *source*, a node where all the arrows point away.

18. Let  $2\alpha$ ,  $2\beta$ , and  $2\gamma$  be the edge labels radiating from a well, with  $a$ ,  $b$ , and  $c$  the values in the regions opposite each label. Still assuming that  $f$  is positive definite, prove that
  - a)  $a$ ,  $b$ , and  $c$  satisfy the triangle inequality
  - b)  $a$ ,  $b$ , and  $c$  are the three smallest values of  $f$ .
19. In particular, consider  $\alpha = \beta = \gamma = 1$ . Prove (by working backwards down the arrows) that the graph is connected.
20. a) Draw the form where  $(a, b, c) = (2, 3, 4)$ . This is called a "single source".  
 b) Draw the form where  $(a, b, c) = (2, 3, 5)$ . This is called a "double source".

Negative definite forms are pretty similar to positive definite forms, of course. What other combinations of sign are possible? Well, there's the trivial 0 form. Then there's three fairly interesting types: forms that can be positive or negative but never zero, forms that can be zero or positive (which are pretty similar to ones that are zero or negative), and most interesting of all, forms that can be positive, negative, or zero.

21. If a form takes on positive and negative values but never zero, show that the set of edges with a positive number on one side and negative on the other is a single, infinite path. Hint: show that there's one such edge; show that following it forward will always connect to another such edge; and use the climbing lemma and connectedness to show that there are no such edges off the path.
22. Draw the path for the quadratic form from way back in problem 7,  $3x^2 + 6xy - 5y^2$ . What do you notice about the path? Can you now answer problem 7 completely?
23. Prove that the path is always periodic for any quadratic form that takes positive and negative values but never zero. Hint: the determinant of  $F$  is invariant. Use that to prove there are only finitely many choices for  $a$ ,  $b$ , and  $h$  that can occur along the path.

Now consider a form that is *positive semidefinite*: that is, always positive or zero.

24. By considering one of the places where it equals zero, and following the path around it, show that the form is simply a scalar multiple of  $x^2$ .

Now consider a form that takes on all three signs (positive, negative, and zero).

25. By starting from a region where the form equals zero, prove that when you follow an edge that separates positive and negative along the border of that region you eventually reach another region where the form equals zero.

26. Analyze as completely as possible the structure of the rest of the graph.

27. Consider the special case where there is no edge that separates positive and negative as in problem 25, because there are two adjacent regions where the form equals zero. Prove that in this case, the form is a multiple of  $xy$ .

And now for something completely different: the study of which integers are perfect squares mod other integers. You may have heard of quadratic reciprocity and seen it proved, but this proof is remarkable in that it never squares anything or mentions primes.

You may be familiar with the Legendre symbol, defined for any integer  $a$  and prime  $p$  to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is square mod } p. \\ -1 & \text{if } a \text{ is not square mod } p. \end{cases}$$

The Jacobi symbol is traditionally defined for odd nonprime  $n$  to be the product for all the prime factors of  $n$  of the Legendre symbol:  $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\left(\frac{a}{r}\right)\dots$

But Conway introduced me to an alternate definition due to Zolotarev:

$$\left(\frac{a}{n}\right) = \text{the sign of the permutation obtained by multiplying by } a \text{ modulo } n$$

so that for example, multiplying by 3 mod 11 gives

$$(0)(1,3,9,5,4)(2,6,7,10,8)$$

which has no even length cycles, and hence its sign is positive (in fact,  $3 = 5^2 \pmod{11}$ , so the traditional definition gives the same answer). (Recall that a permutation is called positive, or even, iff it can be made of an even number of swaps, or equivalently, iff it has an even number of cycles of even length.)

Conway also introduced me to another convenient notation. He calls a number *positive modulo  $m$*  iff it is strictly between 0 and  $\frac{m}{2}$ , and *negative modulo  $m$*  iff it is strictly between  $-\frac{m}{2}$  and 0.  $\frac{m}{2}$  is said to be *ambiguous modulo  $m$* .

28. Prove that the two definitions are equivalent. [This might be much easier to prove using some of the subsequent problems, which don't depend on this one, so go ahead.]

29. Prove that  $\left(\frac{-1}{n}\right)$  is the sign of  $n$  modulo 4.

30. Prove that  $\left(\frac{a}{n}\right) = (-1)^s$ , where  $s$  is the number of positive numbers  $k \pmod n$  for which  $ak$  is negative mod  $n$ . Hint: do an example, and factor the permutations into a product of one which separates positive and negative numbers and one which swaps between the two sets.

31. If  $a > 0$ , then  $s$  is the number of integers strictly between 0 and  $n/2$  which lie in intervals of the form

$$\left[\left(l - \frac{1}{2}\right)\frac{n}{a}, l\frac{n}{a}\right].$$

32. Prove that this symbol is periodic: if  $m = \pm n \pmod{4a}$ , then  $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$ .

33. Prove that if  $m$  and  $n$  are relatively prime and  $m + n$  is a multiple of 4, then  $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$ .

34. Prove quadratic reciprocity:  $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$  for relatively prime odd integers  $p$  and  $q$ .