An introduction to number theory and Diophantine equations

Lillian Pierce

April 20, 2010

Lattice points and circles

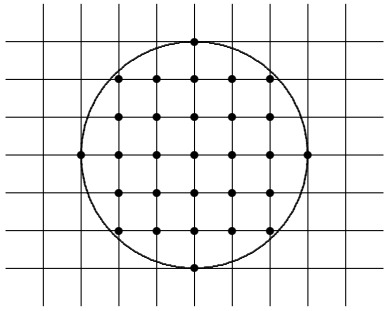
What is the area of a circle of radius r? You may have just thought without hesitation "Why, the area of a circle of radius r is πr^2." And that's true. Humans have understood how to compute the area of a circle for a long time. There is even an Egyptian papyrus (the Rhind papyrus) dating from about 1650 BCE that demonstrates an understanding of π and its fundamental connection to circles. We all agree that the area $A(r)$ of a circle of radius r satisfies the equation

$$A(r) = \pi r^2. \tag{1}$$

Now suppose we draw a grid of squares in the plane with sides of length 1 (and pick one vertex of the grid and call it the origin $(0, 0)$). We'll call the vertices of the grid "integer lattice points" or just "lattice points," since the coordinates of the vertices are integers, i.e. belong to the set

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Next, suppose we draw a circle of radius r centered at the origin. How many lattice points are enclosed in the circle? (We will also count points that lie precisely on the circle itself.) For example, for a circle of radius 1, there are 5 lattice points inside the circle. For a circle of radius 3, there are 29 lattice points inside the circle.



Let's denote by $N(r)$ the number of lattice points in a circle of radius r (including points on the circle itself). Is there a precise formula for $N(r)$, like equation (1) for $A(r)$? It turns out that this is a hard question to answer. The mathematician Carl Friedrich Gauss proposed in 1801 that the number of lattice points $N(r)$ is almost the same as the area $A(r)$ of the circle, but not quite. Precisely, Gauss proved that

$$N(r) = \pi r^2 \pm E(r), \tag{2}$$

where $E(r)$ is an error term defined by

$$E(r) = |\#\{\text{lattice points in circle}\} - \text{area of circle}\,|.$$

How big can the error term be? This is the really hard part of the question. The size of the error term $E(r)$ depends on the radius r of the circle in question, and for some radii the error might be bigger than for others.[1,2]

The Gauss circle problem

The problem of determining the size of $E(r)$ is called *the Gauss circle problem* and it is a very old and difficult—and unsolved—problem. Gauss showed that the biggest the error term could be is $E(r) \leq 2\sqrt{2}\pi r$. More recently, in 1915, two mathematicians named G. H. Hardy and E. Landau proved that $E(r)$ can sometimes be as big as $r^{1/2+\epsilon}$, where ϵ is an arbitrarily small positive real number. So the difference between the number of lattice points inside the circle and the area of the circle is somewhere between $r^{1/2+\epsilon}$ and r. Mathematicians think that the "correct" upper bound for $E(r)$ is $r^{1/2+\epsilon}$, in the sense that the error can be at least this big, but no bigger. We still don't know what the true size of the error term is, more than 200 years after Gauss's work, and nearly 100 years after the work of Hardy and Landau![3]

Why is the Gauss circle problem so difficult? Let's put everything into equations. The set of points (x, y) that lie on a circle $S(r)$ of radius r (centered at the origin) are those points that satisfy the equation

$$x^2 + y^2 = r^2. \tag{3}$$

[1] Is it possible to choose r such that $E(r) = 0$? Remember that $N(r)$ simply counts points and so must be a positive integer, while $A(r) = (3.14159....) \cdot r^2$ doesn't look like an integer unless you pick the radius r very carefully. So the first step would be to choose r such that $A(r)$ is an integer. In this instance, you're allowed to choose r to be any real number you like—it doesn't have to be a positive integer.

[2] In equation (2) you see that sometimes the error term $E(r)$ is subtracted and sometimes it is added, i.e. sometimes there are fewer lattice points in the circle than the area and sometimes there are more. Should we expect there to be a paucity of lattice points 50% of the time (i.e. subtraction in (2)) and an excess of lattice points the other 50% of the time (i.e. addition in (2))? Or should we expect that there is some kind of bias, so that there is usually a paucity, or usually an excess? We'll explore these questions in class.

[3] But mathematicians keep making progress. In 2003, Huxley showed that $E(r) \leq r^{0.6298\ldots}$. It would be big news to push this all the way down to $E(r) \leq r^{1/2+\epsilon}$.

We'll now define the (closed) disk $D(r)$ of radius r to be the set of points lying on or within this circle, so that $D(r)$ is the set of points (x, y) satisfying

$$x^2 + y^2 \leq r^2. \tag{4}$$

The area enclosed by the circle $S(r)$ (equivalently the area of the disk $D(r)$) is πr^2, and in some sense this is the "number" of real solutions to the equation (4).

Now let's restrict our attention to integer lattice points. The integer lattice points (x, y) that lie on the circle $S(r)$ are solutions to the equation (3) such that both x and y are integers.[4] Similarly, the integer lattice points that lie inside the disk $D(r)$ are solutions to (4) with x, y integers, and so the quantity $N(r)$ we are interested in is the number of such solutions to (4).

Finding integer solutions is hard!

The reason the Gauss circle problem is so hard is, roughly speaking, this: *It is much harder to find integer solutions to equations than it is to find real number solutions to equations.* Moreover, it is much harder to find the precise number of integer solutions that satisfy an *equation* like (3) than it is to find the number of integer solutions that satisfy an *inequality* like (4). This interesting difficulty will be a key focus of our course.

The difficulty of finding (and counting) integer solutions to equations might seem counterintuitive at first. After all, isn't it much easier to think about whole numbers like $4, 18, -3, 21$ instead of about real numbers like $\pi, \sqrt{2}, \frac{1}{319}$? The point is that it is much easier to solve an equation like (3) if we can take x, y to be any real numbers we like, while it is very restrictive to insist that x, y must be integers.

Equation (3) is an example of a *Diophantine equation*, namely an indeterminate polynomial equation with integer coefficients for which we desire integer solutions. This type of equation is named after the Greek mathematician Diophantus of Alexandria, who lived in the 3rd century CE. Finding integer solutions to Diophantine equations is one of the major problems in number theory, and despite being hundreds (even thousands) of years old, remains an area of active research to this day. One of the great beauties of Diophantine problems is that they are easy to state, but very tricky to solve!

More Diophantine problems

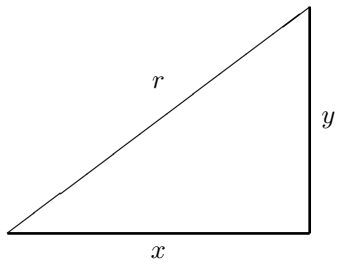
The theme of this course will be exploring Diophantine equations and understanding why it is so much harder to find integer solutions to such equations, rather than real number solutions. Along the way we will encounter many famous problems, some of which have been solved, and some of which haven't. By

[4] Does (3) have any solutions with x, y integers if r is not an integer? Let's think about this. If x and y are integers, then x^2 and y^2 are integers, so $x^2 + y^2$ must be an integer. Therefore r^2 must be an integer. But this doesn't mean that r must be an integer. For example, we can choose r such that $r^2 = 2$, but r is not an integer!

the end of the course you'll be able to spot "hard" questions from "easy" ones, you'll know some of the techniques used by number theorists to approach Diophantine equations, and you'll have a collection of important problems to pose to your friends, your family and yourself. Diophantine problems are beautiful and tricky enough to keep a mathematician occupied for her entire life! Here are a few more examples of important, mysterious, and aesthetically pleasing Diophantine equations that we will encounter in the course.[5]

Pythagorean triples

Equation (3), namely $x^2 + y^2 = r^2$, might look familiar from geometry: it is the same equation that governs the Pythagorean theorem for right triangles, as you can see if you take a right triangle with perpendicular sides of lengths x and y and hypotenuse of length r. Thus asking for solutions of (3) with x, y, r positive integers is the same as asking for right triangles of side lengths x, y, r. We might ask: given a fixed value for r, how many such triangles are there? If we let r vary freely, are there infinitely many such triangles?



Fermat's Last Theorem

Of course, we don't have to look at only squares of integers, like x^2. More generally, suppose we ask for positive integer solutions x, y, r to

$$x^3 + y^3 = r^3 \tag{5}$$

or

$$x^4 + y^4 = r^4. \tag{6}$$

How many integer solutions are there to these equations? These look very similar to equation (3) but the situation turns out to be very different! In fact, Fermat conjectured in 1637 that *there are no positive integer solutions to equations (5) and (6)!* This is part of what is known as Fermat's Last Theorem, which turned out to be so deep and difficult that it was only finally proved by Princeton professor Andrew Wiles (in coordination with other important contributors) in 1995.

[5]The questions posed below may be quite hard, very hard, or even unsolved, so don't worry if you can't answer them! We'll talk about them in more detail during the course.

Sums of squares

Looking at higher powers like x^3 and x^5 is one way to generalize equation (3), but we could also consider what happens when we stick with squares like x^2 but take sums of many squares. For example, we could ask for integer solutions to

$$x^2 + y^2 + z^2 + w^2 = r^2. \tag{7}$$

Given a fixed r, how many integer solutions to this equation are there? This is an important question that relates to *Lagrange's Four Squares Theorem.*

The twin prime conjecture

If you add prime numbers into the mix, things become even more difficult.[6] For example: the *Twin Prime Conjecture* asks if there are infinitely many pairs of prime numbers p, q that satisfy the equation

$$q = p + 2. \tag{8}$$

It is easy to spot a few examples of twin prime pairs, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, but are there infinitely many such pairs? We still don't know.[7]

The Goldbach conjecture

The *Goldbach Conjecture* proposes that every even number $N > 2$ may be written as a sum of two odd prime numbers:

$$N = p + q. \tag{9}$$

We don't know if this is true either.

[6] Recall that a number p is prime if it is divisible only by itself and 1. The first few prime numbers are $2, 3, 5, 7, 11, 13....$

[7] If we remove the restriction that p and q be prime in equation (8) and simply ask for real number solutions to the equation $y = x + 2$, what geometric object does this describe? Are there infinitely many real number solutions (x, y) to this equation? This is a striking example of how easy it can be to find real number solutions, while it is so hard to find prime solutions.