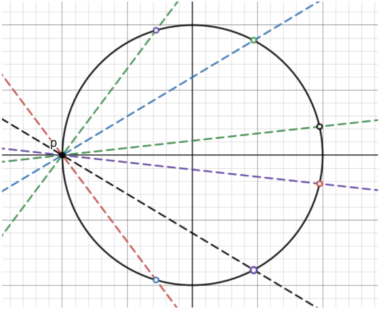
Lecture 2: Heights

Brian Lehmann
Boston College

Counting points

Last time we saw how to classify all Pythagorean triples. A key idea was using the geometry of the circle $x^2 + y^2 = 1$.



Finding rational points

Counting points

Today we are going to "count" Pythagorean triples.

Of course, since there are infinitely many we do not literally "count" them. Instead, we will analyze how many tuples (a, b, c) there are such that

$$\max\{|a|, |b|, |c|\} \leq T$$

for some positive number T. This gives us a sense of "how dense" Pythagorean triples are inside all triples of integers.

Warm-up problem

We start with a warm-up problem which is similar to our original problem, but has a few key differences that make it easier to understand.

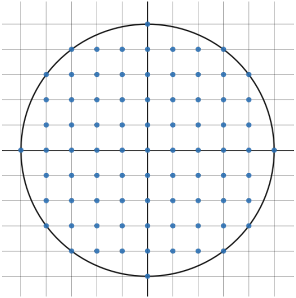
Question

Fix a positive number r. How many pairs of integers (x, y) satisfy $x^2 + y^2 \leq r^2$?

In other words: how many integer points in $\mathbb{R}^2$ have distance $\leq r$ from the origin?

Warm-up problem

Geometrically, we are counting the number of integer points in the ball $B_0(r)$ of radius r centered at the origin.



81 integer points in $B_0(5)$

Counting these integer points is known as "Gauss' circle problem."

Warm-up problem

We let $N(r)$ denote the number of integer pairs (x, y) such that $x^2 + y^2 \leq r^2$. The following table records $N(r)$ for some small integer values of r:

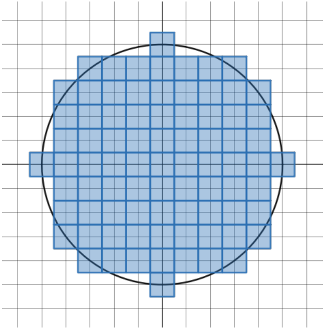
r	1	2	3	4	5	6	7	8	9	10
N(r)	5	13	29	49	81	113	149	197	253	317

It looks like $N(r)$ grows proportionally to r^2.

Estimate

Here is a heuristic argument justifying this estimate.

For each integer point $p \in B_0(r)$, let's draw a square of side length 1 centered at p. The overlap of these squares has zero area and the union of these squares is roughly the circle $B_0(r)$.



Estimate

Comparing areas, we see that

$$N(r) \approx \pi r^2.$$

r	1	2	3	4	5	6	7	8	9	10
N(r)	5	13	29	49	81	113	149	197	253	317
round(πr^2)	3	13	28	50	79	113	154	201	254	314

This estimate is pretty good! Our real goal is to control the error term: if we write $N(r) = \pi r^2 + E(r)$, can we put an upper bound on $|E(r)|$?

Gauss' result

Theorem (Gauss)

$$\pi r^2 - \sqrt{2}\pi r + \frac{1}{2} \leq N(r) \leq \pi r^2 + \sqrt{2}\pi r + \frac{1}{2}$$

It is common to write

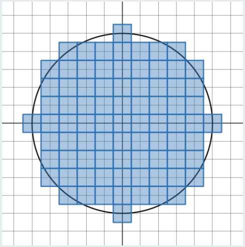
$$N(r) = \pi r^2 + O(r)$$

to signify that the error term is bounded by a linear function in r, namely, $|E(r)| \leq \sqrt{2}\pi r + \frac{1}{2}$.

Gauss' result

Proof

For each integer point $p \in B_0(r)$, consider the square with unit side length centered at p. Take the union of all such squares to get a shape $R \subset \mathbb{R}^2$.



Gauss' result

Proof

Suppose that x is a point in R. By definition, there is some integer point p in $B_0(r)$ such that x is contained in the unit square centered at p. By the triangle inequality,

$$\begin{aligned} d(x,\vec{0}) &\leq d(x,p) + d(p,\vec{0}) \\ &\leq \frac{1}{\sqrt{2}} + r \end{aligned}$$

We conclude that $x \in B_0(r + \frac{1}{\sqrt{2}})$. In other words,

$$R \subset B_0\left(r + \frac{1}{\sqrt{2}}\right).$$

Gauss' result

Proof

Conversely, suppose that $y \in B(r - \frac{1}{\sqrt{2}})$. Every point in $\mathbb{R}^2$ is at most $\frac{1}{\sqrt{2}}$ away from the closest integer point. If we let p denote the closest integer point to y, then

$$\begin{aligned} d(p, \vec{0}) &\leq d(p, y) + d(y, \vec{0}) \\ &\leq \frac{1}{\sqrt{2}} + \left(r - \frac{1}{\sqrt{2}}\right) \\ &= r \end{aligned}$$

Since $p \in B_0(r)$, we conclude that $y \in R$. In other words,

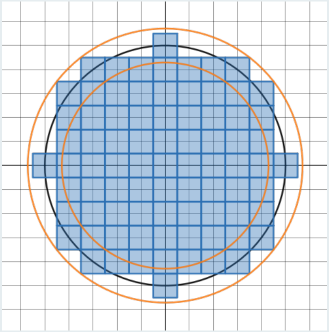
$$B_0\left(r - \frac{1}{\sqrt{2}}\right) \subset R.$$

Gauss' result

Proof

In sum,

$$B_0\left(r - \frac{1}{\sqrt{2}}\right) \subset R \subset B_0\left(r + \frac{1}{\sqrt{2}}\right)$$



Counting points

Gauss' circle problem

Counting rational points

Gauss' result

Proof.

Thus

$$\mathrm{area}\left(B_0\left(r-\frac{1}{\sqrt{2}}\right)\right)\leq \mathrm{area}(R)\leq \mathrm{area}\left(B_0\left(r+\frac{1}{\sqrt{2}}\right)\right).$$

Computing areas, we see that

$$\pi\left(r-\frac{1}{\sqrt{2}}\right)^2\leq N(r)\leq \pi\left(r+\frac{1}{\sqrt{2}}\right)^2.$$

□

Conjecture

Modern mathematicians have improved the bound on the error term. The conjectural "best" bound is:

Conjecture

$N(r) = \pi r^2 + O(r^{\frac{1}{2}+\epsilon})$.

It is known that the exponent must be $> \frac{1}{2}$ (Hardy), but the precise value is not known! The current best upper bound on the exponent is $0.6274\ldots$.

Primitive circle problem

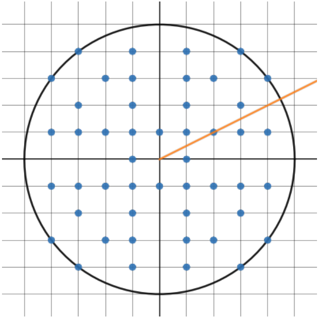
We next "upgrade" our question with a harder variant.

Question

Fix a positive number r. How many **relatively prime** pairs of integers (x, y) satisfy $x^2 + y^2 \leq r^2$?

This is known as the primitive circle problem.

Primitive circle problem



Primitive circle problem

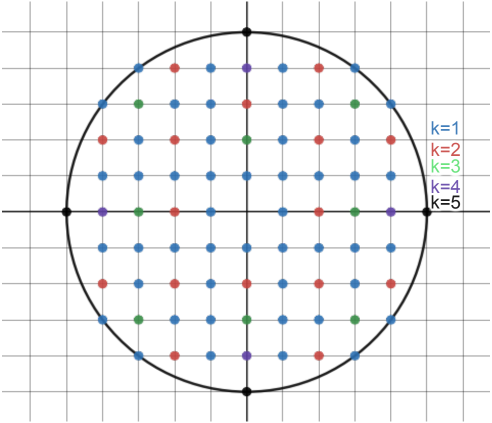
Each primitive point is the "first one" on the ray connecting it to the origin.

Primitive circle problem

Let $N^{prim}(r)$ denote the number of relatively prime pairs of integers (x, y) with $x^2 + y^2 \leq r^2$. We will estimate this value by relating it to $N(r)$.

Every point (x, y) in $B_0(r)$ except for $(0, 0)$ has a unique expression $k \cdot (x_{prim}, y_{prim})$ where k is a positive integer k and (x_{prim}, y_{prim}) is relatively prime. We let $N(r, k)$ denote the number of points in $B_0(r)$ which are associated to the number k.

Primitive circle problem



Different k values

Primitive circle problem

We have two important equations. First, every point with non-zero coordinates has some k associated to it:

$$N(r) = 1 + \sum_{k=1}^{r} N(r,k).$$

(Here the 1 accounts for the origin.)

Second, every point counted by $N(r,k)$ will be a primitive point if we scale down by k:

$$N(r,k) = N^{prim}\left(\frac{r}{k}\right).$$

Primitive circle problem

Counting points

Gauss' circle problem

Counting rational points

Combining these two equations:

$$N(r) = 1 + \sum_{k=1}^{r} N^{prim}\left(\frac{r}{k}\right).$$

In this situation one can “reverse” the roles of N^{prim} and N using the Mobius inversion formula:

$$N^{prim}(r) = \sum_{k=1}^{r} \mu(k)\left(N\left(\frac{r}{k}\right) - 1\right).$$

It would take a little time to set up Mobius inversion, so instead we will use a (less rigorous) heuristic argument to estimate the size of $N^{prim}(r)$.

Primitive circle problem

We already know that $N(r) \approx \pi r^2$ and we would like to find an approximation $N^{prim}(r) \approx Cr^2$. Let's substitute this into our equation:

$$\begin{aligned}\pi r^2 &\approx \sum_{k=1}^{r} C\left(\frac{r}{k}\right)^2 \\ &\approx Cr^2\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{r^2}\right)\end{aligned}$$

Solving for C and taking a limit as $r \to \infty$, we have

$$C \approx \frac{\pi}{\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots\right)}$$

Primitive circle problem

The famous Riemann zeta function has made an appearance!

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots$$

In fact, by Euler's solution to the Basel problem we know the precise value of this series: $\zeta(2) = \frac{\pi^2}{6}$. Substituting backwards, we see that $C = \frac{6}{\pi}$, or equivalently:

$$N^{prim}(r) \approx \frac{6}{\pi} r^2.$$

A more careful argument using Mobius inversion shows that

$$N^{prim}(r) = \frac{6}{\pi} r^2 + O(r \log r).$$

Counting rational points

Now we return to the setting of Pythagorean triples. In keeping with our geometric theme, we will focus on rational points on the circle $x^2 + y^2 = 1$. How can we measure the "size" of a rational point?

Definition

Let (x, y) be a non-zero point with rational coordinates. There is a unique (up to sign) triple of relatively prime integers (a, b, c) such that $x = \frac{a}{c}$ and $y = \frac{b}{c}$. The height of the point is

$$H(x, y) = \max\{|a|, |b|, |c|\}.$$

Counting rational points

The height is a measure of the "arithmetic complexity" of a point: what is the size of the numbers needed to write the fractions defining the point?

Example: $H(\frac{3}{5}, \frac{4}{5}) = \max\{|3|, |4|, |5|\} = 5$.

Note that points that are close together can have very different heights. For example, $H(1, 0) = 1$ but $H(1, \frac{1}{100}) = 100$.

Counting rational points

Question

Fix a positive number T. How many rational points (x, y) on the circle $x^2 + y^2 = 1$ satisfy $H(x, y) \leq T$?

Note that for rational points on the circle the height is particularly easy to compute. Indeed, every such point has the form $(\frac{a}{c}, \frac{b}{c})$ where $a^2 + b^2 = c^2$. Thus we simply have

$$H(x, y) = |c|.$$

Counting rational points

The previous question can be rephrased by clearing denominators:

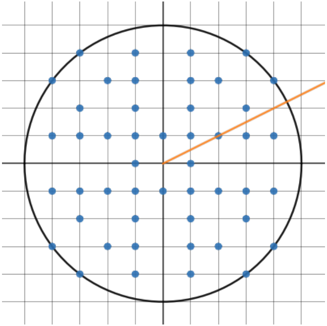
Question

Fix a positive number T. How many relatively prime pairs of integers (x, y) satisfy $x^2 + y^2 \leq T^2$ **and** $x^2 + y^2$ is the square of an integer?

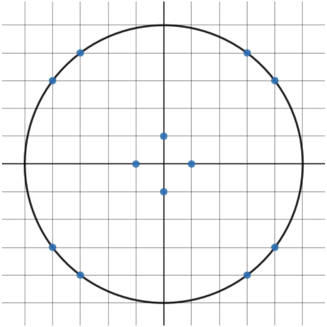
We will let $M(T)$ denote the number of relatively prime pairs of integers (x, y) which satisfy $x^2 + y^2 \leq T^2$ and $x^2 + y^2$ is the square of an integer.

Counting rational points

This is very close to the primitive circle problem, but looks much harder due to the "gaps" in our counting problem!



Primitive circle problem



Height problem

Rational parametrizations

The key idea is to use the parametrization of the circle from last time.

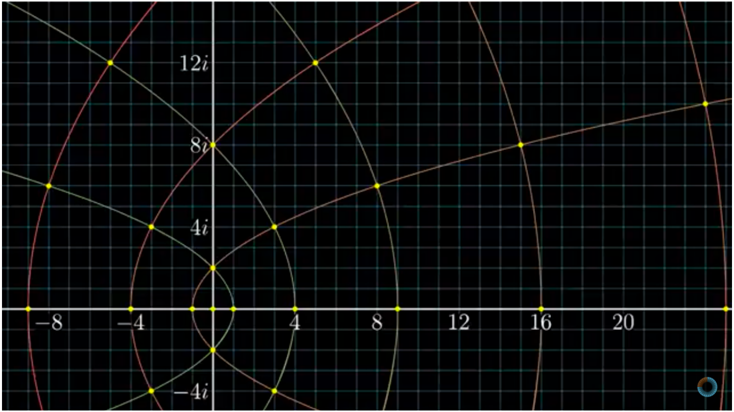
We will "clear denominators" to write the parametrization as a 2-variable map instead of a 1-variable map:

$$\varphi : (m, n) \mapsto (m^2 - n^2, 2mn)$$

Remember, when m, n are integers then the quantities $m^2 - n^2, 2mn$ are the first two entries in a Pythagorean triple (whose last entry is $m^2 + n^2$).

Note that φ is the same as the squaring map $z \mapsto z^2$ in complex analysis!

Rational parametrizations



https://youtube.com/clip/UgkxHflmOEnVwvKAULWpj-86pB-aNxUVfRkO

Rational parametrizations

The good news is that the map

$$\varphi : (m, n) \mapsto (m^2 - n^2, 2mn)$$

allows us to turn our original problem into an easier problem:

Key Observation

Counting relatively prime integer pairs (x, y) such that $x^2 + y^2$ is a perfect square and $x^2 + y^2 \leq T^2$ is roughly the same as counting relatively prime integer pairs (m, n) such that $m^2 + n^2 \leq T$.

We first need to put in some hard work relating the pairs (x, y) and the pairs (m, n).

Rational parametrizations

The following theorem describes how φ interacts with Pythagorean triples.

Theorem

Suppose that (x, y) is a relatively prime pair of integers such that $x^2 + y^2$ is the square of an integer. Then one of x, y is even and the other is odd.

1. *If y is even, there are two relatively prime pairs (m, n) satisfying $\varphi(m, n) = (x, y)$.*
2. *If x is even, there are two relatively prime pairs (m, n) satisfying $\varphi(m, n) = (2x, 2y)$.*

Conversely, if (m, n) is a relatively prime pair of integers then $\varphi(m, n)$ falls into one of the two categories above.

Counting using parametrization

Consider all relatively prime pairs (m, n) satisfying $m^2 + n^2 \leq T$. For each such (m, n) its image will have the form (x, y) or $(2x, 2y)$ for a relatively prime pair (x, y) such that $x^2 + y^2$ is the square of an integer.

- If y is even, then

  $$x^2 + y^2 = (m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$$

  is at most T^2.

- If x is even, then

  $$(2x)^2 + (2y)^2 = (m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$$

  is at most T^2. In other words, $x^2 + y^2 \leq \frac{T^2}{4}$.

Counting using parametrization

Next let's identify the sizes of the various sets:

- The number of relatively prime pairs (m, n) satisfying $m^2 + n^2 \leq T$ is $N^{prim}(\sqrt{T})$.
- The number of relatively prime pairs (x, y) such that y is even and $x^2 + y^2$ is the square of an integer $\leq T^2$ is $\frac{1}{2}M(T)$.
- The number of relatively prime pairs (x, y) such that x is even and $x^2 + y^2$ is the square of an integer $\leq \frac{T^2}{4}$ is $\frac{1}{2}M(\frac{T}{2})$.

Altogether we have

$$\frac{1}{2}N^{prim}(\sqrt{T}) = \frac{1}{2}M(T) + \frac{1}{2}M\left(\frac{T}{2}\right).$$

(The left-hand side includes the factor $1/2$ to account for the fact that φ is 2-to-1.)

Counting using parametrization

We can isolate $M(T)$ by repeated substitution:

$$\begin{aligned}
M(T) &= N^{prim}(\sqrt{T}) - M\left(\frac{T}{2}\right) \\
&= N^{prim}(\sqrt{T}) - \left(N^{prim}\left(\sqrt{\frac{T}{2}}\right) - M\left(\frac{T}{4}\right)\right) \\
&= N^{prim}(\sqrt{T}) - N^{prim}\left(\sqrt{\frac{T}{2}}\right) + \left(N^{prim}\left(\sqrt{\frac{T}{4}}\right) - M\left(\frac{T}{8}\right)\right) \\
&= \dots
\end{aligned}$$

Counting using parametrization

Since $N^{prim}(T)$ approaches 0 as $T \to 0$, this alternating series has a limit:

$$M(T) = \sum_{k=0}^{\infty} (-1)^k N^{prim}\left(\sqrt{\frac{T}{2^k}}\right).$$

We can now use the fact that $N^{prim}(r) \approx \frac{6}{\pi} r^2$:

$$\begin{aligned} M(T) &\approx \sum_{k=0}^{\infty} (-1)^k \frac{6}{\pi} \left(\frac{T}{2^k}\right) \\ &\approx \frac{6T}{\pi} \sum_{k=0}^{\infty} \frac{(-1)^k}{2^k} \\ &\approx \frac{4T}{\pi} \end{aligned}$$

Summary

We have achieved our goal of counting how many rational points on the circle have height at most T.

Theorem

Let $M(T)$ denote the number of rational points on the circle $x^2 + y^2 = 1$ which have height at most T. Then

$$M(T) \approx \frac{4}{\pi} T.$$

This is a special case of the Batyrev-Manin Conjecture which predicts the asymptotic growth rate of $M(T)$ for a more general set of polynomial equations.

Exercises

Exercises:

1. Sums of squares: study sums of the form $x^2 + y^2$ using properties of complex numbers.
2. Lattice points and area: can we generalize Gauss' circle problem to other shapes? What is the relationship between the area of a shape in $\mathbb{R}^2$ and the number of lattice points it contains?

Images made using Desmos and taken from 3Blue1Brown.