GAUSS'S CIRCLE PROBLEM

UPDATE: These are old course notes which are no longer being revised. For the most recent version please see my "pre-book" at `www.math.uga.edu/~pete/4400FULL.pdf`, in which this handout appears as Chapter 12.

1. Introduction

We wish to study a very classical problem: how many lattice points lie on or inside the circle $x^2 + y^2 = r^2$? Equivalently, for how many pairs $(x, y) \in \mathbb{Z}^2$ do we have $x^2 + y^2 \leq r^2$? Let $L(r)$ denote the number of such pairs.

Upon gathering a bit of data, it becomes apparent that $L(r)$ grows quadratically with r, which leads to consideration of $\frac{L(r)}{r^2}$. Now:

$$L(10)/10^2 = 3.17.$$

$$L(100)/100^2 = 3.1417.$$

$$L(1000)/1000^2 = 3.141549.$$

$$L(10^4)/10^8 = 3.14159053.$$

The pattern is pretty clear!

Theorem 1. *As $r \to \infty$, we have $L(r) \sim \pi r^2$. Explicitly,*

$$\lim_{r\to\infty} \frac{L(r)}{\pi r^2} = 1.$$

Once stated, this result is quite plausible geometrically: suppose that you have to tile an enormous circular bathroom with square tiles of side length 1 cm. The total number of tiles required is going to be very close to the area of the floor in square centimeters. Indeed, starting somewhere in the middle you can do the vast majority of the job without even worrying about the shape of the floor. Only when you come within 1 cm of the boundary do you have to worry about pieces of tiles and so forth. But the number of tiles required to cover the boundary is something like a constant times the perimeter of the region in centimeters – so something like $C\pi r$ – whereas the number of tiles in the interior is close to πr^2. Thus the contribution to the boundary is neglible: precisely, when divided by r^2, b it approaches 0 as $r \to \infty$.

I myself find this heuristic convincing but not quite rigorous. More precisely, I believe it for a circular region and become more concerned as the boundary of the region becomes more irregularly shaped, but the heuristic doesn't single out exactly what nice properties of the circle are being used. Moreover the "error" bound is fuzzy: it would be useful to know an explicit value of C.

To be more quantitative about it, we define the error

$$E(r) = |L(r) - \pi r^2|,$$

so that Theorem 1 is equivalent to the statement

$$\lim_{r\to\infty} \frac{E(r)}{r^2} = 0.$$

The above heuristic suggests that $E(r)$ should be bounded above by a linear function of r. The following elementary result was proved by Gauss in 1837.

Theorem 2. *For all $r \geq 7$, $E(r) \leq 10r$.*

Proof. Let $P = (x, y) \in \mathbb{Z}^2$ be such that $x^2 + y^2 \leq r^2$. To P we associate the square $S(P) = [x, x + 1] \times [y, y + 1]$, i.e., the unit square in the plane which has P as its lower left corner. Note that the diameter of $S(P)$ – i.e., the greatest distance between any two points of $S(P)$ – is $\sqrt{2}$. So, while P lies within the circle of radius r, $S(P)$ may not, but it certainly lies within the circle of radius $r + \sqrt{2}$. It follows that the total area of all the squares $S(P)$ – which is nothing else than the number $L(r)$ of lattice points – is at most the area of the circle of radius $r + \sqrt{2}$, i.e.,

$$L(r) \leq \pi(r + \sqrt{2})^2 = \pi r^2 + 2\sqrt{2}\pi r + 2.$$

A similar argument gives a lower bound for $L(r)$. Namely, if (x, y) is any point with distance from the origin at most $r - \sqrt{2}$, then the entire square $(\lfloor x\rfloor, \lfloor x + 1\rfloor) \times (\lfloor y\rfloor, \lfloor y + 1\rfloor)$ lies within the circle of radius r. Thus the union of all the unit squares $S(P)$ attached to lattice points on or inside $x^2 + y^2 = r$ covers the circle of radius $r - \sqrt{2}$, giving

$$L(r) \geq \pi(r - \sqrt{2})^2 = \pi r^2 - 2\sqrt{2}\pi r + 2.$$

Thus

$$E(r) = |L(r) - \pi r^2| \leq 2\pi + 2\sqrt{2}\pi r \leq 7 + 9r \leq 10r,$$

the last inequality holding for all $r \geq 7$. □

This argument skillfully exploits the geometry of the circle. I would like to present an alternate argument with a much different emphasis.

The first step is to notice that instead of counting lattice points in an expanding sequence of closed disks, it is equivalent to fix the plane region once and for all – here, the unit disk $D : x^2 + y^2 \leq 1$ – and consider the number of points $(x, y) \in \mathbb{Q}^2$ with $rx, ry \in \mathbb{Z}$. That is, instead of dividing the plane into squares of side length one, we divide it into squares of side length $\frac{1}{r}$. If we now count these "$\frac{1}{r}$-lattice points" inside D, a moment's thought shows that this number is precisely $L(r)$.

Now what sort of thing is an area? In calculus we learn that areas are associated to integrals. Here we wish to consider the area of the unit disk as a **double integral** over the square $[-1, 1]^2$. In order to do this, we need to integrate the **characteristic function** χ_D of the unit disk: that is, $\chi(P)$ evaluates to 1 if $P \in D$ and $\chi(P) = 0$ otherwise. Now the division of the square $[-1, 1]^2$ into $4r^2$ subsquares of side length $\frac{1}{r}$ is exactly the sort of sequence of partitions that we need to define a Riemann sum: that is, the maximum diameter of a subrectangle in the partition is $\frac{\sqrt{2}}{r}$, which tends to 0 as $r \to \infty$. Therefore if we choose any point $P^*_{i,j}$ in each subsquare, then

$$\Sigma_r := \frac{1}{r^2} \sum_{i,j} \chi(P^*_{i,j})$$

is a sequence of Riemann sums for χ_D, and thus

$$\lim_{r\to\infty} \Sigma_r = \int_{[-1,1]^2} \chi_D = \text{Area}(D) = \pi.$$

But we observe that Σ_r is very close to the quantity $L(r)$. Namely, if we take each sample point to be the lower left corner of corner of the corresponding square, then $r^2\Sigma_r = L(r) - 2$, because every such sample point is a lattice point (which gets multiplied by 1 iff the point lies inside the unit circle) and the converse is true except that the points $(1,0)$ and $(0,1)$ are not chosen as sample points. So

$$\lim_{r\to\infty} \frac{L(r)}{r^2} = \lim_{r\to\infty} \frac{L(r)-2+2}{r^2} = \lim_{r\to\infty} \Sigma_r + 0 = \pi.$$

The above argument is less elementary than Gauss's and gives a weaker result: no explicit upper bound on $E(r)$ is obtained. So why have we bothered with it? The answer lies in the generality of this latter argument. We can replace the circle by any **plane region** $R \subset [-1,1]^2$. For any $r \in \mathbb{R}^{>0}$, we define the r-dilate of R,

$$rR = \{rP \mid P \in R\}.$$

This is a plane region which is "similar" to R in the usual sense of Euclidean geometry. Note that if $R = D$ is the closed unit disk then $rD = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq r^2\}$ is the closed disk of radius r. Therefore a direct generalization of the counting function $L(r)$ is

$$L_R(r) = \#\{(x,y) \in \mathbb{Z}^2 \cap rR\}.$$

As above, we can essentially view $\frac{L_R(r)}{r^2}$ as a sequence of Riemann sums for $\int_{[-1,1]^2} \chi_R$ – "essentially" because any lattice points with x or y coordinate equal to 1 exactly will contribute to $L_R(r)$ but not to the Riemann sum. But since the total number of $\frac{1}{r}$-squares which touch the top and/or right sides of the square $[-1,1]^2$ is $4r+1$, this discrepancy goes to 0 when divided by r^2. (Another approach is just to assume that R is contained in the interior $(-1,1)^2$ of the unit square. It should be clear that this is no real loss of generality.) We get the following result:

Theorem 3. *Let $R \subset [-1,1]^2$ be a planar region. Then*

$$\lim_{r\to\infty} \frac{L_R(r)}{r^2} = \text{Area}(R). \tag{1}$$

There is a remaining technical issue: what exactly do we mean by a "plane region"?[1] Any subset of $[-1,1]^2$? A Lebesgue measurable subset? Neither of these answers is correct: take

$$I = \{(x,y) \in [-1,1]^2 \mid x,y \in \mathbb{R} \setminus \mathbb{Q}\},$$

i.e., the subset of the square $[-1,1]^2$ consisting of points both of whose coordinates are irrational. Then I is obtained by removing from $[-1,1]^2$ a set of Lebesgue measure zero, so I has Lebesgue measure 4 and thus $\int_{[-1,1]^2} \chi_I$ exists in the Lebesgue sense and is equal to 4. On the other hand, I contains no rational points whatsoever, so for all $r \in \mathbb{Z}^+$, $L_R(r) = 0$. Thus, if we restrict r to positive integral values, then both sides of (1) are well-defined, but they are unequal: $0 \neq 4$.

[1]The reader without a strong undergraduate background in real analysis can safely ignore this discussion.

Looking back at the argument, what is needed is precisely the **Riemann integrability** of the characteristic function χ_D of the region D. It is a basic fact that a bounded function on a bounded domain is Riemann integrable if and only if it is continuous except on a set of measure zero. The characteristic function χ_D is discontinuous precisely along the boundary of D, so the necessary condition on D is that its boundary have measure zero. (Explicitly, this means that for any $\epsilon > 0$, there exists an infinite sequence R_i of open rectangles whose union covers D and such that the sum of the areas of the rectangles is convergent and less than or equal to ϵ.) In geometric measure theory, such regions are called **Jordan measurable**, and this is the condition we need on our "planar region".

Jordan measurability is a relatively mild condition on a region: for instance any region bounded by a piecewise smooth curve (a circle, ellipse, polygon...) is Jordan measurable. In fact a large collection of regions with fractal boundaries are Jordan measurable: for instance Theorem 3 applies with R a copy of the **Koch snowflake**, whose boundary is a nowhere differentiable curve.

2. The Question of Better Bounds

2.1. **The soft/hard dichotomy.** As in the previous section, suppose we have a plane region $R \subset [-1,1]^2$, and consider the function $L_R(r)$ which counts the number of lattice points in the dilate rR of R. The main qualitative, or **soft**, result of the last section was

$$L_R(r) \sim \text{Area}(R)r^2.$$

But if we take a more *quantitative*, or **hard**, view, this is only the beginning. Namely, as before, we define

$$E_R(r) = |L_R(r) - \text{Area}(R)r^2|.$$

Theorem 3 tells us that $\lim_{r\to\infty} E_R(r) = 0$: this is a fundamentally soft-analytic result. A hard-analytic result would give an explicit upper bound on $E_R(r)$. Theorem 1 does just this, albeit in the special case where R is the closed unit disk:

$$E_R(r) \leq 10r.$$

Here are some natural questions:

Question 1. *(Gauss's Circle Problem) In the case of $R = D$, how much can one improve on Gauss's bound $E_D(r) \leq 10r$? Can we find nontrivial lower bounds? What is the "truth" about $E_D(r)$?*

Question 2. *Can one give an explicit upper bound on $E_R(r)$ for an arbitrary plane region R? Could we have, for instance, that $E_r(R)$ is always bounded by a linear function of r? Or by an even smaller power of r?*

Question 1 has received much attention over the years. Let's look again at the data:

$$r = 10: \; L(r) = 317, \; \pi r^2 \approx 314, \; E(r) = 2.8407\ldots$$

$$r = 100: \; L(r) = 31417, \; \pi r^2 \approx 31415.926, \; E(r) = 1.0734\ldots$$

$$r = 1000: \; L(r) = 3141549, \pi r^2 \approx 3141592.653, \; E(r) = 43.653\ldots$$

$$r = 10000: \; L(r) = 314159053, \; \pi r^2 \approx 314159265.358, \; E(r) = 212.3589\ldots$$

We now attempt to describe $E(r)$ by a **power law**: i.e., to find a real number α such that $E(r)$ grows like r^α. If $E(r) \approx r^\alpha$, then $\log E(r) \approx \alpha \log r$, so that to test for a power law we should consider the ratio $P(r) := \frac{\log E(r)}{\log r}$ and see whether it tends towards some constant α as $r \to \infty$. We have at the moment only four values of r, so this is quite rough, but nevertheless let's try it:

$$r = 10 : P(r) = .453\ldots,$$

$$r = 100 : P(r) = .01538\ldots,$$

$$r = 1000 : P(r) = .54667\ldots,$$

$$r = 10000 : P(r) = .5817\ldots.$$

Whatever is happening is happening quite slowly, but it certainly seems like $E(r) \leq Cr^\alpha$ for some α which is safely less than 1.

The first theoretical progress was made in 1904 by a Polish undergraduate, in competition for a prize essay sponsored by the departments of mathematics and physics at the University of Warsaw. The student showed that there exists a constant C such that $E_D(r) \leq Cr^{\frac{2}{3}}$. His name was **Waclaw Sierpinski**, and this was the beginning of a glorious mathematical career.[2]

On the other hand, in 1916 G.H. Hardy and E. Landau, independently, proved that *there does not exist* a constant C such that $E(r) \leq Cr^{\frac{1}{2}}$. The conventional wisdom however says that $r^{\frac{1}{2}}$ is very close to the truth: namely, it is believed that for every real number $\epsilon > 0$, there exists a constant C_ϵ such that

$$E(r) \leq C_\epsilon r^{\frac{1}{2}+\epsilon}. \tag{2}$$

Remark: It is not hard to show that this conjecture implies that

$$\lim_{r\to\infty} P(r) = \lim_{r\to\infty} \frac{\log E(r)}{\log r} = \frac{1}{2}.$$

(Note that the calculations above certainly are not sufficient to suggest this result. It would therefore be interesting to extend these calculations and see if convergence to $\frac{1}{2}$ becomes more apparent.)

Note that Theorem 1 above tells us we can take $\epsilon = \frac{1}{2}$ and $C_\epsilon = 10$, whereas Sierpinski showed that we can take $\epsilon = \frac{1}{6}$.[3] The best current bound was proven by Huxley in 1993: he showed that (2) holds for every $\epsilon > 19/146 = 0.13\ldots$. In early 2007 a preprint of Cappell and Shaneson appeared on the arxiv, which claims to establish (2) for every $\epsilon > 0$. As of this writing (Spring of 2009) the paper has not been published, nor do I know any expert opinion on its correctness.

As for Question 2, we begin with the following simple but enlightening example.

[2]Sierpinski (1882-1969) may well be the greatest Polish mathematician of all time, and Poland is a country with an especially distinguished mathematical tradition. Sierpinski is most remembered nowadays for the fractal triangle pattern that bears his name. I have encountered his work several times over the years, and the work on the Gauss Circle Problem is typical of his style: his theorems have elementary but striking statements and difficult, intricate proofs.

[3]I don't know what value he had for $C_{\frac{1}{3}}$ or even whether his proof gave an explicit value.

Example: Let $R = [-1, 1]^2$ be the square of sidelength 2 centered at the origin. Then $\text{Area}(R) = 4$, so that for any $r \in \mathbb{R}^+$ we have $\text{Area}(rR) = 4r^2$. On the other hand, for $r \in \mathbb{Z}^+$, we can determine $L_R(r)$, the number of lattice points in $[-r, r]^2$ exactly: there are $2r + 1$ possible values for the x coordinate and the same number of possible values for the y-coordinate, so that $L_r(R) = (2r + 1)^2 = 4r^2 + 4r + 1$. In this case we have

$$E_R(r) = |L_r(R) - \text{Area}(rR)| = 4r + 1,$$

so that the true error is a linear function of r. This makes us appreciate Sierpinski's result more: to get a bound of $E_D(r) \leq Cr^\alpha$ for some $\alpha < 1$ one does need to use properties specific to the circle: in the roughest possible terms, there cannot be as many lattice points on the boundary of a curved region as on a straight line segment.

More formally, in his 1919 thesis van der Corput proved the following result:

Theorem 4. *Let $R \subset \mathbb{R}^2$ be a bounded planar region whose boundary is C^∞-smooth and with nowhere vanishing curvature. Then there exists a constant C (depending on R) such that for all sufficiently large $r \in \mathbb{R}^{>0}$,*

$$|L_R(r) - \text{Area}(R)r^2| \leq Cr^{\frac{2}{3}}.$$

It is also known that this result is best possible – there are examples of regions with very nice boundaries in which the power $\frac{2}{3}$ cannot be lowered. (Thus again, the circle is very special!) There are many results which study how the behavior of the error term depends on the assumptions one makes about the boundary of R. To go to the other extreme, a 1997 result of L. Colzani shows that for any bounded region R whose boundary has fractal dimension at most α (this has a technical meaning particular to Colzani's paper; we do not give an explicit definition here), then

$$|L_r(R) - \text{Area}(R)r^2| \leq Cr^{2-\alpha}.$$

As far as I know, it is an **open problem** to give corresponding lower bounds: for instance, to construct, for any $\epsilon > 0$, a region R such that $|L_r(R) - \text{Area}(R)r^2| > r^{2-\epsilon}$ for infinitely many positive integers r. (I myself do not know how to construct such a region for *any* $\epsilon < 1$.)

3. Connections to average values

The reader may well be wondering why the Gauss Circle Problem counts as number theory. On the one hand, as we will see later on, number theory is very much concerned with counting lattice points in certain planar and spatial reasons. But more specifically, Gauss' Circle Problem has to do with the average value of an arithmetical function.

Namely, define $r_2(n)$ to be the function which counts the number of integers (x, y) such that $n = x^2 + y^2$. The Full Two Squares Theorem says that $r_2(n) > 0$ iff $2 \mid \text{ord}_p(n)$ for every $p \equiv 3 \pmod 4$. As you have seen in the homework, in practice this condition behaves quite erratically. Certainly the function $r_2(n)$ does not have any nice limiting behavior at $n \to \infty$: on the one hand it is 0 infinitely often, and on the other hand it assumes arbitrarily large values.

Much more regularity is displayed by the function $r_2(n)$ "on average." Namely, for any function $f : \mathbb{Z}^+ \to \mathbb{C}$, we define a new function

$$f_{\mathrm{ave}} : n \mapsto \frac{1}{n}\left(f(1) + \ldots + f(n)\right).$$

As its name suggests, $f_{\mathrm{ave}}(n)$ is the average of the first n values of f.

It is also convenient to work also with the summatory function $F(n) := \sum_{k=1}^n f(k)$. The relation between them is simple:

$$F(n) = n \cdot f_{\mathrm{ave}}(n).$$

Now we claim that we already know the asymptotic behavior of the average value for $r_2(n)$.

Theorem 5. *For $f(n) = r_2(n)$, $F(n) \sim \pi n$ and $f_{\mathrm{ave}}(n) \sim \pi$.*

Proof. Indeed, $F(n) = r_2(1) + \ldots + r_2(n)$ counts the number of lattice points on or inside the circle $x^2 + y^2 \leq n$, exceping the origin. Therefore

$$F(n) = L_D(\sqrt{n}) - 1 \sim \pi(\sqrt{n})^2 - 1 \sim \pi n.$$

□

In this context, the Gauss Circle Problem is equivalent to studying the error between $F(n)$ and πn. Studying errors in asymptotic expansions for arithmetic functions is one of the core topics of analytic number theory.

We remark with amusement that the average value of $r_2(n)$ is asymptotically constant and equal to the irrational number π: obviously there is no n for which $r_2(n) = \pi$ exactly!

In fact there is a phenomenon here that we should take seriously. A natural question is how often is $r_2(n) = 0$? We know that $r_2(n) = 0$ for all $n = 4k + 3$, so it is equal to zero at least $\frac{1}{4}$ of the time. But the average value computation allows us to do better. Suppose that there exists a number $0 < \alpha \leq 1$ such that $r_2(n) = 0$ at most α proportion of the time. Then $r_2(n) < 0$ at least $1 - \alpha$ of the time, so the average value of $r_2(n)$ is at least $8(1 - \alpha)$. Then $\pi \geq 8(1 - \alpha)$, or

$$\alpha \geq 1 - \pi/8 \approx .607.$$

That is, we've shown that $r_2(n) = 0$ more than 60% of the time.[4]

In fact this only hints at the truth. In reality, $r_2(n)$ is equal to zero "with probability one". In other words, if we pick a large number N and choose at random an elment $1 \leq n \leq N$, then the probability that n is a sum of two squares approaches 0 as $N \to \infty$. This exposes one of the weaknesses of the arithmetic mean (one that those who compose and grade exams become well aware of): without further assumptions it is unwarranted to assume that the mean value is a "typical" value in any reasonable sense. To better capture the notion of typicality one can import further statistical methods and study the **normal order** of an arithmetic function. With regret, we shall have to pass this concept over entirely as being too delicate

[4]This argument was not intended to be completely rigorous, and it isn't. What it really shows is that it is *not* the case that $r_2(n) = 0$ on a set of density at least $\alpha = 1 - \pi/8$ (the density of a subset of integers is defined in [Primes: Infinitude, Density and Substance]). But this is morally the right conclusion: see below.

for our course. See for instance G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, for an excellent treatment.

The lattice point counting argument generalizes straightforwardly (but fruitfully) to higher-dimensional Euclidean space $\mathbb{R}^N$. For instance, the analogous argument involving lattice points on or inside the sphere of radius r in $\mathbb{R}^3$ gives:

Theorem 6. *The number $R_3(r)$ of integer solutions (x, y, z) to $x^2 + y^2 + z^2 \leq r^2$ is asymptotic to $\frac{4}{3}\pi r^3$, with error being bounded by a constant times r^2.*

Corollary 7. *The average value of the function $r_3(n)$, which counts representations of n by sums of three integer squares, is asymptotic to $\frac{4}{3}\pi\sqrt{n}$.*

We can similarly compute nice asymptotic expressions for the average value of $r_k(n)$ – the number of representations of n as a sum of k squares – for any k, provided only we know a formula for the volume of the unit ball in $\mathbb{R}^k$. We leave it to the reader to derive (or look up!) such formulas and thereby compute an asymptotic for the average value of $r_4(n)$.