Math 408

L-functions and Sphere Packing

Steven Miller: sjm1@williams.edu

https://web.williams.edu/Mathematics/sjmiller/public_html/408Fa20/

Lecture 31: November 30, 2020

Gauss Circle Problem

in dimensions 8 & 24 to constructing a radial function f on $\mathbb{R}^d$ ($d=8$ or 24) such that

$$f(\sqrt{2n}) = \hat{f}(\sqrt{2n}) = \hat{f}'(\sqrt{2n}) = 0, \quad n \geq n_0 = \begin{cases} 1, & d=8 \\ 2, & d=24 \end{cases}$$

$$f'(\sqrt{2n}) = 0, \ n > n_0$$

such that $f(0) = \hat{f}(0) = 1$, $f(x) \leq 0$ for $x \geq n_0$,

& $\hat{f} \geq 0$,

where we tacitly identify radial functions with f'ns on rays from the origin, &

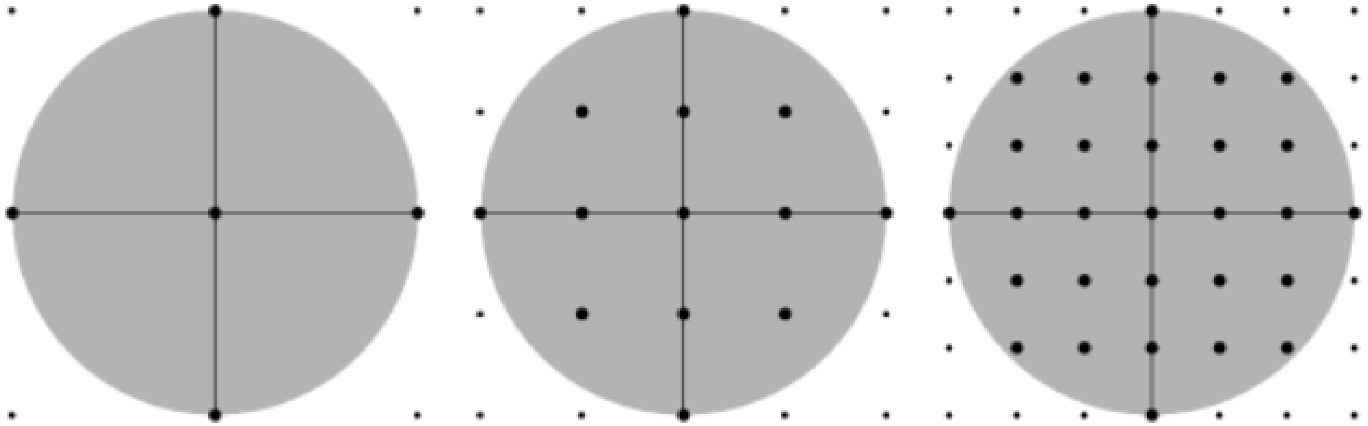
$$\hat{f}(r) = \int_{\mathbb{R}^d} f(x) e^{-2\pi i \langle r, x \rangle} dx$$

is the d-dimensional Fourier transform.

Henry Cohn & I did many numerical experiments & found conjectural constructions of such f'ns. They had numerical features suggestive of a modular form connection, but we could not find it.

https://mathworld.wolfram.com/GausssCircleProblem.html

Gauss's Circle Problem



Count the number of lattice points $N(r)$ inside the boundary of a circle of radius r with center at the origin. The exact solution is given by the sum

$$N(r) = 1 + 4\lfloor r \rfloor + 4\sum_{i=1}^{\lfloor r \rfloor}\left\lfloor\sqrt{r^2 - i^2}\right\rfloor$$

$$= 1 + 4\sum_{i=1}^{r^2}(-1)^{i-1}\left\lfloor\frac{r^2}{2i-1}\right\rfloor$$

$$= 1 + 4\sum_{i=0}^{\infty}\left(\left\lfloor\frac{r^2}{4i+1}\right\rfloor - \left\lfloor\frac{r^2}{4i+3}\right\rfloor\right)$$

Gauss Circle Problem:

What do you think the main term is?

How many lattice points (standard lattice) inside the circle of radius r centered at the origin?

Gauss Circle Problem:

What do you think the main term is?
How many lattice points (standard lattice) inside the circle of radius r centered at the origin?

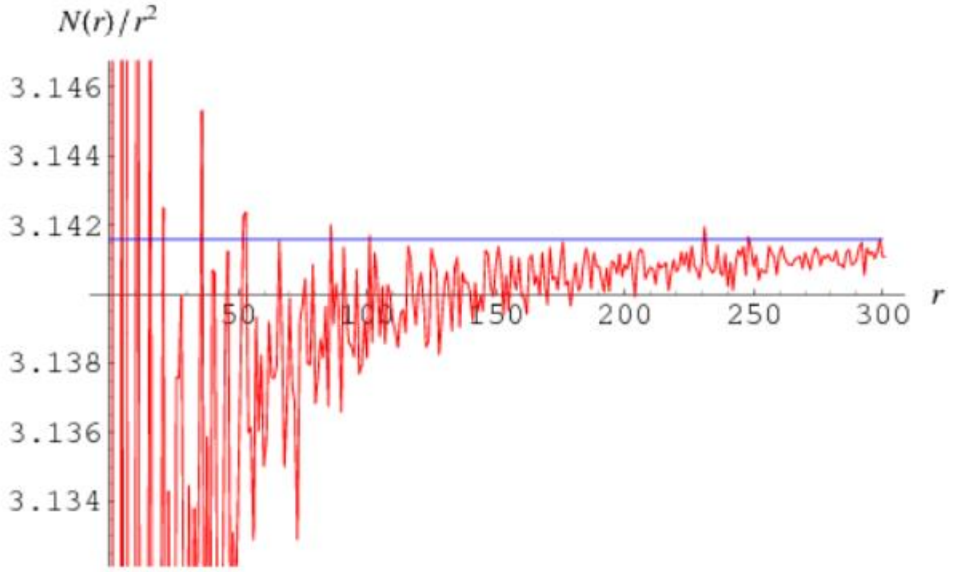
Gauss showed that

$$N(r) = \pi r^2 + E(r), \tag{7}$$

where

$$|E(r)| \leq 2\sqrt{2}\,\pi r \tag{8}$$

(Hardy 1999, p. 67).



The first few values of $N(r)/r^2$ are 5, 13/4, 29/9, 49/16, 81/25, 113/36, 149/49, 197/64, 253/81, 317/100, 377/121, 49/16, ... (OEIS A000328 and A093837). As can be seen in the plot above, the values of r such that $N(r)/r^2 > \pi$ are $r = 2$, 3, 4, 6, 11, 16, 21, 36, 52, 53, 86, 101, ... (OEIS A093832).

Gauss Circle Problem:

What do you think the main term is?

How many lattice points (standard lattice) inside the circle of radius r centered at the origin?

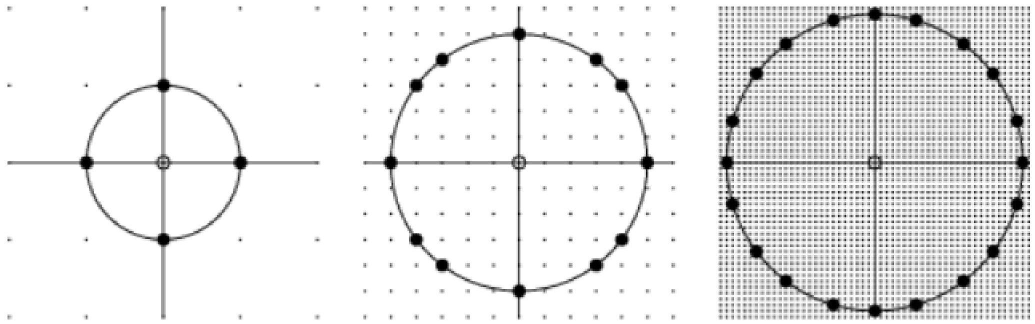
What are the issues with counting?

Gauss Circle Problem:

How many lattice points (standard lattice) inside the circle of radius r centered at the origin?

What are the issues with counting?

One issue are points on the boundary – how many can there be?



The number of lattice points on the Circumference of circles centered at (0, 0) with radii 0, 1, 2, ... are 1, 4, 4, 4, 4, 12, 4, 4, 4, 4, 12, 4, 4, ... (Sloane's A046109). The following table gives the smallest Radius $r \leq 368,200$ for a circle centered at (0, 0) having a given number of Lattice Points $L(r)$. Note that the high water mark radii are always multiples of five.

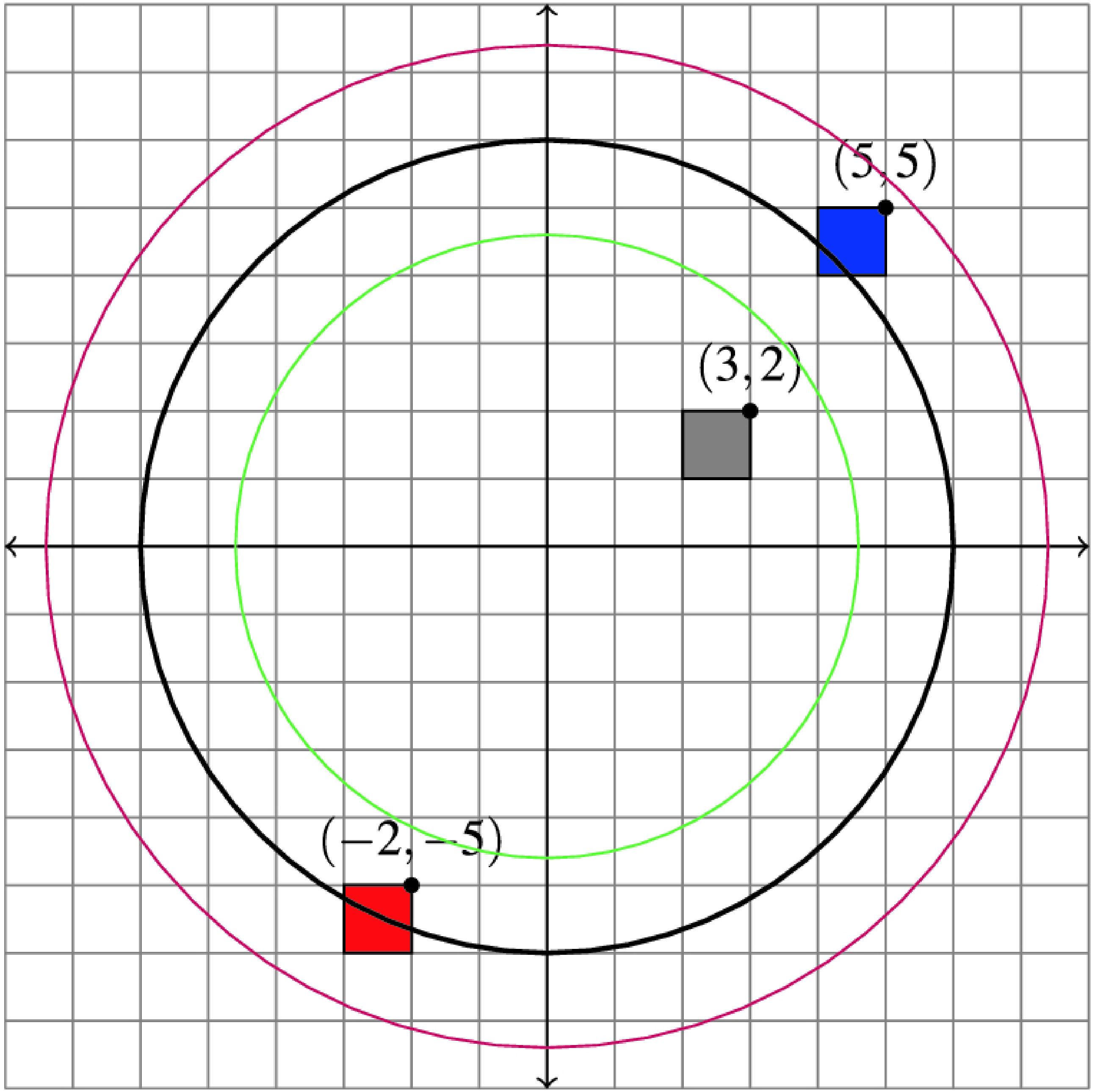
https://archive.lib.msu.edu/crcmath/math/math/c/c314.htm

$L(r)$	r	$L(r)$	r
1	0	108	1,105
4	1	132	40,625
12	5	140	21,125
20	25	156	203,125
28	125	180	5,525
36	65	196	274,625
44	3,125	252	27,625
52	15,625	300	71,825
60	325	324	32,045
68	390,625	420	359,125
76	$\leq 1,953,125$	540	160,225
84	1,625		
92	$\leq 48,828,125$		
100	4,225		

Gauss Circle Problem:

What do you think the main term is?

How many lattice points (standard lattice) inside the circle of radius r centered at the origin?



https://link.springer.com/chapter/10.1007/978-3-030-02604-2_9

Gauss Circle Problem:

How many lattice points (standard lattice) inside the circle of radius r centered at the origin?

Understand the main term: expect πr^2, what is the error term? Write as $N(r) = \pi r^2 + E(r)$, $|E(r)| \leq r^{\theta}$.

Gauss Circle Problem:

How many lattice points (standard lattice) inside the circle of radius r centered at the origin?

Understand the main term: expect πr^2, what is the error term? Write as $N(r) = \pi r^2 + E(r),\ |E(r)| \leq r^{\theta}$.

θ	approx.	citation
1	1.00000	Dirichlet
2/3	0.66667	Voronoi (1903), Sierpiński (1906), van der Corput (1923)
37/56	0.66071	Littlewood and Walfisz (1925)
33/50	0.66000	van der Corput (1922)
27/41	0.65854	van der Corput (1928)
15/23	0.65217	
24/37	0.64865	Chen (1963), Kolesnik (1969)
35/54	0.64815	Kolesnik (1982)
278/429	0.64802	Kolesnik
34/53	0.64151	Vinogradov (1935)
7/11	0.63636	Iwaniec and Mozzochi (1988)
46/73	0.63014	Huxley (1993)
131/208	0.62981	Huxley (2003)

Philosophy of Square-Root Cancelation

For many problems if summing N "random" terms of order 1 expect sum to be 0, with fluctuations of size $\sqrt{N}$.
Homework problem: Write a computer program to do at least 100,000,000 tosses of a fair coin, with +1 for each head and -1 for each tail. Plot where after each of the first 10,000 tosses. Also plot where you are after every 10,000$^{\text{th}}$ toss. Compare your plots to $\pm 2\sqrt{N}$. If you have issues coding look below or happy to chat; took less than 5 minutes in Mathematica.

The Central Limit Theorem is one of the gems of probability, saying the sum of nice independent random variables converges to being normally distributed as the number of summands grows. As a powerful application of Stirling's formula, we'll show it implies the Central Limit Theorem for the special case when the random variables $X_1, \dots, X_{2N}$ are all binomial random variables with parameter $p = 1/2$. It's technically easiest if we normalize these by

$$\text{Prob}(X_i = n) \;=\; \begin{cases} 1/2 & \text{if } n = 1 \\ 1/2 & \text{if } n = -1 \\ 0 & \text{otherwise.} \end{cases} \tag{18.1}$$

Let $X_1, \dots, X_{2N}$ be independent binomial random variables with probability density given by (18.1). Then the mean is zero as $1 \cdot (1/2) + (-1) \cdot (1/2) = 0$, and the variance of each is

$$\sigma^2 \; = \; (1-0)^2 \cdot \frac{1}{2} + (-1-0)^2 \cdot \frac{1}{2} \; = \; 1.$$

Finally, we set

$$S_{2N} \; = \; X_1 + \cdots + X_{2N}.$$

Its mean is zero. This follows from

$$\mathbb{E}[S_{2N}] \; = \; \mathbb{E}[X_1] + \cdots + \mathbb{E}[X_{2N}] \; = \; 0 + \cdots + 0 \; = \; 0.$$

Similarly, we see the variance of S_{2N} is $2N$. We therefore expect S_{2N} to be on the order of 0, with fluctuations on the order of $\sqrt{2N}$.

Let's consider the distribution of S_{2N}. We first note that the probability that $S_{2N} = 2k+1$ is zero. This is because S_{2N} equals the number of heads minus the number of tails, which is always even: if we have k heads and $2N-k$ tails then S_{2N} equals $2N-2k$.

The probability that S_{2N} equals $2k$ is just $\binom{2N}{N+k}\left(\frac{1}{2}\right)^{N+k}\left(\frac{1}{2}\right)^{N-k}$. This is because for S_{2N} to equal $2k$, we need $2k$ more 1's (heads) than -1's (tails), and the number of 1's and -1's add to $2N$. Thus we have $N+k$ heads (1's) and $N-k$ tails (-1's). There are 2^{2N} strings of 1's and -1's, $\binom{2N}{N+k}$ have exactly $N+k$ heads and $N-k$ tails, and the probability of each string is $\left(\frac{1}{2}\right)^{2N}$. We wrote $\left(\frac{1}{2}\right)^{N+k}\left(\frac{1}{2}\right)^{N-k}$ to show how to handle the more general case when there is a probability p of heads and $1-p$ of tails.

We now use Stirling's Formula to approximate $\binom{2N}{N+k}$. We find

$$\begin{aligned}
&\binom{2N}{N+k} \\
\approx\quad & \frac{(2N)^{2N}e^{-2N}\sqrt{2\pi\cdot 2N}}{(N+k)^{N+k}e^{-(N+k)}\sqrt{2\pi(N+k)}(N-k)^{N-k}e^{-(N-k)}\sqrt{2\pi(N-k)}} \\
=\quad & \frac{(2N)^{2N}}{(N+k)^{N+k}(N-k)^{N-k}}\sqrt{\frac{N}{\pi(N+k)(N-k)}} \\
=\quad & \frac{2^{2N}}{\sqrt{\pi N}}\frac{1}{(1+\frac{k}{N})^{N+\frac{1}{2}+k}(1-\frac{k}{N})^{N+\frac{1}{2}-k}}.
\end{aligned}$$

The rest of the argument is just doing some algebra to show that this converges to a normal distribution. There is, unfortunately, a very common trap people frequently fall into when dealing with factors such as these. To help you avoid these in the future, we'll describe this common error first and then finish the proof.

$$\left(1+\frac{k}{N}\right)^{N+\frac{1}{2}+k}\left(1-\frac{k}{N}\right)^{N+\frac{1}{2}-k} \rightarrow e^{2k^2/N}.$$

We show that $\left(1+\frac{k}{N}\right)^{N+\frac{1}{2}+k}\left(1-\frac{k}{N}\right)^{N+\frac{1}{2}-k} \rightarrow e^{k^2/N}$. The importance of this calculation is that it highlights how crucial *rates* of convergence are. While it's true that the main terms of $(1 \pm \frac{k}{N})^N$ are $e^{\pm k}$, the error terms (in the convergence) are quite important, and yield large secondary terms when k is a power of N. What happens here is that the secondary terms from these two factors reinforce each other. Another way of putting it is that one factor tends to infinity while the other tends to zero. Remember that $\infty \cdot 0$ is one of our undefined expressions; it can be anything depending on how rapidly the terms grow and decay; we'll say more about this at the end of the section.

The short of it is that we cannot, sadly, just use $\left(1+\frac{w}{N}\right)^N \approx e^w$. We need to be more careful. The correct approach is to take the logarithms of the two factors, Taylor expand the logarithms, and then exponentiate. This allows us to better keep track of the error terms.

Before doing all of this, we need to know roughly what range of k will be important. As the standard deviation is $\sqrt{2N}$, we expect that the only k's that really matter are those within a few standard deviations from 0; equivalently, k's up to a bit more than $\sqrt{2N}$. We can carefully quantify exactly how large we need to study k by using Chebyshev's Inequality (Theorem 17.3.1). From this we learn that we need only study k where $|k|$ is at most $N^{\frac{1}{2}+\epsilon}$. This is because the standard deviation of S_{2N} is $\sqrt{2N}$. We then have

$$\operatorname{Prob}(|S_{2N} - 0| \geq (2N)^{1/2+\epsilon}) \ \leq \ \frac{1}{(2N)^{2\epsilon}},$$

because $(2N)^{1/2+\epsilon} = (2N)^{\epsilon}\operatorname{StDev}(S_{2N})$. Thus it suffices to analyze the probability that $S_{2N} = 2k$ for $|k| \leq N^{1/2+1/9}$.

We now come to the promised lemma which tells us what the right value is for the product; the proof will show us how we should attack problems like this in general.

Lemma 18.3.1 *For any $\epsilon \leq 1/9$, for $N \to \infty$ with $|k| \leq (2N)^{1/2+\epsilon}$, we have*

$$\left(1+\frac{k}{N}\right)^{N+\frac{1}{2}+k}\left(1-\frac{k}{N}\right)^{N+\frac{1}{2}-k} \longrightarrow e^{k^2/N}e^{O(N^{-1/6})}.$$

Proof: Recall that for $|x| < 1$,

$$\log(1+x) = \sum_{n=1}^{\infty}\frac{(-1)^{n+1}x^n}{n}.$$

As we're assuming $k \leq (2N)^{1/2+\epsilon}$, note that any term below of size k^2/N^2, k^3/N^2 or k^4/N^3 will be negligible. Thus if we define

$$P_{k,N} \quad := \quad \left(1+\frac{k}{N}\right)^{N+\frac{1}{2}+k} \left(1-\frac{k}{N}\right)^{N+\frac{1}{2}-k}$$

then using the big-Oh notation from §B.4 we find

$$\begin{aligned}
\log P_{k,N} \quad &= \quad \left(N+\frac{1}{2}+k\right)\log\left(1+\frac{k}{N}\right)^{N+\frac{1}{2}+k} \\
&\quad + \left(N+\frac{1}{2}-k\right)\log\left(1-\frac{k}{N}\right)^{N+\frac{1}{2}-k} \\
&= \quad \left(N+\frac{1}{2}+k\right)\left(\frac{k}{N}-\frac{k^2}{2N^2}+O\left(\frac{k^3}{N^3}\right)\right) \\
&\quad + \left(N+\frac{1}{2}-k\right)\left(-\frac{k}{N}-\frac{k^2}{2N^2}+O\left(\frac{k^3}{N^3}\right)\right) \\
&= \quad \frac{2k^2}{N}-2\left(N+\frac{1}{2}\right)\frac{k^2}{2N^2}+O\left(\frac{k^3}{N^2}+\frac{k^4}{N^3}\right) \\
&= \quad \frac{k^2}{N}+O\left(\frac{k^2}{N^2}+\frac{k^3}{N^2}+\frac{k^4}{N^3}\right).
\end{aligned}$$

As $k \le (2N)^{1/2+\epsilon}$, for $\epsilon < 1/9$ the big-Oh term is dominated by $N^{-1/6}$, and we finally obtain that

$$P_{k,N} \quad = \quad e^{k^2/N} e^{O(N^{-1/6})},$$

which completes the proof. $\square$

We now finish the proof of S_{2N} converging to a Gaussian. Combining Lemma 18.3.1 with (18.2) yields

$$\binom{2N}{N+k}\frac{1}{2^{2N}} \quad \approx \quad \frac{1}{\sqrt{\pi N}}\, e^{-k^2/N}$$

(the careful analysis in the lemma alerted us to the existence of the factor $e^{-k^2/N}$, which our fast and loose calculations missed). The proof of the Central Limit Theorem in this case is completed by some simple algebra. We're studying $S_{2N} = 2k$, so we should replace k^2 with $(2k)^2/4$. Similarly, since the variance of S_{2N} is $2N$, we should replace N with $(2N)/2$. While these may seem like unimportant algebra tricks, it's very useful to become comfortable at doing this. By doing such small adjustments we make it easier to compare our expression with its conjectured value.

We find

$$\text{Prob}(S_{2N} = 2k) \;=\; \binom{2N}{N+k}\frac{1}{2^{2N}} \quad\approx\quad \frac{2}{\sqrt{2\pi\cdot(2N)}}\,e^{-(2k)^2/2(2N)}.$$

Remember S_{2N} is never odd. The factor of 2 in the numerator of the normalization constant above reflects this fact, namely the contribution from the probability that S_{2N} is even is twice as large as we would expect, because it has to account for the fact that the probability that S_{2N} is odd is zero. Thus it looks like a Gaussian with mean 0 and variance $2N$. For N large such a Gaussian is slowly varying, and integrating from $2k$ to $2k+2$ is basically $2/\sqrt{2\pi(2N)}\;\cdot\;\exp -(2k)^2/2(2N)$. $\square$

As our proof was long, let's spend some time going over the key points. We were fortunate in that we had an explicit formula for the probability, and that formula involved binomial coefficients. We used Chebyshev's inequality to limit which probabilities we had to investigate. We then expanded using Stirling's formula, and did some algebra to make our expression look like a Gaussian.

For a nice challenge: Can you generalize the above arguments to handle the case when $p \neq 1/2$.