Summary

The goal of this report is to shine a light over what a few students investigated during UBC's SRP. More specifically, we'll take a look at the Lattice Point Problem, going over its significance and connection with various other topics in math. However, the main goal of this report is not to understand the problem itself, but to observe how different techniques can be applied to it, and how those techniques are used in different context.

First, we will establish what the problem actually is, so let's get a few definitions out of the way. Let tD be the disk of radius t in the $\mathbb{R}^2$ plane (i.e. D would be the unit disk, etc.). Let

$$N(t) := \#\{tD \cap \mathbb{Z}^2\}$$

So $N(t)$ is the number of lattice points contained in the disk of radius t. Intuitively, $N(t) \approx \pi t^2$ or $N(t) = \pi t^2 + E(t)$. The goal of the problem is to find a bound to $E(t)$. This version of problem (also referred to as the ”Gauss Circle” problem) is the one we will focus on, but there are many different version that consider different shapes and dimensions.

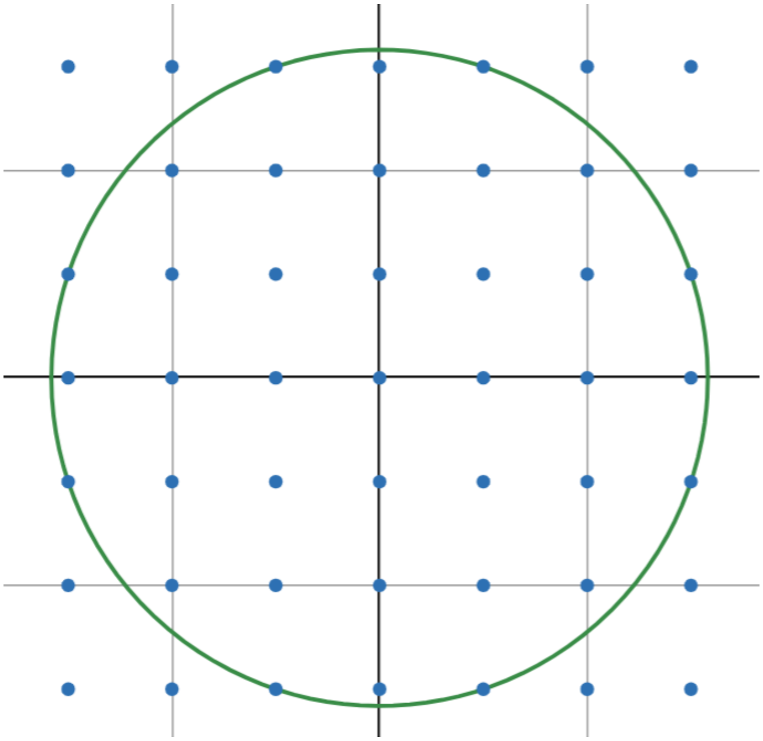

Figure 1: Lattice Points in Circle

The goal of modern research on the topic is to find a bound on $E(t)$. Godfrey Harold Hardy, a British mathematician of the 19-20th century, conjectured that the bound is

$$|E(t)| \leq C_\epsilon t^{\frac{1}{2}+\epsilon}$$

For any $\epsilon > 0$. Currently, the best bound we know of is $E(t) \leq Ct^q$, with

$$\frac{1}{2} < q \leq \theta$$

where $\theta \approx 0.3144$ and $-\theta$ is the unique solution to the equation

$$-\frac{8}{25}x - \frac{1}{200}\left(\sqrt{2(1-14x)} - 5\sqrt{-1-8x}\right)^2 + \frac{51}{200} = -x$$

The lower bound was found by Hardy in 1915, and the upper bound by Xiaochun Li and Xuerui Yang in 2023[1].

The problem, when generalized to shapes other then a circle, finds application in many different applied fields, mostly in cryptography, integer programming, crystallography, quantum mechanics, and combinatorics. Meanwhile, for pure mathematics, it has obvious relevance in number theory, but also toric Hilbert functions and Kostant's partition function in representation theory. The methods modern mathematicians use to study the problem include the circle method (developed by Hardy and Littlewood), fourier analysis, Minkowski's Theorem for convex sets in $\mathbb{R}^n$, and various lattice reduction techniques (such as Lenstra-Lenstra-Lovász algorithm)[2−5].

Our reading was based on Alex Iosevich's "A View from the Top: Analysis, Combinatorics and Number Theory"[6], specifically chapters 11 and 12. The endpoint and goal of those chapter is to prove a theorem established by Wacław Sierpiński in 1903:

$$|E(t)| \leq Ct^{\frac{2}{3}} \tag{1}$$

binding the aforementioned error term. In chapter 11, Iosevich introduces oscillatory integrals of the form

$$I_f(R) = \int_a^b e^{iRf(x)}dx$$

and develops some tools to study them. For example **theorem 11.4:** if f is a once differentiable function such that $|f'(x)| \geq 1$ and f' is non-monotone, then

$$|I_f(R)| \leq \frac{4}{R}$$

Another example is **theorem 11.11:** let $\chi_D(x) = 1$ if $x \in D$ and 0 otherwise, and let

$$\widehat{\chi}_D(\xi) = \int_D e^{-2\pi i x\xi}dx$$

be the fourier transform of χ_D. Then, $|\widehat{\chi}_D(\xi)| \leq C|\xi|^{-\frac{3}{2}}$. Moving onto chapter 12, where Iosevich makes use of these results and other tenniques to establish (1). We now see an outline of the proof. Let

$$\begin{aligned} N_x(t) &= \sum_{n\in\mathbb{Z}^2} \chi_{tD}(x-n) \\ N_R(t) &= t^2 \sum_{m\neq(0,0)} \widehat{\chi}_D(tm)\pi^{-1}\widehat{\chi}_D(m/R) \\ N_R(t) &= \pi t^2 + E_R(t) \end{aligned}$$

through an application of theorem 11.11, we can show that

$$|E_R(t)| \leq Ct^{\frac{1}{2}}R^{\frac{1}{2}} \tag{2}$$

Now, we would love use $N_R(t)$ to get a bound on $N(t)$, which is exactly what we do. We can easily show that $\widehat{f*g}(\xi) = \widehat{f}(\xi)\widehat{g}(\xi)$, that leads us to

$$N_R(t) = R^2 \sum_{n\in\mathbb{Z}^2} \chi_{tD} * \chi_{R^{-1}D}(n) \tag{3}$$

which leads us to the more significant

$$N(t) \leq N_R(t+R^{-1}) \tag{4}$$

Now we finally come to our wanted conclusion, we can write:

$$N_R(t+R^{-1}) = \pi(t+R^{-1}) + E_R(t+R^{-1})$$

using this along with (2) and (3) we get

$$|E(t)| \leq C(tR^{-1} + |E_R(t)|)$$

with this and (2) and taking $R = t^{\frac{1}{3}}$ we finally see that

$$|E(t)| \leq Ct^{\frac{2}{3}}$$

proving (1).

It can be interesting what tools were used in the proof, and why they were used.

(1) The fourier transfrom:

$$\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e^{-i2\pi\xi x}dx$$

is an incredibly flexible tool used in a variety of fields (including: signal processing, data analysis, engineering, quantum mechanics and astronomy)$^{7-10}$. It's effect (among other things) is to move the function f into the frequency domain. This can make it easier to understand properties of f, especially if it is a periodic function (like $N_x(t)$ is, as we will show below).

(2) Convolutions:

$$f * g(t) = \int_{-\infty}^{\infty} f(t-\tau)g(\tau)d\tau$$

Which we used above to manipulate $N_R(t)$ in order to relate it to $N(t)$. Generally, convolution can be use to tweak certain function in order to make them more manageable. Taking a convolution with a smoothing function (such as a Gaussian) can result in a smooth version of the original function. Other known functions can be used to shift and scale the study function.

(3) Integration:

Finally, why use analysis at all to understand what is seemingly a number theoretic problem? Well, we can attempt to answer this with a picture. Going back to integration in $\mathbb{R}^2$, we can view the process of integrating over a set $S \subseteq \mathbb{R}^2$ as measuring the number of disjoint unit squares with integer edge coordinates. Take for exampe:

$$\int_0^1 x dx$$

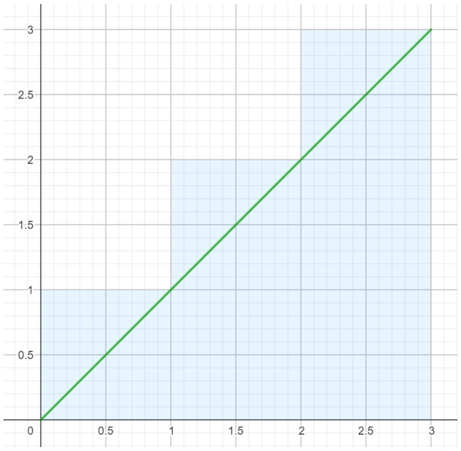

Figure 2: Integral of $f(x) = x$

As we can approximate the area under the curve by an integral, we can approximate the number of lattice points in a similar manner.

Solution to exercises

Exercise 12.2: Let $\chi_t D(x) : \mathbb{Z}^2 \to \{0,1\}$ s.t. $\chi_t D(x) = 1$ if x is in the disk of radius t centered at $(0,0)$ in the $\mathbb{Z}^2$, and 0 otherwise. Define

$$N(t) = \sum_{n \in \mathbb{Z}^2} \chi_t D(n) \tag{5}$$

$$N_x(t) = \sum_{n \in \mathbb{Z}^2} \chi_t D(x-n) \tag{6}$$

For $x \in \mathbb{R}^2$. Our goal is to prove that (2) is a periodic function. More explicitly, $N(t)_x = N(t)_{x+m}$ for any $m \in \mathbb{Z}^2$.

$$\begin{aligned} N(t)_{x+m} &= \sum_{n \in \mathbb{Z}^2} \chi_t D(x+m-n) && (7) \\ &= \sum_{l \in \mathbb{Z}^2} \chi_t D(x-l) \qquad \text{Let } l = n-m \in \mathbb{Z}^2 && (8) \\ &= \sum_{n \in \mathbb{Z}^2} \chi_t D(x-n) = N_x(t) && (9) \end{aligned}$$

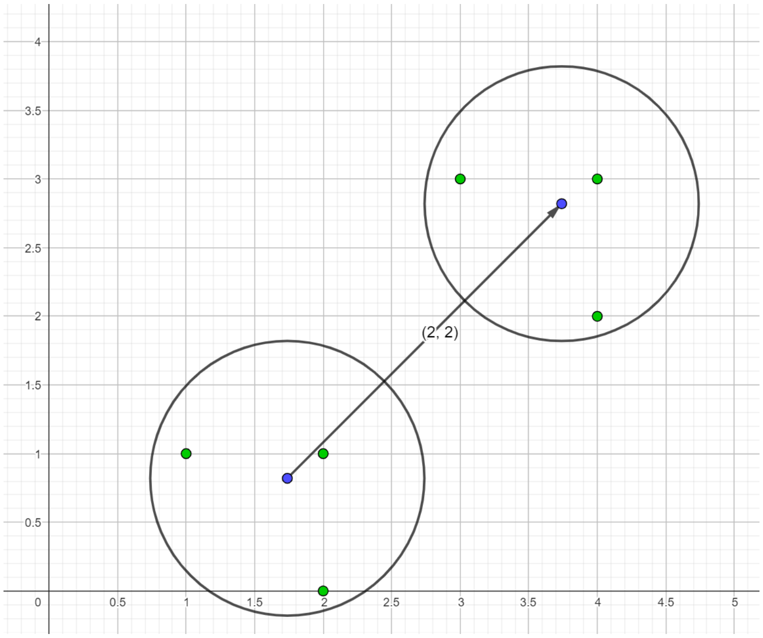

Figure 3: Translation of Disk by Integer Vector

Intuitively, $N(t)$ measures the sum of all lattice points in the disk of radius t centered at the origin, while $N_x(t)$ measures the number of lattice points in the disk or radius t

centered at x. What we just prove shows that if we change the coordinates of our center x (in $\mathbb{R}^2$) by integer values, the disk at the new center contains the same number of lattice points as the one before the move.

Exercise 11.1: Let

$$I_f(R) = \int_a^b e^{iRf(x)}dx$$

where f is a suitably differentiable function and R is a large parameter. Johannes van der Corput has shown that if f is once differentiable, f' is either strictly increasing or strictly decreasing, and $|f'(x)| \geq 1$, then

$$|I_f(R)| \leq \frac{4}{R}$$

We will now show that the monotonicity condition is necessary for the result to follow.

$$\begin{aligned} I_f(R) &= \int_a^b \frac{1}{iRf'(x)} \frac{d}{dx} \left(e^{iRf(x)} \right) dx \\ &= \frac{e^{iRf(x)}}{iRf'(x)} |_a^b - \int_a^b e^{iRf(x)} \frac{d}{dx} \left(\frac{1}{iRf'(x)} \right) dx = I + II \end{aligned}$$

Since $|f'(x)| \geq 1$ we can see that

$$|I| = \left| \frac{e^{iRf(b)}}{iRf'(b)} - \frac{e^{iRf(a)}}{iRf'(a)} \right| \leq \frac{2}{R}$$

Now, we argue that since $e^{iRf(x)} = \cos(Rf(x)) + i\sin(Rf(x))$, we can say if

$$\int_a^b \cos(Rf(x))dx > \frac{2}{R}$$

then the conclusion of the theorem is false. We must have $|f'(x)| > 1$ and f' non-monotonic. It is simpler to describe the function based on its behaviour. Let $g(x)$ be a function such that $g(x) \geq 1$ and $g(x)$ is increasing when closer to 0 and decreasing when closer to ±10. Then let $f(x) = \int g(x)dx$ (or $f(x)$ is the anti-derivative of $g(x)$), this function satisfies all the properties we need, and it grows smaller near ±10 and greater around 0. The result, when observing the $\cos(Rf(x))$ function look something like this:

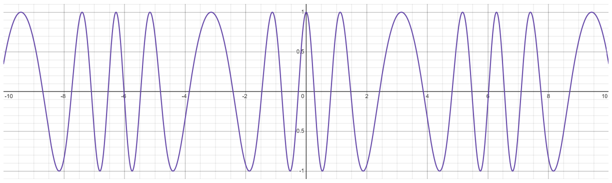

Figure 4: Graph of $\cos(Rf(x))$

We can tweak $g(x)$ to make the curve wider near ±10, and therefore letting the integral grow above $\frac{2}{R}$. When we take $R \to \infty$, the only effect is to increase the frequency of the cosine function, which ultimately does not affect its area. Thus, the conclusion of the theorem cannot be true.

References and related readings

(1) Li, Xiaochun, and Xuerui Yang (2023), “An Improvement on Gauss’s Circle Problem and Dirichlet’s Divisor Problem.” arXiv.Org,
arxiv.org/abs/2308.14859.

(2) Del Pia, A., Weismantel, R. (2012) On convergence in mixed integer programming. Math. Program. 135, 397–412. https://doi.org/10.1007/s10107-011-0476-9

(3) Chris Peikert (2016), ”A Decade of Lattice Cryptography”, Foundations and Trends® in Theoretical Computer Science: Vol. 10: No. 4, pp 283-424.
http://dx.doi.org/10.1561/0400000074

(4) David Iglesias, Jesús Yepes Nicolás, Artem Zvavitch, Brunn-Minkowski type inequalities for the lattice point enumerator, Advances in Mathematics, Volume 370, 107193, ISSN 0001-8708, https://doi.org/10.1016/j.aim.2020.107193.

(5) Mujeerulla, M., Preethi, Khan, M.S. et al. Demerits of Elliptic Curve Cryptosystem with Bitcoin Curves Using Lenstra–Lenstra–Lovasz (LLL) Lattice Basis Reduction. Arab J Sci Eng 49, 4109–4124 (2024). https://doi.org/10.1007/s13369-023-08116-w

(6) Alex Iosevich (2007) ”A View from the Top: Analysis, Combinatorics and Number Theory”

(7) Ervin Sejdić, Igor Djurović, LJubiša Stanković (2011), ”Fractional Fourier transform as a signal processing tool: An overview of recent developments”, Signal Processing, Volume 91, Issue 6, Pages 1351-1369
https://doi.org/10.1016/j.sigpro.2010.10.008.

(8) A. C. Gilbert, P. Indyk, M. Iwen and L. Schmidt (2014), ”Recent Developments in the Sparse Fourier Transform: A compressed Fourier transform for big data,” in IEEE Signal Processing Magazine, vol. 31, no. 5, pp. 91-100, doi: 10.1109/MSP.2014.2329131

(9) Horwitz, L.P (2020). Fourier transform, quantum mechanics and quantum field theory on the manifold of general relativity. Eur. Phys. J. Plus 135, 479.
https://doi.org/10.1140/epjp/s13360-020-00446-0

(10) Bernd Klein et al.,(2006) ”A new generation of spectrometers for radio astronomy: fast Fourier transform spectrometer,” Proc. SPIE 6275, Millimeter and Submillimeter Detectors and Instrumentation for Astronomy III, 627511; https://doi.org/10.1117/12.670831