Randomness and Patterns in Gauss Sums

Scholars: Ka Fung Tjin, Elsie Wang, Yifan Zhang
Faculty Mentor: A.J. Hildebrand
University of Illinois at Urbana-Champaign

Background: Carl Friedrich Gauss

- Carl Friedrich Gauss (1777 - 1855) was one of the greatest mathematicians for his contributions to many fields, including number theory.
- At the age of 7, Gauss discovered a formula for summing n consecutive integers.
- Gauss invented Gauss sums and found a formula for them in 1805.

"Hardly a week may have gone by in the last four years without one or more unsuccessful attempts to unravel this knot. [...] But all the brooding, the searching, was to no avail, and I had sadly to lay down my pen again. A few days ago, I finally succeeded—not by my efforts, but by the grace of God, I should say." —Carl Friedrich Gauss on Gauss' Formula

Introduction: Quadratic Residues and Gauss Sums

Quadratic Residues

An integer n not divisible by p is called a **quadratic residue** modulo p if the congruence $n \equiv x^2 \bmod p$ has a solution, and a **quadratic non-residue** modulo p otherwise. The Legendre symbol modulo p, $\left(\frac{n}{p}\right)$, encodes quadratic residues and non-residues as follows:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue mod } p, \\ -1 & \text{if } n \text{ is a quadratic non-residue mod } p \end{cases}$$

Gauss Sums: Two Versions

$$G(p) = \sum_{n=1}^{p} e^{2\pi i n^2/p} = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{2\pi i n/p}$$

exponential quadratic residue

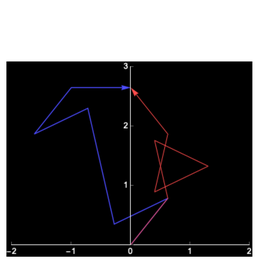
Gauss' Formula: The exact values of the Gauss sums $G(p)$ are given by the following formula:

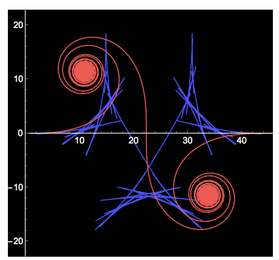
$$G(p) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \bmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Random Walks Based on Gauss Sums

Create random walks starting at the origin, with the n-th step given by $e^{2\pi i n^2/p}$ or $\left(\frac{n}{p}\right) e^{2\pi i n/p}$.

The graphs on the right are the random walks for $p = 7$ and $p = 2081$. As a result of the **Gauss' formula**, the two walks take different paths to the same end points. For $p = 7$, the end point is $(0, \sqrt{7})$. For $p = 2081$, the end point is $(\sqrt{2081}, 0)$.

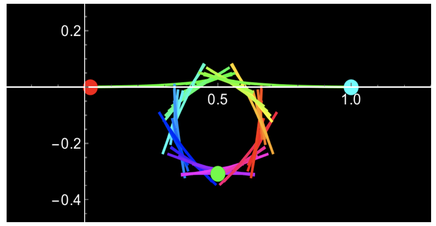




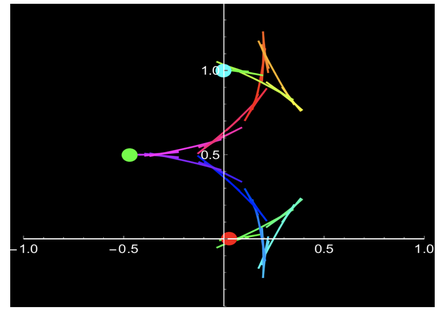
References

- D. H. Lehmer, "Incomplete Gauss sums", *Mathematika* 23 (1976), 125-135.
- Moore, R. R., and A. J. van der Poorten. "On the thermodynamics of curves and other curlicues."*Miniconference on Geometry and Physics*, 1989.

Patterns of Quadratic Residue Gauss Walks



- There are 8 shapes for the walk, which are determined by congruences mod 24.
- 2 of the 8 shapes are shown here. For the graph above, $2521 \equiv 1(24)$. For the graph on the right, $1619 \equiv 11(24)$.



The red, green, and blue points represent the starting point, the halfway point, and the ending point, respectively.

Cubic Gauss Sums

Cubic Gauss Sum: Definition

$$G_3(p) = \sum_{n=1}^{p} e^{2\pi i n^3/p}$$

Formulas: (p's are primes under this section)

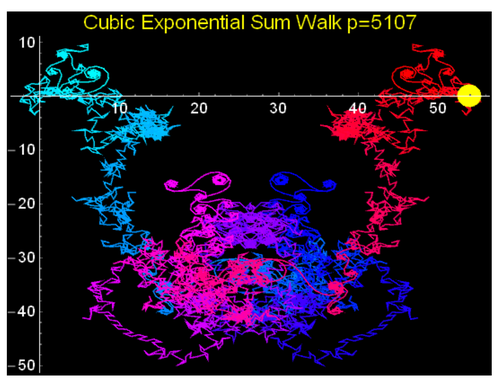
- For primes $p \equiv 5 \bmod 6$:

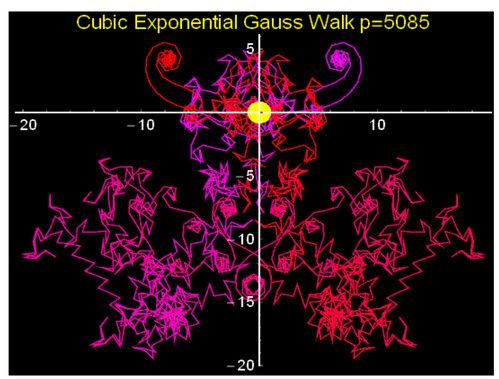
$$G_3(p^n) = \begin{cases} 0 & \text{if } n = 3m+1, \\ p^{2m+1} & \text{if } n = 3m+2, \\ p^{2m} & \text{if } n = 3m. \end{cases}$$

- $G_3(\prod_i p_i^{\alpha_i}) = \prod_i G_3(p_i^{\alpha_i})$ if $p_i \equiv 5 \bmod 6$.
- For primes $p \equiv 1 \bmod 6$:

$$G_3(p^n) = \begin{cases} ??? & \text{if } n = 3m+1, \\ p^{2m+1} & \text{if } n = 3m+2, \\ p^{2m} & \text{if } n = 3m. \end{cases}$$

- $G_3(\prod_i p_i^{\alpha_i}) = 0$ if there is a p_i such that $p_i \equiv 5 \bmod 6$ and $\alpha_i = 1$.
- $G_3(p^\alpha \cdot N) = G_3(p^3)^\beta \cdot G_3(p^\gamma \cdot N)$ if $\alpha = 3 \cdot \beta + \gamma$. Repeating this procedure until all powers of primes ≤ 3. Then we can further simplify the value by noting that $G_3(p_1^3 \cdot N) = p_1 \cdot G_3(p_1^2 \cdot N)$.





The graphs above are random walks based on cubic Gauss sums. These graphs show some randomness, but also exhibit curlicue patterns and symmetries.The endpoints of the random walks are indicated by yellow dots.