A Theorem of Gauss

Jonggoo Kang

Ian Whitehead

Senior Paper

Abstract

Carl Friedrich Gauss was an extremely well known mathematician, who has contributed largely in science, especially in number theory in mathematics. Since Gauss is a big part of number theory, comprehending the Gauss' Theorem is very crucial in advancing more deeply into the study of number theory. The Gauss' Theorem with sub-theorems will be introduced, followed by step-by-step proves of actually achieving the ultimate theorem. Multiple numerical applications and examples will be provided for better digestion of the theoretical and actual uses.

Introduction

Carl Friedrich Gauss is usually called the "Prince of Mathematicians." He had made noticeable influences in mathematical and scientific fields. Although he made marvelous contributions in almost all fields of mathematics, it is not wrong to say that his favorite area was number theory. Gauss even once claimed that "Mathematics is the queen of the sciences, and the number theory is the queen of mathematics." Gauss revolutionized the behavior of functions on the complex numbers, combinations of real and imaginary numbers, developing the study of number theory to the next level. Although number theory is purely theoretical with not very abundant practical applications, it is a beautiful subject as much as the principle of the universe. The origin of number theory was due to Gauss' Theorem, which will be introduced in this paper.

A Theorem of Gauss

The most interesting and mysterious part of number theory was Fermat's Last Theorem. It states for the equation $x^n + y^n = z^n$, there are no whole number solutions where $x * y * z \neq 0$, and $n > 2$. Fermat has left the statement "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain." on his paper *Fermat's Engima*. When Fermat passed away, multiple well-known mathematicians have tried to prove this theorem for 350 years, but they had no luck. It was not until the presence of Andrew Wiles, using the Gauss' Theorem as a stepping-stone in 1995. Therefore, Gauss' Theorem is the most basic beginning area in studying number theory.

Theorem 1.1.1

Let M_P be the number of Projective solutions to the equation $x^3 + y^3 + z^3 = 0$ with x, y, z in the finite field $\mathbb{F}_P$

(a) If $P \not\equiv 1 \bmod 3$, then $M_P = P + 1$

(b) If $P \equiv 1 \bmod 3$, then there are integers A and B such that $4P = A^2 + 27B^2$, and $A \equiv 1 \bmod 3$. Then, $M_P = P + 1 + A$.

Recall: Projective solutions means that

(1) We do not count the trivial solution $(0, 0, 0)$

(2) We identify a solution (x, y, z) with all of its non-zero multiples (ax, ay, az)

Proof of (a) Suppose $P \equiv 1 \bmod 3$. Then, the map $a \to a^3$is a bijection itself. This is because the group $\mathbb{F}_P$ is cyclic of order $P - 1$. Thus, the number of projective solutions of $x^3 + y^3 + z^3 = 0$ is the same as the number of projective solutions of $x + y + z = 0$, which is $P + 1$. Hence, $M_P = P + 1$.

Proof of (b) Suppose $P \equiv 1 \bmod 3$. Then, the map $a \to a^3$ is neither one to one nor onto. Thus, the image of this homomorphism is a subgroup, which we denote, R, so $R = \{x^3 : x \in \mathbb{F}_P\}$. The subgroup R has index 3 inside $\mathbb{F}_P$. The kernel of the homomorphism $x \to x^3$consists of three elements $1, \mu, \mu^2$satisfying , $\mu^3 = 1$.

Example 1.1.2

For example of (a), If $p = 5$, then $\mathbb{F}_5$ we have, $1^3 \equiv 1,\ \ 2^3 \equiv 3,\ \ 3^2 \equiv 2,\ \ 4^3 \equiv 4$. So, in this case, $P \equiv 2 \not\equiv 1\ (mod\ 5)$, every element of $\mathbb{F}_P$ has a unique cube root. Thus, the number of solutions of $x^3 + y^3 + z^3 = 0$ is equal to the number of solutions to the linear equation $x + y + z = 0$.

Hence, $M_P = P + 1 = 5 + 1 = 6$

Example 1.1.3

If $P = 7$, then $x^3 + y^3 + z^3 = 0$ mod 7. Then, the cubes mod 7 will be $0^3 \equiv 0,\ 1^3 \equiv 1,\ 2^3 \equiv 1,\ 3^3 \equiv 6,\ 4^4 \equiv 1,\ 5^3 \equiv 6,\ 6^3 \equiv 6$. In this case, $R = \{0, 1, 6\}$. To check, $x^3 + y^3 + z^3 = 0$ mod 7 if $R = \{0, 1, 6\}$, then

$$x^3 + \ y^3 + \ z^3 \equiv 0\ mod\ 7$$

$$\begin{pmatrix}0\\1\\6\end{pmatrix} + \begin{pmatrix}0\\1\\6\end{pmatrix} + \begin{pmatrix}0\\1\\6\end{pmatrix} \equiv 0\ mod\ 7$$

Now, we can have 6 cases

	x^3	y^3	z^3	Total Number
Case 1	0	0	0	1
Case 2	0	1	6	9
Case 3	0	6	1	9
Case 4	1	0	6	9

Case 5	1	6	0	9
Case 6	6	0	1	9
Case 7	6	1	0	9

Now,

For Case 1, since it is a trivial solution, there is an only solution (0 0 0).

For Case 2, we have solutions

(0 1 6), (0 1 5), (0 1 6),

(0 2 3), (0 2 5), (0 2 6),

(0 4 3), (0 4 5), (0 4 6).

For Case 3,

(1 0 3), (1 0 5), (1 0 6),

(2 0 3), (2 0 5), (2 0 6)

(4 0 3), (4 0 5), (4 0 6)

For Case 4,

(1 0 3), (1 0 5), (1 0 6),

(2 0 3), (2 0 5), (2 0 6),

(4 0 3), (4 0 5), (4 0 6).

For Case 5,

(1 3 0), (1 5 0), (1 6 0),

(2 3 0), (2 5 0), (2 6 0),

(4 3 0), (4 5 0), (4 6 0).

For Case 6,

(3 0 1), (3 0 2), (3 0 4),

(5 0 1), (5 0 2), (5 0 4),

(6 0 1), (6 0 2), (6 0 4).

For Case 7,

(3 1 0), (3 2 0), (3 4 0),

(5 1 0), (5 2 0), (5 4 0),

(6 1 0), (6 2 0), (6 4 0).

Since we have 6 cases, which satisfy to $x^3 + y^3 + z^3 \equiv 0 \; mod \; 7$, each case has following 9 solutions. Thus, we have $6 \times 9 = 54$ points. We also have one trivial solution in Case 1. Hence, we have $54 + 1 = 55$ points total.

The theorem states that M_P is the number of projective solutions to the $x^3 + y^3 + z^3 = 0$. We count the points projectively; we do not count the trivial solution, but we identify a solution (x, y, z) with all of its non-zero multiples (ax, ay, az). Thus, for first points of Case 3, we have (1, 0, 3). Now, we multiply the point by integer 2, 3, 4, 5, 6. Then, we have (1, 0, 3), (2, 0, 6), (3, 0, 2), (4, 0, 5), (5, 0, 1), (6, 0, 1). These 6 lists count as one solution. Since we have total 54 points, $\frac{54}{6} = 9$. Therefore, $M_P = 9$.

Since $M_P = P + 1 + A$, we can get M_P.

$$4P = A^2 + 27B^2$$

$$4 \times 7 = A^2 + 27B^2$$

$$28 = A^2 + 27B^2$$

$$28 = A^2 + 27(1)$$

$$A^2 = 28 - 27$$

$$A = \pm 1$$

Thus, A = 1.

Hence $M_P = P + 1 + A = 7 + 1 + 1 = 9$.

Theorem 1.1.4

Suppose N is the number of solutions mod P. Then, $M_P = \frac{N-1}{P-1}$

Example 1.1.5

If $P = 7, then\ N = 55$ as we have seen in the Example 1.1.3.

Therefore, $M_P = \frac{55-1}{7-1} = \frac{54}{6} = 9$.

Example 1.1.6

If $p = 3$, then $0^3 \equiv 0,\ 1^3 \equiv 1,\ 2^3 \equiv 2$. Thus, $R = \{0, 1, 2\}$.

To check, $x^3 + y^3 + z^3 = 0$ mod 3 if $R = \{0, 1, 2\}$, then

$$x^3 + y^3 + z^3 \equiv 0\ mod\ 3$$

$$\begin{pmatrix}0\\1\\2\end{pmatrix} + \begin{pmatrix}0\\1\\2\end{pmatrix} + \begin{pmatrix}0\\1\\2\end{pmatrix} \equiv 0\ mod\ 3$$

Case 1: (0 0 0)

Case 2: (0 1 2)

Case 3: (0 2 1)

Case 4: (1 0 2)

Case 5: (1 2 0)

Case 6: (1 1 1)

Case 7: (2 0 1)

Case 8: (2 1 0)

Case 9: (2 2 2)

Therefore, $N = 9$

Hence, $M_P = \frac{N-1}{P-1} = \frac{9-1}{3-1} = \frac{8}{2} = 4$.

Example 1.1.7

If $P = 5$, then $0^3 \equiv 0,\ 1^3 \equiv 1,\ 2^3 \equiv 3,\ 3^2 \equiv 2,\ 4^3 \equiv 4.$

Thus, $R = \{0, 1, 2, 3, 4\}$. To check, $x^3 + y^3 + z^3 = 0 \bmod 3$ if $R = \{0, 1, 2\}$, then

$$x^3 + y^3 + z^3 \equiv 0 \; mod \; 3$$

$$\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \equiv 0 \; mod \; 3$$

Case 1: (0 0 0)

Case 2: (0 1 4)

Case 3: (0 2 3)

Case 4: (0 3 2)

Case 5: (0 4 1)

Case 6: (1 0 4)

Case 7: (1 4 0)

Case 8: (1 2 2)

Case 9: (1 3 1)

Case 10: (1 1 3)

Case 11: (2 0 3)

Case 12: (2 3 0)

Case 13: (2 1 2)

Case 14: (2 2 1)

Case 15: (2 4 4)

Case 16: (3 0 2)

Case 17: (3 2 0)

Case 18: (3 3 4)

Case 19: (3 4 3)

Case 20: (3 1 1)

Case 21: (4 0 1)

Case 22: (4 1 0)

Case 23: (4 2 4)

Case 24: (4 4 2)

Case 25: (4 3 3)

Therefore, $N = 25$.

Hence, $M_P = \frac{N-1}{P-1} = \frac{25-1}{5-1} = \frac{24}{4} = 6$.

Definition 1.1.9 R has two cosets at S and T.

Let b = primitive root, then $R = \{b^{3n}\} \subset \mathbb{Z}/P$, then we have two cosets $S = \{b^{3n+1}\} \subset \mathbb{Z}/P,\ T = \{b^{3n+2}\} \subset \mathbb{Z}/P$

Then, $|R| = |S| = |T| = \frac{P-1}{3}$

Example 1.1.8 Back to **Example 1.1.3**, if $P = 7$, 3 is a primitive root.

Thus, $3^0 \equiv 1,\ 3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5$

Then, $R = \{1, 6\}, S = \{3, 4\}, T = \{2, 5\}$

Now, $|R| = |S| = |T| = \frac{P-1}{3} = \frac{7-1}{3} = \frac{6}{3} = 2$

Definition 1.1.10 Let $|XYZ|$ denote the number of solving $x_1 + x_2 + x_3 = 0$, where $x \in X, y \in Y, z \in Z$. If $x^3 + y^3 + z^3 = 0$, we have two cases.

<u>Case1</u>: we have non-zero solution, thus $x, y, z \neq 0$

Thus, we have 27|RRR| non zero solutions of $x^3 + y^3 + z^3 = 0$

<u>Case2</u>: we have projective solution, in which that none of x, y, or z is 0

Thus, there is 9|RRR| projective solutions of $x^3 + y^3 + z^3 = 0$.

In which that non of x, y, or z is 0

Claim now that there are 9 projective solutions, where on of the coordinates is zero. Therefore, we can suppose $x = 0$, then let y is anything, but z is the cube root of unity times by y. We combine these calculations. We have the number M_p of projective solutions is$\frac{9[RRR]}{m} + 9 = 9\left(\frac{[RRR]}{m} + 1\right), where\ m = \frac{P-1}{3}$

It is clear that $[\mathrm{RR}\mathbb{F}_P] = \mathrm{m}^2$ since each R has m choices, and $\mathbb{F}_P$has just 1 choice. Also, $\mathbb{F}_P = \{0\} \cup R \cup S \cup T$. Therefore, we can conclude that $m^2 = [RR\{0\}] + [RRR] + [RRS] + [RRT]$. Now, we fix elements $s \in S, and\ t \in T$.

Since $[RRS] + [sR, sR, sS] = [SST]\ and\ [RRT] = [tR, tR, tT] = [TTS]$, we can write them as $[RR\{0\}] + [RRR] + [SST] + [TTS] = m^2$ and $[\{0\}TS] + [RTS] + [STS] + [TTS] = m^2$

Now, by using the fats that $[\{0\}TS] = 0$ and $[RR\{0\}] = m$, then we finally get

$$M_P = 9\frac{[RTS]}{m}$$

In order to get [RTS] more brilliantly, we now use the concept of the pth Roots of Unity; so we use some complex numbers to prove gadgets for keeping track of information about the sets R, S, and T.

Conclusion

In order to finish the entire proving of the Gauss' Theorem, few more concepts are required. Although this is not a complete proof, I wish the readers were able to follow the numerical and theoretical explanation and examples with no hardships.