

THE SOLUTIONS OF $X^3 + Y^3 + Z^3 = 0$ AND KUMMER'S CONJECTURE

MARK BRANSON

ABSTRACT. Gauss discovered an elegant solution to finding the number of solutions to the Fermat curve in a finite field. This discovery is detailed, with focus on those finite fields \mathbb{F}_p where $p \equiv 1 \pmod{3}$ (since the proof is surprisingly straightforward for $p \not\equiv 1 \pmod{3}$). Kummer's conjecture relates to the cubic Gauss sums, which are used in the proof. Although the conjecture has been proven false, it is an excellent example of the need for mathematical rigor - even with modern computers, the results obtained from Kummer's computations remain compelling. Computational results of these sums are given, along with an algorithm for computing them.

1. INTRODUCTION

Finding the number of solutions to an elliptic curve in a finite field is an important and difficult problem. There exists a general result, the Hasse-Weil theorem, which is true for all non-singular irreducible curves of genus g over the finite field \mathbb{F}_p . Of course, the relatively simple curve $x^3 + y^3 = 1$, also known as the Fermat curve, satisfies these conditions, and thus is subject to the estimate provided by the Hasse-Weil theorem. However, there exists a much earlier theorem, from Gauss's *Disquisitiones Arithmeticae*, which provides a concrete answer to the number of solutions for this particular curve in projective space.

A more difficult problem related to Gauss's proof is Kummer's Conjecture. Kummer conjectured that certain sums α_1 , α_2 , and α_3 from Gauss's proof are related in a certain way, and supported his conjecture by computing these values for all primes congruent to $1 \pmod{3}$ up to 500 (a computation consisting of summing a certain 166 of the 499th roots of unity, for the largest such prime). While Kummer's calculations were impressive (and correct - they were computationally verified by von Neumann and Goldstine on an early supercomputer), his conjecture proved incorrect. This proof, however, came 133 years later, and was much more involved than Gauss's proof of the number of solutions.

2. GAUSS'S THEOREM

Theorem 2.1. *Consider the Fermat curve, $x^3 + y^3 = 1$, in homogeneous form: $X^3 + Y^3 + Z^3 = 0$. Take this curve on the finite field \mathbb{F}_p where p is prime. Then there exist two cases for the number of solutions in this field, denoted by M_p :*

Case 1: *If $p \not\equiv 1 \pmod{3}$, then $M_p = p + 1$.*

Case 2: *If $p \equiv 1 \pmod{3}$, then $\exists A, B \in \mathbb{Z}$ such that $4p = A^2 + 27B^2$, where A and B are unique up to change of sign, and either $A \equiv 1 \pmod{3}$ or $-A \equiv 1 \pmod{3}$. If $A \not\equiv 1 \pmod{3}$, change the sign of A . Then $M_p = p + 1 + A$.*

Although a straightforward proof of Gauss's theorem is possible, such a proof would elide over many intriguing results covered in its course. To avoid this, we will prove the theorem as a series of lemmas, aiming to provide a unifying proof of the theorem through these lemmas¹. First, we will prove Case 1.

Lemma 2.1. *If $p \not\equiv 1 \pmod{3}$, then $M_p = p + 1$*

Proof. Consider the multiplicative group of \mathbb{F}_p , \mathbb{F}_p^* . \mathbb{F}_p^* is composed of all the elements of \mathbb{F}_p except $\{0\}$. This group \mathbb{F}_p^* is a cyclic group of order $p - 1$. Since $p \not\equiv 1 \pmod{3}$, $3 \nmid p - 1$. Therefore, if $x^3 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{3}$. This implies that the kernel of the map $x \rightarrow x^3$ is trivial, and thus that the map is injective on \mathbb{F}_p . Since $x \rightarrow x^3$ is injective, the problem of finding solutions to $X^3 + Y^3 + Z^3 = 0$ is reduced to finding solutions to $X + Y + Z = 0$. This is a line in the projective plane, and has exactly $p + 1$ solutions in the field \mathbb{F}_p . Thus, $M_p = p + 1$. ■

Although the first case admits a rather simple proof, the second case is considerably more difficult to prove. We will tackle it in a similar fashion - by looking at the map $x \rightarrow x^3$. Clearly, this map is neither injective nor surjective (consider a similar argument with the kernel of the map). However, it still provides an interesting way to divide the group into several subgroups.

Lemma 2.2. *\mathbb{F}_p can be written as a disjoint union $\mathbb{F}_p = \{0\} \cup R \cup S \cup T$ where R is the subgroup of cubic residues:*

$$R = \{x^3 : x \in \mathbb{F}_p^*\}$$

and S and T are cosets of R in \mathbb{F}_p^ .*

Proof. Clearly, R is a subgroup of \mathbb{F}_p^* (since the multiple of two cubic residues will be a cubic residue). Since the map $x \rightarrow x^3$ is not surjective, this group has order less than $p - 1$. However, by Lagrange's Group Theorem [Hun], the order of R times the index of R is equal to the order of \mathbb{F}_p^* . Thus, since the order of R must divide m (since $x^{3m} = 1$), the index of R must be a multiple of 3. However, since the kernel of the map consists of exactly 3 elements, we know that the index of R is 3. We call R the set of cubic residues, and we call its two cosets S and T . Since R has order m , S and T also have order m and all three sets are disjoint. Therefore, \mathbb{F}_p can be written as the disjoint union $\mathbb{F}_p = \{0\} \cup R \cup S \cup T$. ■

Note that R, S, T each have m elements. Also, note that $-1 \pmod{p} \in R$. Since R is a subgroup, and S and T are cosets of R , we see that $-R = R$, $-S = S$, and $-T = T$.

Of course, partitioning our group into smaller groups is only a step in this proof. Now we wish to find the number of projective solutions by looking at these subgroups. In order to do this, we define a counting operation on sets.

Definition 1. *Let $[XYZ]$ or $[X, Y, Z]$ denote the number of triples $(x, y, z) \in X \times Y \times Z$ such that $x + y + z = 0$.*

The symbol $[XYZ]$ has many interesting properties, some of which will be of use to us later in the proof. These properties are enumerated below:

- (1) If Z and W are disjoint, then $[XY(Z \cup W)] = [XYZ] + [XYW]$.

¹The proof of Gauss's Theorem is taken from [ST], with much of the same notation and explanatory notes added by the author

- (2) If $a \neq 0$, $[XYZ] = [aX, aY, aZ]$.
 (3) $[XYZ]$ is independent of the ordering of the sets. Thus, $[XYZ] = [YXZ] = [XZY] = [YZX] = [ZXY] = [ZYX]$.

Now we wish to use this terminology to say something concrete about the number of solutions of $X^3 + Y^3 + Z^3 = 0$. We do this by splitting into another two cases.

Lemma 2.3. *Consider the following two cases:*

Case 1: : If X , Y , and Z are all three not equal to zero, then there are $\frac{27[RRR]}{p-1}$ solutions to $X^3 + Y^3 + Z^3 = 0$.

Case 2: : There are 9 solutions to $X^3 + Y^3 + Z^3 = 0$ if one of the X , Y , or Z is equal to 0.

Proof. (Case 1) Clearly, the number of ways of writing 0 as a sum of 3 nonzero cubes is exactly $[RRR]$, since any cube is in R . However, each cube corresponds to 3 different values in \mathbb{F}_p . Thus, the number of solutions to $X^3 + Y^3 + Z^3 = 0$ in Euclidean space is $27[RRR]$. However, we are working in projective space, so we need to look at the number of solutions in homogeneous coordinates. Thus, we wish to identify (x, y, z) and (ax, ay, az) , where a is in \mathbb{F}_p . There are $p-1$ such a , since we do not consider the trivial solution $(0, 0, 0)$. Thus, the number of solutions to $X^3 + Y^3 + Z^3 = 0$ is $\frac{27[RRR]}{p-1}$. ■

Proof. (Case 2) Let one of the values, say Z , be 0. Then $X \neq 0$ and $Y \neq 0$, since either of these would imply that $(X, Y, Z) = (0, 0, 0)$, and we do not allow the trivial solution in homogeneous coordinates. Therefore, $X^3 = -Y^3$. If we pick any value in \mathbb{F}_p^* for X (of which there are $p-1$), then we get 3 values for Y . Thus, if $Z = 0$, there are $3(p-1)$ solutions to $X^3 + Y^3 + Z^3 = 0$ in Euclidean space. Similarly, there are $3(p-1)$ solutions if $X = 0$ or $Y = 0$. Thus, there are $3*3(p-1) = 9(p-1)$ solutions in Euclidean space. As in Case 1, in order to get the number of solutions in projective space, we divide by $p-1$. Thus, there are $\frac{9(p-1)}{p-1} = 9$ solutions to the equation $X^3 + Y^3 + Z^3 = 0$ in homogeneous coordinates on \mathbb{F}_p . ■

The lemma above gives us this corollary:

Corollary 2.1. $M_p = \frac{27[RRR]}{p-1} + 9 = 9\left(\frac{3[RRR]}{p-1} - 1\right)$.

Corollary 2.1 gives us a concrete link between our sets R , S , and T and the value M_p . However, while this result is of some value, computing M_p from this information is still nontrivial, since it necessitates computing the subgroup of cubic residues and finding $[RRR]$. Thus, we want to continue working with this equation and try to eliminate the $[RRR]$. We'll use the properties of the $[XYZ]$ operation that we listed earlier. In order to simplify our notation, we'll use the variable m to denote $\frac{p-1}{3}$.

Since $\mathbb{F}_p = \{0\} \cup R \cup S \cup T$, we can use property 3 to see that

$$(1) \quad [RR\mathbb{F}_p] = [RR\{0\}] + [RRR] + [RRS] + [RRT]$$

Note that $[RR\mathbb{F}_p] = m^2$, since $\forall X, Y \in R, \exists Z \in \mathbb{F}_p$ such that $X + Y + Z = 0$. Now, let $s \in S$ and $t \in T$. By property 2, $[RRS] = [sR, sR, sS] = [SST]$ and $[RRT] = [tR, tR, tT] = [TTS]$. Therefore, Equation 1 becomes

$$(2) \quad m^2 = [RR\{0\}] + [RRR] + [SST] + [TTS]$$

Now, using the fact that $[\mathbb{F}_p TS] = m^2$ and the fact that $\mathbb{F}_p = \{0\} \cup R \cup S \cup T$, we can obtain the similar equation

$$(3) \quad m^2 = [\{0\}TS] + [RTS] + [STS] + [TTS]$$

Of course, $[\{0\}TS] = 0$, since this is the number of solutions to $t = -s, t \in T, s \in S, S = -S$, and $T \cap S = \emptyset$. Also, $[RR\{0\}] = m$, since each $r \in R$ has a unique inverse in R . Therefore, if we substitute in these values and subtract equation 3 from equation 2, we get

$$(4) \quad m + [RRR] = [RTS]$$

If we combine this result with the formula we got in Corollary 2.1, we see that

$$(5) \quad M_p = \frac{9[RTS]}{m}$$

At this point, having obtained a succinct formula for M_p , we take a bit of a departure from the direct line of reasoning that we've been following. We'll take advantage of this little break to define the cubic Gauss sums, and then go on to explain how they help with finding an explicit formula for M_p .

Definition 2. *The three cubic Gauss sums, α_1 , α_2 , and α_3 are defined as follows:*

$$\alpha_1 = \sum_{r \in R} \zeta^r$$

$$\alpha_2 = \sum_{s \in S} \zeta^s$$

$$\alpha_3 = \sum_{t \in T} \zeta^t$$

where ζ is the first p^{th} root of unity, $e^{\frac{2\pi i}{p}}$.

These three numbers (which are, in fact, purely real) form the roots of a polynomial with coefficients in \mathbb{Z} . This polynomial is the connection between these cubic Gauss sums and the proof of the main theorem.

We start by multiplying together α_2 and α_3

$$(6) \quad \alpha_2 \alpha_3 = \sum_{s \in S} \zeta^s \sum_{t \in T} \zeta^t = \sum_{s \in S, t \in T} \zeta^{s+t} = \sum_{x \in \mathbb{F}_p} N(x) \zeta^x$$

where $N(x)$ is the number of $(s, t) \in S \times T$ such that $s + t = x$. Observe that

$$(7) \quad N(x) = [ST\{-x\}] = [rS, rT, -rx] = [ST-rx] = N(rx)$$

Thus $N(x) = N(y)$ provided that x and y are both in R, S , or T . Therefore,

$$(8) \quad mN(x) = [S, T, Rx] = \begin{cases} [\text{STR}] & \text{if } x \in R \\ [\text{STS}] & \text{if } x \in S \\ [\text{STT}] & \text{if } x \in T \end{cases}$$

Define three integers a, b , and c such that $a = N(x)$ if $x \in R$, $b = N(x)$ if $x \in S$, and $c = N(x)$ if $x \in T$. Note then, that, if we take combine (5) and (8), we obtain

$$(9) \quad ma = [STR] = [RTS] \Rightarrow M_p = \left(\frac{9}{m}\right) ma = 9a.$$

Now the proof of our main theorem has been reduced to finding the value of this a . In order to find that value, we look at several other equations, drawn directly from (6) and (7), by substituting in a, b , and c appropriately.

$$(10) \quad \alpha_2\alpha_3 = a\alpha_1 + b\alpha_2 + c\alpha_3$$

If we take different combinations of α 's in the same way we did in (6), we find that

$$(11) \quad \alpha_3\alpha_1 = a\alpha_2 + b\alpha_3 + c\alpha_1$$

$$(12) \quad \alpha_1\alpha_2 = a\alpha_3 + b\alpha_1 + c\alpha_2$$

We will use these three equations, along with a simple identity based on the definitions of the α_i . The simple identity is this: Since our three α_i contain all powers of ζ except $\zeta^0 = 1$, $\alpha_1 + \alpha_2 + \alpha_3 + 1 = \sum_{i \in \mathbb{F}_p} \zeta^i$. However, $(\zeta - 1) \sum_{i \in \mathbb{F}_p} \zeta^i = \zeta^p - 1 = 1 - 1 = 0$, so we see that

$$(13) \quad \alpha_1 + \alpha_2 + \alpha_3 = -1$$

Now we're ready to find a . First, we add together (10), (11), and (12), to get

$$(14) \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = (a + b + c)(\alpha_1 + \alpha_2 + \alpha_3) = -(a + b + c)$$

by taking advantage of our simple identity in (13). However, if we recall the definitions of a, b , and c , we remember that, using (8), we get

$$(15) \quad m(a + b + c) = [STR] + [STS] + [STT]$$

Of course, (3) tells us that this is equal to m^2 . Therefore,

$$(16) \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -m$$

We use (16) and (13) to compute the sum of the squares of the cubic Gauss sums.

$$(17a) \quad \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$$

$$(17b) \quad = (-1)^2 - 2(-m)$$

$$(17c) \quad = 1 + 2m$$

Now we wish to find the multiple of the three cubic Gauss sums. We find this by multiplying (10), (11), and (12) by the Gauss sum that not contained in their LHS's.

$$(18a) \quad \alpha_1(\alpha_2\alpha_3) = \alpha_1(a\alpha_1 + b\alpha_2 + c\alpha_3)$$

$$(18b) \quad \alpha_2(\alpha_3\alpha_1) = \alpha_2(a\alpha_2 + b\alpha_3 + c\alpha_1)$$

$$(18c) \quad \alpha_3(\alpha_1\alpha_2) = \alpha_3(a\alpha_3 + b\alpha_1 + c\alpha_2)$$

If we sum these equations, then reduce using (17) and (16), we find that

$$(19a) \quad 3\alpha_1\alpha_2\alpha_3 = a(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + (b+c)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$$

$$(19b) \quad = a(1 + 2m) + (b+c)(-m)$$

$$(19c) \quad = a + (2a - b - c)m$$

$$(19d) \quad \Rightarrow \alpha_1\alpha_2\alpha_3 = \frac{a + (2a - b - c)m}{3}$$

For our convenience, we'll assign another dummy variable, k , equal to $(2a - b - c)$ here. Note that k also equals $3a - m$ by (15). Therefore, using (9), we see that $M_p = 3(k + m) = 3k + p - 1$, so finding this k will also complete the proof.

We said above that we were looking for a polynomial with the cubic Gauss sums as roots. We are now prepared to state that polynomial in a reasonable form, and do so, using the equalities we've worked out (namely (13), (16), and (19) to simplify the polynomial.

$$(20a) \quad F(t) = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)$$

$$(20b) \quad = t^3 - (\alpha_1 + \alpha_2 + \alpha_3)t^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)t - \alpha_1\alpha_2\alpha_3$$

$$(20c) \quad = t^3 - (-1)t^2 + (-m)t - \left(\frac{a + km}{3}\right)$$

$$(20d) \quad = t^3 + t^2 - mt - \left(\frac{a + km}{3}\right)$$

Now we wish to construct another polynomial, this one with roots $\beta_i = 1 + 3\alpha_i$. Using our identities for α_i (once again, (13), (16), and (19)) we find that

$$(21a) \quad \beta_1 + \beta_2 + \beta_3 = 0$$

$$(21b) \quad \beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3 = -3p$$

$$(21c) \quad \beta_1\beta_2\beta_3 = (3k - 2)p$$

So we find that the polynomial with roots β_i is

$$\begin{aligned}
(22a) \quad G(t) &= (t - \beta_1)(t - \beta_2)(t - \beta_3) \\
(22b) \quad &= t^3 - (\beta_1 + \beta_2 + \beta_3)t^2 + (\beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3)t - \beta_1\beta_2\beta_3 \\
(22c) \quad &= t^3 - (0)t^2 + (-3p)t - (3k - 2)p \\
(22d) \quad &= t^3 - (3p)t - (3k - 2)p
\end{aligned}$$

If we let $A = 3k - 2$, we see that $M_p = 3k + p - 1 = A + 2 + p - 1 = p + 1 + A$ which is exactly the formula that we expected to get for Gauss's Theorem. However, we still need to establish that this A must be the same as the one referred to in Gauss's Theorem. To do this, we first take the discriminant of both F and G

$$\begin{aligned}
(23a) \quad D_F &= (b - c)^2 p^2 \\
(23b) \quad D_G &= 4 * (27p^3) - 27A^2 p^2
\end{aligned}$$

Since $\beta_i - \beta_j = 3(\alpha_i - \alpha_j)$, though, we know that $D_G = (27)^2 D_F$. Therefore,

$$\begin{aligned}
(24a) \quad D_G &= (27)^2 (b - c)^2 p^2 = 4 * (27p^3) - 27A^2 p^2 \\
(24b) \quad 27(b - c)^2 &= 4p - A^2 \\
(24c) \quad 4p &= 27(b - c)^2 + A^2 \\
(24d) \quad 4p &= 27B^2 + A^2
\end{aligned}$$

Letting $B = b - c$, we see that we can write $4p$ in the way that we wanted to. Thus, we have proven the existence of the A and B that we wanted. All that remains to complete the proof is to show that this A is uniquely determined by (24d) and the condition that $A \equiv 1 \pmod{3}$. We prove by contradiction.

Proof of Uniqueness. Assume there exists another pair (A_1, B_1) that satisfy these conditions. Then

$$4p(B_1^2 - B^2) = (A^2 + 27B^2)B_1^2 - (A_1^2 + 27B_1^2)B^2 = (AB_1 + A_1B)(AB_1 - A_1B)$$

Since $p|4p(B_1^2 - B^2)$, it must divide one of the two factors on the RHS. Assume $p|(AB_1 + A_1B)$. Now we multiply together our two different formulae for $4p$. We get

$$16p^2 = A^2 A_1^2 + 27B^2 A_1^2 + 27B_1^2 A^2 + (27)^2 B_1^2 B^2$$

Thus, we see that

$$16p^2 - (AA_1 - 27BB_1)^2 = 27(AB_1 + A_1B)^2$$

Since $p | (AB_1 + A_1B)$, p^2 must divide $(AA_1 - 27BB_1)^2$. Therefore, we can divide both sides by p^2 .

$$16 - \left(\frac{AA_1 - 27BB_1}{p} \right)^2 = 27 \left(\frac{AB_1 + A_1B}{p} \right)^2$$

Clearly, the RHS is less than 16, and the LHS is 27 times the square of an integer. Therefore, that integer must be 0, so $AB_1 + A_1B = 0$. This means that we can choose λ such that

$$\lambda = \frac{B_1}{B} = -\frac{A_1}{A}$$

Thus we can write $A_1 = \lambda A$ and $B_1 = \lambda B$. If we substitute this back into (24d) we see that

$$A^2 + 27B^2 = 4p = \lambda^2(A^2 + 27B^2) \Rightarrow \lambda = \pm 1$$

Since A and A_1 are both congruent to 1 mod 3, λ must be 1, so $A_1 = A$. Therefore A is unique. ■

This completes the proof of Gauss's Theorem. An automated algorithm for applying Gauss's Theorem is given in Section 4.

3. KUMMER'S CONJECTURE

Gauss's theorem, although interesting, is only a small part of this paper. Our primary topic is actually Kummer's Conjecture. Kummer made this conjecture regarding the cubic Gauss sums in [Kum] in 1846. The conjecture is as follows:

Consider the set \mathfrak{P} , the set of all primes congruent to 1 modulo 3. Consider the three subsets of \mathfrak{P} , \mathfrak{P}_1 , \mathfrak{P}_2 , and \mathfrak{P}_3 where

$$\mathfrak{P}_1 = \{p \in \mathfrak{P} : \alpha_1 < \alpha_2 \text{ and } \alpha_1 < \alpha_3\}$$

$$\mathfrak{P}_2 = \{p \in \mathfrak{P} : \alpha_1 > \alpha_2 \text{ xor } \alpha_1 > \alpha_3\}$$

$$\mathfrak{P}_3 = \{p \in \mathfrak{P} : \alpha_1 > \alpha_2 \text{ and } \alpha_1 > \alpha_3\}$$

where the α_i are the cubic Gauss sums.

Conjecture (Kummer's Conjecture). *The number of elements in the sets \mathfrak{P}_1 , \mathfrak{P}_2 , and \mathfrak{P}_3 have ratios 1:2:3 respectively. Namely, there are twice as many elements in \mathfrak{P}_2 as in \mathfrak{P}_1 , and three times as many in \mathfrak{P}_3 as in \mathfrak{P}_1 .*

Note. *The careful reader will note that, as the cubic Gauss sums are sums of complex numbers, such inequalities should be meaningless. However, because of the property that $-R = R$, $-S = S$, and $-T = T$, our three α_i are actually real numbers - for every complex number in the sum ζ^x , its complex conjugate ζ^{-x} is also in the sum.*

Kummer made this conjecture after having considered the values of the cubic Gauss sums for all such primes up to 500 - a noteworthy accomplishment at his time, considering that finding each value would require the solution of a cubic equation or the addition of a large number of cosines. For the primes congruent to 1 mod 3 less than 500, Kummer found that

$$\mathfrak{P}_1 = \{97, 139, 151, 199, 211, 331, 433\}$$

$$\mathfrak{P}_2 = \{13, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 487\}$$

$$\mathfrak{P}_3 = \{7, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349, 409, 421, 439, 457, 463, 499\}$$

The ratios of size between these sets, 7 : 14 : 24, suggested to Kummer that the sets \mathfrak{P}_i would have ratios 1 : 2 : 3 if all such primes were considered, since the ratios were so close for a small number of primes. Because of the complexity of calculating α_1 , α_2 , and α_3 , Kummer's conjecture remained a quite reasonable idea until very recent times. In 1952, Von Neumann and Goldstine tested the supercomputer

MANIAC (Mathematical Analyzer, Numerical Integrator, And Computer [Col]) by finding and checking the values of α_1 , α_2 , and α_3 for all such primes less than 2000. They found that Kummer's table was correct for those primes up to 500. The numbers of primes in each class less than 2000 are (29 : 46 : 73), a ratio of approximately (1 : 1.6 : 2.51). These ratios are significantly different from Kummer's conjectured ratios, significant enough to cast serious doubt on the validity of the conjecture.

2000 such computations was a significant feat for MANIAC, but fifty years later, such feats are easily carried out on any home computer. The following table of the number of primes in each set was computed using the algorithms detailed in section 4 on an ordinary home computer.

n	\mathfrak{P}_1	\mathfrak{P}_2	\mathfrak{P}_3	Ratio
500	7	14	24	(1:2:3.42)
1000	15	22	43	(1:1.46:2.86)
2000	29	46	73	(1:1.58:2.51)
3000	41	68	98	(1:1.65:2.39)
5000	66	113	151	(1:1.71:2.28)
7000	106	144	194	(1:1.35:1.83)
10000	138	201	272	(1:1.45:1.97)
12000	174	227	310	(1:1.30:1.78)

TABLE 1. Cardinality of \mathfrak{P}_i for all primes less than n and corresponding ratios.

While the results from MANIAC may have caused some doubt for Kummer, the numbers given above would most certainly have concerned him. As larger primes are considered, the difference between the first set and the other two seems to be getting proportionally smaller. The actual ratio for all such primes, proven in [HBP], is in fact (1:1:1). However, this proof is far beyond the scope of this paper, so the result (and the falsity of Kummer's conjecture) will remain stated without proof.

4. ALGORITHMS FOR COMPUTING THESE VALUES

The primary focus of this project (and thus this paper) is to discuss the algorithms used for computing number M_p from Gauss's theorem, and the ratios between the sets \mathfrak{P}_i in Kummer's conjecture. All of the algorithms listed below were implemented in LISP, using the CLISP interpreter on a 730 MHz processor machine with 256 MB of RAM.

The algorithm used for finding M_p was relatively simple, as the only difficult part was finding A if the prime happened to be congruent to 1 mod 3.

Algorithm 4.1. *Let p be a natural number.*

Step 1: : *If p is not a prime, print an error message and return 0.*

Step 2: : *If $p \not\equiv 1 \pmod{3}$, return $(p + 1)$.*

Step 3: : *Compute the value of A .*

Step 4: : *Return $(p + 1 + A)$.*

The only non-trivial portion of this algorithm is the computation of A . The easiest method for computing A is to conduct an exhaustive search of all possible B and find the one which produces an integral A . Since $B = \sqrt{\frac{4p-A^2}{27}} < \sqrt{\frac{4p-1}{27}}$, which is less than 1000 for all primes less than 6.75 million, this is not difficult. The computation of A thus has $O[\sqrt{p}]$, which means that the overall algorithm has complexity $O[\sqrt{p}]$.

Algorithm 4.2. *Let p be a natural number.*

Step 1: : For all B such that $1 \leq B \leq \lfloor \sqrt{\frac{4p-1}{27}} \rfloor$, let $A = \sqrt{4p - 27B^2}$ if $\sqrt{4p - 27B^2}$ is in \mathbb{Z} .

Step 2: : If $A \not\equiv 1 \pmod{3}$, return $-A$. Else return A .

These two algorithms are sufficient to compute M_p for any prime p . The computation of the Kummer sums, though, is slightly more complicated. The first step taken was to split the problem into many smaller problems, like finding the set R , computing each of the α_i , finding which set a particular p belongs to, etc. Once the problem had been broken into these distinct subproblems, creating an algorithm for each proved simple. The overall algorithm ended up looking like this:

Algorithm 4.3. *Let N be a natural number and create 3 lists P_i , each one to contain the numbers from a particular \mathfrak{P}_i . Let p range through all the positive primes congruent to $1 \pmod{3}$ less than N .*

Step 1.: Find the set of cubic residues R of p .

Step 2.: Compute the cosets S and T from R .

Step 3.: Find the cubic Gauss sums α_i by summing the appropriate p^{th} roots of unity.

Step 4.: Check that the α_i are roots of the polynomial in (20). If not, generate an error message that the algorithm is incorrect.

Step 5.: Compare the α_i to find the set that p belongs to, and add p to the list containing numbers of that type.

Once p has ranged through all these numbers, return the size of each list P_i .

The first step has complexity $O[p]$, since it runs through each value in $\{1, \dots, p-1\}$ and finds the cube of that value, adding it to R if necessary. Similarly, the second step has $O[p]$, since it consists of multiplying each element in R by an element not in R and the square of that same element. Step 4 sums $(p-1)$ elements, so it also has order $O[p]$. The last two steps run in constant time. Therefore, the complexity of finding which set a particular p belongs to is $O[p]$.

However, this complexity is actually dominated by the task of finding whether the algorithm can even be applied or not - namely, by the primality test. The best known primality test, an extremely new result published in [AKS], runs in $O[\ln^{12} p]$. The simpler primality test used for this problem runs in $O[\sqrt{p}]$. Since each number (actually, each odd number congruent to $1 \pmod{3}$, but this does not alter the complexity) less than N must be checked for primality, the overall complexity of the algorithm is $O[N^{\frac{3}{2}}]$.

The actual LISP code used in the project is included in the first appendix.

APPENDIX A. LISP CODE

```

;;This function computes the value of M_p from Gauss's Theorem.
(defun computeMp (p)
  (cond ((not (or (oddp p) (eql p 2)))
    (princ p)
    (princ " is not a prime.")
    (- p p)
  )
  (t (cond ((not (eql 1 (rem p 3)))(+ p 1))
    (t (+ p 1 (computeA p)))
  )
  )
  )

;;Computes the value of A needed for Gauss's theorem
(defun computeA (p)
  (let ((b (+ (floor (sqrt (/ (- (* 4 p) 1) 27))) 2))
    (a 0))
    (dotimes (b (1- b) a)(cond (
    (eql (round
      (sqrt (- (* 4 p) (* 27 (expt b 2))))))
      (sqrt (- (* 4 p) (* 27 (expt b 2))))))
    (setq a (sqrt (- (* 4 p) (* 27 (expt b 2))))))
  )
    (cond ((not (eql 1 (rem a 3))) (setq a (- a)))
    (t a))
  )
  )

;;This function finds the value of a particular \alpha_i when
;;passed l, the appropriate coset R, S or T,
and the prime p
(defun findAn (l p)
  (let ((a 0))
    (dolist (item l a)
      (setf a (+ a (cos (/ (* 2 pi item) p))))
    )
  )
  )

;;Returns the set of cubic residues for a given p
(defun findR (p)
  (let ((R ()))
    (n (- p 1))
  )
  )

```

```

(tau 0))
      (dotimes (n (- n 1) R)
        (setq tau (mod (expt (+ n 1) 3) p))
        (cond ((not (member tau R))
              (setq R (append R (list tau))))))
      )
    )
  )

;;returns one of the cosets of R for p
(defun findS (p)
  (let ((R (findR p))
        (S ()))
    (sigma 2)
    (n (+ (/ (- p 1) 3) 1))
    (setq sigma (do ((sigma 2 (1+ sigma))
                    ((not (member sigma R)) sigma)))
              (dotimes (n (- n 1) S)
                (setq S (append S (list (mod (* sigma (nth n R)) p))))))
    )
  )
)

;;returns the other coset of R for p
(defun findT (p)
  (let ((R (findR p))
        (S ()))
    (sigma 2)
    (n (+ (/ (- p 1) 3) 1))
    (setq sigma (do ((sigma 2 (1+ sigma))
                    ((not (member sigma R)) sigma)))
              (dotimes (n (- n 1) S)
                (setq S (append S (list
(mod (* (expt sigma 2)(nth n R)) p))))))
    )
  )
)

;;This function returns one of the two roots of the
;;polynomial which should have roots \alpha_1, \alpha_2,
;;and \alpha_3
(defun findsecondRoot (p)
  (let ((a1 (findan (findR p) p))
        (a2 0))

```

```

      (/ (- (- -1 a1)
        (sqrt (+
          (expt (+ 1 a1) 2)
          (* 4 (-
            (/ (- p 1) 3)
            (* a1 (+ 1 a1))
          )
        )
      )
    )
  )
)

```

```

;;This function returns the other of the two roots of the
;;polynomial.

```

```

(defun findthirdRoot (p)
  (let ((a1 (findan (findR p) p))
        (a2 0))
    (/ (+ (- -1 a1)
      (sqrt (+
        (expt (+ 1 a1) 2)
        (* 4 (-
          (/ (- p 1) 3)
          (* a1 (+ 1 a1))
        )
      )
    )
  )
)
)
)

```

```

;;returns the number of the set  $\mathfrak{P}_i$  that p belongs to.

```

```

(defun alrank (p)
  (let ((rank -1)
        (tol (expt 10 -8)))
    (R (findR p))
    (S (findS p))
    (V (findT p)))
)

```



```

)
)

;;Returns a list of the numbers in  $\frac{P}{D}$  between n1 and n2
(defun numbersoftype (n1 n2 D)
  (let ((i (- (+ n2 1) n1))
        (L ()))
    (dotimes (i (1- i) L)(cond((and (eq 0 (rem (- (+ i n1) 1) 3))
                                     (oddprimep (+ i n1))
                                     (eq (alrank (+ i n1)) D))
      (setq L (append L (list (+ i n1))))))
    )
  )
)

;;Returns the number of elements in the three sets  $\frac{P_1}{D}$ ,
;; $\frac{P_2}{D}$ , and  $\frac{P_3}{D}$  between n1 and n2.
(defun kummervalues (n1 n2)
  (list (length (numbersoftype n1 n2 1))
        (length (numbersoftype n1 n2 2))
        (length (numbersoftype n1 n2 3)))
)

;;Returns a list of the three sets  $\frac{P_1}{D}$ ,  $\frac{P_2}{D}$ ,
;;and  $\frac{P_3}{D}$  between n1 and n2.
(defun kummerprimes (n1 n2)
  (list (numbersoftype n1 n2 1)
        (numbersoftype n1 n2 2)
        (numbersoftype n1 n2 3))
)

```

REFERENCES

- [AKS] Agrawal, M.; Kayal, N.; Saxena, N. "Primes Is in P." <http://www.cse.iitk.ac.in/primality.pdf>. [12/09/02].
- [Col] Von Neumann, John. *The Columbia Encyclopedia*, 6th ed. New York: Columbia University Press, 2002. www.bartleby.com/65/. [12/09/02].
- [HBP] Heath-Brown D.; Patterson, S. "The distribution of Kummer sums at prime arguments," *J. Reine Angew. Math.* 310 (1979), 111-130
- [Hun] Hungerford, T., *Abstract Algebra: An Introduction*, Saunders College Publishing, Fort Worth, TX: 1997
- [Kum] Kummer, E.E., "De Residuis cubicis disquisitiones nonnullae analyticae," *J. Reine Angew. Math.* 32 (1846), 341-359
- [ST] Silverman, J.; Tate, J., *Rational Points on Elliptic Curves*, Springer-Verlag, New York: 1992 pp. 110-119