COUNTING SOLUTIONS TO DIOPHANTINE EQUATIONS USING JACOBI SUMS

GEOFFREY BARING

Abstract. We develop over the course of this paper the notion of Jacobi sums in the context of their application to counting solutions to equations over finite fields. We introduce some definitions and notation first, then outline the basic properties of finite fields. The number of solutions to a given equation in the field $\mathbb{F}_p$ can be calculated by brute force using a computer, and it is clear that patterns emerge. Once the concept of Gauss and Jacobi sums is introduced, however, the problem takes on a new light, and becomes easier to understand. Finally, we apply this knowledge to the original problem and demonstrate the patterns that emerge for a few specific examples.

Contents

1. Introduction and Definitions

This paper aims to introduce the problem of counting solutions to polynomial equations over a finite field and demonstrate the application of Jacobi sums to this problem. For example, we will look at the equation $x^2 + y^2 = -1$, and try to determine if there is a pattern in the number of solutions to this equation as a function of p. To do so, we will first need to build the notion of multiplicative characters and introduce some of their properties, before discussing Gauss sums briefly. We assume the reader is familiar with the concepts of rings, groups, and fields.

Before moving forward, we will introduce some preliminary definitions and notation which we will use throughout the paper.

We will denote the greatest common divisor of two integers a and b by (a, b). This is defined to be the greatest integer which divides both a and b. We define

the equivalence relation $a \sim b$ if there is an integer n such that $a - b = np$. If this is the case, we will say that $a \equiv b \bmod p$, or that a is equivalent to b modulo p. When p is prime, $\mathbb{Z}/p\mathbb{Z}$, the set of equivalence classes of integers modulo p forms a finite field, which we will denote $\mathbb{F}_p$.

The set $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ is a cyclic group with respect to multiplication.

For the rest of this paper, we will let μ_n represent the set of n-th roots of unity in $\mathbb{C}$, for $n \in \mathbb{N}$. To be precise, for any $n \in \mathbb{N}$, we define $\omega_n = e^{\frac{2\pi i}{n}}$, and then let $\mu_n = \{1, \omega_n, \omega_n^2, \cdots, \omega_n^{n-1}\}$. Thus, for any element $k = \omega_n^\lambda \in \mu_n, k^n = \omega_n^{\lambda n} = e^{\frac{2\pi i n\lambda}{n}} = e^{2\pi i\lambda} = 1$. We will also define $\mu_n^0 = \mu_n \cup \{0\}$. Here 0 refers to the complex number $0 + 0i$, not to be confused with the zero element of a finite field. This definition will become useful later on, when we wish to define multiplicative characters, simply as a means of simplifying the notation used.

2. Equations over Finite Fields

For now, the equations we will look at will have variables in $\mathbb{F}_p$.

For example, given the equation $x^2 = a$ in $\mathbb{F}_p$, the solutions, or roots to the polynomial $x^2 - a$, are any x such that $x \cdot x \equiv a \bmod p$. Given the equation $x^2 + y^2 = a$ over the same finite field, the solutions are pairs of points (x, y) belonging to the set $\mathbb{F}_p \times \mathbb{F}_p$ such that the analagous equality holds.

In this paper, we will focus first on the equations (2.1) through (2.4) listed below in order to gain a better understanding of them and of their properties, before moving on to more general cases.

$$x^2 + y^2 = 0 \tag{2.1}$$

$$x^2 + y^2 = -1 \tag{2.2}$$

$$x^2 + 2xy + y^2 = -1 \tag{2.3}$$

$$y^2 = x^3 + 1. \tag{2.4}$$

Note that the first equation differs from the others since it is homogeonous, whereas the others are not. (2.2) is a homogenous equation plus a constant, and of course (2.4) differs from the others as it is of one higher degree.

3. Counting Solutions

Because the fields we are looking at are finite, the number of solutions to any of these equations must be finite. Later, we will develop a formula for each of the above equations in order to illustrate the approach to this problem. This will require developing Gauss and Jacobi sums first, however. For the specific examples above, we can first get a sense of what kind of pattern there might be by directly counting out the number of solutions for these equations for the first few fields.

For most values of p, this will become tedious, so we will use a computer program to do the calculation for us. For each of the given equations above, we have used the following C++ code to count the number of solutions in $\mathbb{F}_p$:

```
#include <iostream>
#include <string>
#include <math.h>
#include "primes.h"
```

```
using namespace std;

int main()
{
   int mod, count;

   for(int prime = 0; prime < 26; prime++)
   {
      mod = Primes[prime];
      count = 0;

      for(int x = 0; x < mod; x++)
      {
         for(int y = 0; y < mod; y++)
         {
            if((x + y + 1) % mod == 0)
            {
               count++;
            }
         }
      }

      cout << count << "\n";
   }
}
```

This example simply runs through every element (x, y) in $\mathbb{F}_p^2$ and checks to see if the pair satisfies the equation—here $x^2 + y^2 + 1 = 0(p)$. Although it is somewhat silly, this method works for the first five-hundred primes surprisingly well, despite the calculation taking longer and longer as p increases, as there are many more pairs (x, y) to test. Once the program has finished checking every pair, it prints the number of solutions to the console and begins the process again with the next prime.

Using the above program and others similar, we were able to count the number of solutions to each equation listed in Section 2. The number of solutions to each equation up to the first 30 primes are listed in the table below.

p	$x^2+y^2=0$	$x^2+y^2+1=0$	$x^2+2xy+y^2+1=0$	$y^2=x^3+1$
2	2	2	2	2
3	1	4	0	3
5	9	4	10	5
7	1	8	0	11
11	1	12	0	11
13	25	12	26	11
17	33	16	34	17
19	1	20	0	11
23	1	24	0	23
29	57	28	58	29
31	1	32	0	35
37	73	36	74	47
41	81	40	82	41
43	1	44	0	35
47	1	48	0	47
53	105	52	106	53
59	1	60	0	59
61	121	60	122	47
67	1	68	0	83
71	1	72	0	71
73	145	72	146	83
79	1	80	0	83
83	1	84	0	83
89	177	88	178	89
97	193	96	194	83
101	201	100	202	101
103	1	104	0	83
107	1	108	0	107
109	217	108	218	107
113	225	112	226	113

A pattern in these numbers the reader will notice is the fact that in the first and third equations, the number of solutions in a given field $\mathbb{F}_p$ takes on either a value close to $2p$, if $p \equiv 1 \bmod 4$, whereas when $p \equiv 3 \bmod 4$, the number of solutions is 1 or 0 accordingly. Note that in this case, for the equation $x^2 + y^2 = 0$, the one solution is of course the trivial solution $x = y = 0$.

More precisely, for (2.1), the number of solutions in $\mathbb{F}_p$ is 1 if $p \equiv 1 \bmod 4$ and $2p - 1$ if $p \equiv 3 \bmod 4$. For (2.3), the number of solutions in $\mathbb{F}_p$ is 0 when $p \equiv 1 \bmod 4$ and $2p$ when $p \equiv 3 \bmod 4$. Closer inspection reveals that for (2.2), a similar pattern occurs; when $p \equiv 1 \bmod 4$, the number of solutions is $p - 1$, and when $p \equiv 3 \bmod 4$, the number of solutions is $p + 1$. We will inspect all of these cases as well as the final equation in more detail after having developed the idea of multiplicative characters and Gauss and Jacobi Sums, which are essential to understanding how to calculate the number of solutions to equations such as these for an arbitrary $\mathbb{F}_p$.

4. The Legendre Symbol and other Multiplicative Characters

To understand Gauss and Jacobi sums we must first define the notion of a multiplicative character, which we will do by first defining the Legendre symbol, or the multiplicative character of order 2, and then generalizing to higher orders. In order to define the Legendre symbol, we will first define a quadratic residue. For the rest of this section, we will assume p is a prime greater than 2.

Definition 4.1. Given a finite field $\mathbb{F}_p$, an element $a \in \mathbb{F}_p$ is called a quadratic residue modulo p if there exists an element $x \in \mathbb{F}_p$ such that $x^2 = a$.

In terms of the integers, this is equivalent to the statement that there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod p$. It now becomes easy to define the Legendre symbol.

Definition 4.2. The Legendre symbol is a function $\left(\frac{a}{p}\right)$ from $\mathbb{F}_p$ to $\{0, 1, -1\}$ defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ if } a = 0 \\ 1, \text{ if } a \text{ is a quadratic residue mod } p, \text{ and} \\ -1 \text{ otherwise.} \end{cases}$$

Here we will state without proof two properties of quadratic residues and the Legendre symbol before generalizing to higher order multiplicative characters. The proof of the first property follows from one of the properties of multiplicative characters we will discuss later on. The proof of these properties can be found in Section 1 of Chapter 5 in [1].

Proposition 4.3. *In a given $\mathbb{F}_p^\times$, there are as many elements which are quadratic residues as there are elements which are not quadratic residues.*

Proposition 4.4. *Let p be an odd prime. Then $\left(\frac{a}{p}\right) = a^{(p-1)/2}(p)$.*

We will now expand to the definition of multiplicative characters. In general, the Legendre Symbol can be said to be a function from $\mathbb{F}_p$ to μ_2^0 which sends the zero element of $\mathbb{F}_p$ to $0 \in \mu_2^0$ and extends a function from $\mathbb{F}_p^\times$ to μ_2.

Now the definition can be expanded to higher orders, giving us the notion of a multiplicative character.

Definition 4.5. A multiplicative character of order n on a finite field $\mathbb{F}_p$ is a function $\chi : \mathbb{F}_p \to \mu_n^0$ such that:

(1) $\chi(0) = 0$,
(2) for any $a, b \in \mathbb{F}_p^\times, \chi(ab) = \chi(a)\chi(b)$.

Notice that for the first condition, χ takes $0 \in \mathbb{F}_p$ and send it to $0 \in \mathbb{C}$. Note also that (2) implies that $\chi(1) = 1$.

It is perhaps worth noting that the definition does not really need to include *only* elements of μ_n^0 in the image of $\mathbb{F}_p$. In fact, the definition would be exactly the same without this restriction. If we allow χ to map elements of $\mathbb{F}_p$ to any values of $\mathbb{C}$, not just the n-th roots of unity, we shall see that (2) implies that for any $a \in \mathbb{F}_p, \chi(a) \in \mu_n^0$. In general, we say that (2) means that χ is a *homomorphism*.

Proof. If $a = 0, \chi(a) = 0 \in \mathbb{C}$, which is in μ_n^0 by definition. If $a \neq 0$, then $a^{p-1} = 1$, since $\mathbb{F}_p^\times$ is a cyclic group. Then $\chi(a)^{p-1} = \chi(a^{p-1})$ by condition (2), and thus $\chi(a)^{p-1} = \chi(1) = 1$. □

Proposition 4.6. *Let p be a prime greater than 3 and let $r \in \mathbb{F}_p$ be a generator of the group $\mathbb{F}_p^\times$. Then there exists a multiplicative character $\chi : \mathbb{F}_p \to \mu_3^0$ such that $\chi(r) = \omega_3$ if and only if $p \equiv 1$ mod 3.*

Proof. First, suppose such a character exists, and denote it by χ. Assume by contradiction that $p \equiv 2 \bmod 3$. Since r generates the group, we know that $r^{p-1} = 1$. Then $\chi(r^{p-1}) = \chi(1) = 1$, as χ is a homomorphism. Furthermore, $\chi(r) = \omega_3$ by assumption, and again because χ is a homomorphism, $\chi(r^2) = \omega_3^2$. Continuing this process, we find that for any $r^k \in \mathbb{F}_p$, $\chi(r^k) = \omega_3^k = \omega_3^{k \bmod 3}$. This last equality holds because $\{1, \omega_3, \omega_3^2\}$ forms a cyclic group with multiplication. Then, since $p \equiv 2 \bmod 3$ by assumption, $p - 1 \equiv 1 \bmod 3$, and thus $\chi(r^{p-1}) = \omega_3$. This is in direct contradiction to the previous statement about $\chi(r^{p-1})$, and thus no such χ can exist.

Now, assume $p \equiv 1 \bmod 3$. To show that such a character exists, we will construct one from the generative property of r and show that it is a homomorphism.

To begin, let $\chi(0) = 0$ and $\chi(1) = 1$, and $\chi(r) = \omega_3$. This guarantees that the first condition is met. Now, let $\chi(r^k) = \omega_3^k = \omega_3^{k \bmod 3}$.

Now consider $r^\alpha, r^\beta \in \mathbb{F}_p^\times$, where $\alpha \neq \beta$. $\chi(r^\alpha) \cdot \chi(r^\beta) = \omega_3^{\alpha \bmod 3} \cdot \omega_3^{\beta \bmod 3} = \omega^{(\alpha+\beta) \bmod 3}$, which is equal to $\chi(r^{\alpha+\beta}) = \chi(r^\alpha \cdot r^\beta)$. Note that this is only valid when $p \equiv 1 \bmod 3$ because then $p - 1 \equiv 0 \bmod 3$, and therefore $[\alpha + \beta](3) = [[\alpha + \beta](p-1)](3)$. That is to say, only when $p \equiv 1 \bmod 3$ is this construction of χ well defined.

Thus, for any $a, b \in \mathbb{F}_p$, if $a, b \neq 0$ then condition (2) holds. If one or both of a and b is the zero element of $\mathbb{F}_p$, then $\chi(ab) = \chi(0) = 0 = \chi(a) \cdot \chi(b)$. Thus χ is a homomorphism, and is therefore a multiplicative character. □

Remark 4.7. Note that if $\chi(r) = \omega, \chi(r^2) = \omega^2, \chi(r^3) = 1$, and so on, then since $p \equiv 1 \bmod 3$, this means that $\mathbb{F}_p^\times$ will contain equal numbers of elements which map to each $1, \omega$, and ω^2. This property holds in general, and thus we can obtain Proposition 4.3.

This proof can, of course, be generalized for higher order multiplicative characters. As a result, if $n \equiv 1 \bmod p$, there will be n characters from $\mathbb{F}_p$ to μ_n^0.

Proposition 4.8. *The Legendre Symbol is a multiplicative character of order 2.*

Proof. First, note that $\left(\frac{a}{p}\right)$ can have values $0, -1$, or 1, which make up the three elements of μ_2^0. $\left(\frac{0}{p}\right)$ is defined to be 0, so the first condition is met.

Now consider $r \in \mathbb{F}_p$ such that r is a generator of the group $\mathbb{F}_p^\times$. Assume that r is a quadratic residue modulo p. Then there is an element $a \in \mathbb{F}_p^\times$ such that $r = a^2$. If a generated $\mathbb{F}_p^\times$, then the order of a would be twice the order of r, but then r would not generate $\mathbb{F}_p^\times$. But, if a did not generate $\mathbb{F}_p^\times$, then r could not either, since the order of r is less than that of a. Thus, r cannot be a quadratic residue modulo p, and therefore $\left(\frac{r}{p}\right) = -1$. Since $\omega_2 = -1$, condition (2) is satisfied for our definition.

Finally, consider elements $r^n, r^m \in \mathbb{F}_p^\times$. Using Proposition 4.4, we find that $\left(\frac{r^n \cdot r^m}{p}\right) = (r^{n+m})^{(p-1)/2}(p) = r^{n(p-1)/2} \cdot r^{m(p-1)/2}(p) = \left(\frac{r^n}{p}\right)\left(\frac{r^m}{p}\right)$.

Thus the Legendre symbol is a homomorphism, and therefore it is indeed a multiplicative character.

□

Now we will introduce the trivial multiplicative character.

Definition 4.9. The trivial multiplicative character on $\mathbb{F}_p$, denoted ε, is the function which maps every element of $\mathbb{F}_p$ to 1. It is easy to see this satisfies all of the properties of a multiplicative character except the first, since $\varepsilon(0)$ is defined to be 1 as well.

Proposition 4.10. *If p is a prime and $n \equiv 1$ mod p, then the number of solutions to the equation $x^n = a$ in the field $\mathbb{F}_p$ is $\sum_{\chi^n=\varepsilon} \chi(a)$, where $\chi^n = \varepsilon$ is the condition that the character χ has order dividing n.*

Proof. First, let r be a generator of the group $\mathbb{F}_p^\times$. Note that since $n \equiv 1 \bmod p$, there are exactly n characters of order dividing n, since $\chi(r)$ must be an n-th root of unity, and there will be a unique multiplicative character sending r to each $n-$th root of unity, so that in total, there are n of these characters. For the rest of this proof, we will denote this set of multiplicative characters by $\mathcal{C}$.

Now, if $a = 0$, the equation $x^n = a$ has one solution, namely that in which $x = 0$. Furthermore, $\chi(0) = 0$ for all $\chi \in \mathcal{C}$, except in the case where $\chi = \varepsilon$. Then, $\chi(0) = 1$ by definition, and so the number of solutions to $x^2 = a$ is in fact $\sum_{\chi^n=\varepsilon} \chi(a)$.

In the case where a is an element not equal to zero such that $x^n = a$ is solvable, then there is an element $b \in \mathbb{F}_p^\times$ such that $b^n = a$. Then for each $\chi \in \mathcal{C}$, since $\chi^n = \varepsilon$, $\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \varepsilon(b) = 1$, and thus $\sum_{\chi^n=\varepsilon} \chi(a) = n$, which is the number of solutions to the equation $x^n = a$.

Finally, in the case where $x^n = a$ has no solutions, we need to show that $\sum_{\chi^n=\varepsilon} \chi(a) = 0$. Call this sum T. In the group $\mathbb{F}_p^\times$, $a = r^k$ for some k. Since $x^n = a$ is not solvable, n cannot divide k. Let λ be the function defined by $\lambda(r^k) = e^{2\pi i(k/p-1)}$, and define $\chi = \lambda^{(p-1)/n}$. Then $\chi(a) = \chi(r)^k = e^{2\pi i(k/n)}$, which is not equal to 1, as n does not divide k. Furthermore, $\chi^n = \lambda^{p-1} = \varepsilon$. Using this character χ, we find that $\chi(a)T = T$, and thus $T = 0$. □

Remark 4.11. Notice that if p is an odd prime and $n = 2$, this proposition gives that the number of solutions to $x^2 = a$ is $\sum_{\chi^2=\varepsilon} \chi(a)$, which, since $n = 2$ and there are only two characters of order dividing 2, is $1 + \left(\frac{a}{p}\right)$. This same reasoning can be applied to show that the number of solutions to the equation $x^3 = a$ in $\mathbb{F}_p$ is $1 + \chi(a) + (\chi(a))^2$, where χ is the multiplicative character of order 3 sending r to ω_3. We will use both of these facts when computing the number of solutions to the equations with two variables listed above, but to understand these computations a little better, we will first briefly touch upon Gauss sums before introducing Jacobi sums, the main tool which will prove useful in this problem.

5. Gauss and Jacobi sums

Definition 5.1. If χ is a character on $\mathbb{F}_p$ and $a \in \mathbb{F}_p$, then the sum $\sum_{t\in\mathbb{F}_p} \chi(t)\omega_p^{at}$ is called a Gauss sum on $\mathbb{F}_p$ for the character χ, and is notated $g_a(\chi)$.

The Gauss sum for $a = 1$ is sometimes written simply as $g(\chi)$, and not $g_1(\chi)$.

Definition 5.2. Given two multiplicative characters χ and ψ on $\mathbb{F}_p$, the sum $\sum_{a+b=1} \chi(a)\psi(b)$ is called a Jacobi sum, and is notated $J(\chi, \psi)$. Note that the sum is over all pairs of a and b in $\mathbb{F}_p$ such that $a + b = 1$. If, for example, we are working in $\mathbb{F}_7$, the pairs $a = 6, b = 2$ and $a = 2, b = 6$ both satisfy the equation $a + b = 1$ and are counted as different pairs; thus each is included in the Jacobi sum.

The proof of the next proposition can be found in Section 2 of Chapter 8 in [1].

Proposition 5.3. *If $\chi \neq \varepsilon$, then $|g(\chi)| = \sqrt{p}$.*

We will now show a proof of a theorem presented by Ireland and Rosen, which gives a formula for calculating a Jacobi sum with Gauss sums. We will use this theorem later in demonstrating a bound for the number of solutions to (2.4).

Theorem 5.4. *Let χ and λ be nontrivial characters such that $\chi\lambda \neq \varepsilon$. Then $J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$.*

Proof. Note that

$$\begin{aligned} g(\chi)g(\lambda) &= \big(\sum_{x\in\mathbb{F}_p} \chi(x)\omega_p^x\big)\big(\sum_{y\in\mathbb{F}_p} \lambda(y)\omega_p^y\big) \\ &= \sum_{x,y\in\mathbb{F}_p} \chi(x)\lambda(y)\omega_p^{x+y} \\ &= \sum_{t\in\mathbb{F}_p} \big(\sum_{x+y=t} \chi(x)\lambda(y)\big)\omega_p^t. \end{aligned}$$

In the case where $t = 0$, the inner sum works out to be zero, since when $x+y = 0$, the sum becomes $\sum_{x\in\mathbb{F}_p} \chi(x)\lambda(-x) = \lambda(-1)\sum_{x\in\mathbb{F}_p} \chi\lambda(x)$. This is equal to zero since $\chi\lambda \neq \varepsilon$.

If $t \neq 0$, let $x', y' \in \mathbb{F}_p$ such that $x = tx'$ and $y = ty'$. Such elements must exist since t has a multiplicative inverse, as $\mathbb{F}_p^\times$ is a group with multiplication. Then when $x + y = t, x' + y' = 1$, and therefore

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)J(\chi, \lambda).$$

Thus,

$$g(\chi)g(\lambda) = \sum_{t=\mathbb{F}_p} \chi\lambda(t)J(\chi, \lambda)\omega_p^t = J(\chi, \lambda)g(\chi\lambda),$$

and the proof is complete. □

Corollary 5.5. *If χ, λ, and $\chi\lambda$ are not equal to ε, then $|J(\chi, \lambda)| = \sqrt{p}$.*

Proof. This follow immediately from the previous theorem, simply by taking the absolute value of both sides of the equation and using Proposition 5.3. □

6. The application of Jacobi Sums to Counting Solutions of Equations Over Finite Fields

Now consider the first equation we introduced in Section 2, $x^2+y^2=0$. Imagine we are going to run our computer algorithm for counting the solutions to this equation by hand, instead of on a computer. For each pair $x, y \in \mathbb{F}_p$, we will square both and add one to our count if the sum of the squares is zero. Soon we will realize that there is a better way to count this equation by hand. Because each x^2 is the same as $(-x)^2$, we can save time by counting an extra solution for $(-x), y$ if x, y is a solution. Similarly, we can count $x, (-y)$ and $(-x), (-y)$ as solutions at the same time. Counting in this way, we can see that the total number of solutions to the equation will be $\sum_{a+b=0} N(x^2=a)N(y^2=b)$, where N denotes the number of solutions to the given equation. We will rearrange the sum by substituting b for $b+1$ to get $\sum_{a+b=1} N(x^2=a)N(y^2=b-1)$. Note that this does change the number of solutions to the part of the equation involving y. Then we can use the information in Remark 4.9 to find that

$$N(x^2+y^2=0) = \sum_{a+b=1} (1+(\frac{a}{p}))(1+(\frac{b-1}{p})) = \sum_{a+b=1} \left[1+(\frac{a}{p})+(\frac{b-1}{p})+(\frac{a}{p})(\frac{b-1}{p})\right]$$

$$= \sum_{a+b=1} 1 + \sum_{a+b=1} (\frac{a}{p}) + \sum_{a+b=1} (\frac{b-1}{p}) + \sum_{a+b=1} (\frac{a}{p})(\frac{b-1}{p}).$$

We can see that the first term will sum to p, since for each element $a \in \mathbb{F}_p$, there will be exactly one other element b such that $a+b=1$, namely, one more than the negative of a. For the second and third terms, which depend on only one of a and b, there will also be p terms of the sum, for the same reason. But because for each of these terms the Legendre symbol is either 1, -1, or 0, and there are an equal number of quadratic residues as nonresidues by Proposition 4.3, both the second and third terms will be zero. Thus the sum reduces to

$$N(x^2+y^2=0) = p + \sum_{a+b=1} (\frac{a}{p})(\frac{b-1}{p}),$$

where the second term is a Jacobi sum.

For (2.2), the result is nearly identical. The same process yields

$$N(x^2+y^2=-1) = p + \sum_{a+b=1} (\frac{a}{p})(\frac{b-2}{p}).$$

(2.3) is much easier to analyze. First, notice that $x^2+2xy+y^2=(x+y)^2$, so the number of solutions is really p times the number of solutions to $a^2=-1$, since for each $a \in \mathbb{F}_p$ such that $a^2=-1$, there are p pairs $x, y \in \mathbb{F}_p$ such that $x+y=a$, namely, the pairs $x, a-x$ for each $x \in \mathbb{F}_p$.

If $p \equiv 3 \bmod 4$, then $\frac{p-1}{2}$ is an odd number, and thus $\left(\frac{-1}{p}\right) = -1$ by Proposition 4.4. Then this equation has no solutions, a fact which is in accordance with the table we made above.

If $p \equiv 1 \bmod 4$, then this equation does have solutions. Applying a similar process as above, we find that

$$N((x+y)^2=-1)=pN(x^2=-1)=p[1+(\frac{-1}{p})].$$

Since we know -1 is a square in $\mathbb{F}_p$, $\left(\frac{-1}{p}\right)=1$ and therefore

$$N((x+y)^2=-1)=p(1+1)=2p,$$

again in agreement with our program.

Finally, (2.4) can be analyzed in a similar way to the above, but we will make use of the fact that $N(x^3=a)=1+\left(\frac{a}{p}\right)+(\chi(a))^2$, which we have not used in the above equations, since they were all of degree 3.

We can "split" the equation again in terms of counting its solutions and find that

$$N(y^2=x^3+1)=\sum_{a+b=1}N(y^2=a)N(x^3=-b).$$

Note that the formula includes $N(x^3=-b)$ and not $x^3=b$ because when we rearrange the original equation, we get $y^2-x^3=1$, so b in this case is $-x^3$. Then

$$N(y^2=x^3+1)=\sum_{a+b=1}(1+(\frac{a}{p}))(1+\chi(-b)+\chi^2(-b)).$$

Distributing terms and expanding the sum yields

$$\sum_{a+b=1}1+\sum_{a+b=1}(\frac{a}{p})+\sum_{a+b=1}\chi(-b)+\sum_{a+b=1}(\frac{a}{p})\chi(-b)+\sum_{a+b=1}\chi^2(-b)+\sum_{a+b=1}(\frac{a}{p})\chi^2(-b).$$

The first sum, as we know, becomes p, while the second and third sums are 0. Thus we find that

$$N(y^2=x^3+1)=p+\sum_{a+b=1}(\frac{a}{p})\chi(-b)+\sum_{a+b=1}\chi^2(-b)+\sum_{a+b=1}(\frac{a}{p})\chi^2(-b).$$

Note here that $\chi(-b)=\chi(-1)\chi(b)=(-1)\chi(b)$ when $p\equiv 3 \bmod 4$, and $\chi(b)$ when $p=1(4)$, so this term pushes the number of solutions up or down from p depending on the nature of p. For the middle sum, we find that $\sum_{a+b=1}\chi^2(-b)=\sum_{a+b=1}\chi^2(-1)\chi^2(b)=\sum_{a+b=1}\chi^2(b)$. Since χ^2 is a multiplicative character, this term is also 0, and so

$$N(y^2=x^3+1)=p+\sum_{a+b=1}(\frac{a}{p})\chi(-b)+\sum_{a+b=1}(\frac{a}{p})\chi^2(b).$$

Using Corollary 5.5, we see that the number of solutions is within an error of $2\sqrt{p}$ of p; that is,

$$|p-N(y^2=x^3+1)|<p+2\sqrt{p}.$$

This inequality must be strict because $N(y^2=x^3+1)$ is an integer, whereas $p-2\sqrt{p}$ and $p+2\sqrt{p}$ are not, since p is a prime and therefore $2\sqrt{p}$ is not an integer.

7. Conclusion

We have shown that the problem of counting solutions to diophantine equations modulo p is solvable in specific cases through the development of Gauss and Jacobi sums, which are crucial to understanding it. We outlined four specific equations to examine, and, using these tools, have computed formulas for determining how many solutions these equations will have in a given $\mathbb{F}_p$. Since the use of a computer program to calculate these figures by "brute force" does not give any indication as to why patterns occur, Jacobi Sums proved to be more insightful to exploring the nature of these equations over different $\mathbb{F}_p$.

Acknowledgments

I'd first like to thank my mentor, Gal, without whom I could not have written this paper.

I would also like to thank my parents for their love and support.

8. Bibliography

References

[1] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag New York Inc., 1982.