CONICS (TITLE TBD)

Abstract. to be written

Contents

1. Introduction

to be written

2. Projectivization of the problem

For now, let us fix a conic

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{2.1}$$

as well as a base field $\mathbb{F}_p$, for p an odd prime. (We defer treatment of the case $p = 2$ to §5.)

Let $\mathbb{A}^n$ denote n-dimensional affine space over $\mathbb{F}_p$. Taking the quotient of $\mathbb{A}^3\backslash\{0\}$ by the relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for $\lambda \neq 0$ produces the projective plane $\mathbb{P}^2$. We will write $[X : Y : Z] \in \mathbb{P}^2$ to denote the equivalence class of $(X, Y, Z) \in \mathbb{A}^3\backslash\{0\}$.

Let S denote the solution set of (2.1) in $\mathbb{A}^2$. Our aim is to characterize $|S|$ as a function of a, b, c, d, e, f, and p. To do so, we will first consider the homogeneous equation

$$aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0 \tag{2.2}$$

whose solutions define a set $S' \subset \mathbb{P}^2$. This "projectivization" of the conic enables us to apply the theory of quadratic forms, which we shall do in §3.

There is an evident injection $S \rightarrowtail S'$ sending (x, y) to $[x : y : 1]$. However, elements of S' of the form $[X : Y : 0]$ do not correspond to elements of S. These are solutions "at infinity" in the affine plane. Thankfully, these extraneous solutions are easily characterized: they are the solutions to the equation

$$aX^2 + bXY + cY^2 = 0 \tag{2.3}$$

on the projective line $\mathbb{P}^1$. Call this solution set $S_0 \subset \mathbb{P}^1$.

Lemma 2.1. $|S'| = |S| + |S_0|$.

Proof. A solution $[X : Y : Z]$ of (2.2) corresponds to a solution $(X/Z, Y/Z)$ of (2.1) if $Z \neq 0$ and to a solution $[X : Y]$ of (2.3) if $Z = 0$. □

3. Diagonalization of quadratic forms

(to be written)

4. Counting solutions of a conic in $\mathbb{P}^2$

We precede this undertaking with a brief review of relevant number theory.

The nonzero elements $\mathbb{F}_p^\times \subset \mathbb{F}_p$ form an abelian group under multiplication, and the squaring map

$$s\colon \mathbb{F}_p^\times \xrightarrow{x\mapsto x^2} \mathbb{F}_p^\times$$

is a homomorphism. If p divides $x^2-1=(x+1)(x-1)$, we must have $x=\pm 1 \bmod p$, thus $\ker s = \{\pm 1\}$. The quotient $\mathbb{F}_p^\times/s(\mathbb{F}_p^\times)$ is a group of order two:

$$\mathbb{F}_p^\times/s(\mathbb{F}_p^\times) \cong \{\pm 1\}.$$

Consider the homomorphism

$$\left(\frac{\cdot}{p}\right)\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times/s(\mathbb{F}_p^\times) \cong \{\pm 1\},$$

so that $\left(\frac{a}{p}\right)$ is -1 if a is a nonresidue, and 1 if a is a nonzero residue. For the sake of extending the above map to a monoid homomorphism

$$(\mathbb{F}_p,\times) \to (\{-1,0,1\},\times)$$

one defines $\left(\frac{0}{p}\right)=0$. This completes the definition of the Legendre symbol.

Note that each nonzero residue has exactly two square-roots (as we are assuming $p>2$ throughout).

In §3, we showed that, for an appropriate choice of coordinates, $aX^2+bXY+cY^2$ can be rewritten as

$$a_1X_1^2 + c_1Y_1^2 = 0 \tag{4.1}$$

and similarly, $aX^2+bXY+cY^2+dXZ+eYZ+fZ^2=0$ can be rewritten as

$$a_2X_2^2 + c_2Y_2^2 + f_2Z_2^2 = 0. \tag{4.2}$$

The different subscripts express that the base changes involved for (4.1) and (4.2) need not be the same!

Recall that the assumptions on the original coefficients $a,b,c,d,e,f\in\mathbb{Z}$ were that

- not all of a,b,c are zero, and
- $\gcd(a,b,c,d,e,f)=1$.

If p divides a,b, and c, then $a_1=c_1=0$ above. However, it will never be the case that $a_2=c_2=f_2=0$.

4.1. **Extraneous solutions.** Fix a quadratic nonresidue $r\in\mathbb{F}_p$. By scaling the equation (4.1) and by scaling and permuting the coordinates as appropriate, we can obtain one of the following equivalent forms:

(1) $0=0$ if both a_1,c_1 are zero,
(2) $X^2=0$ if exactly one of a_1,c_1 is zero,
(3) $X^2+Y^2=0$ if a_1c_1 is a nonzero quadratic residue, and
(4) $X^2+rY^2=0$ if a_1c_1 is a nonzero quadratic nonresidue.

The first of these has $|\mathbb{P}^1|=p+1$ solutions.

The second has one solution, namely $[0:1]$.

Evidently Y must be nonzero for the last two cases, so we can rewrite them as $(X/Y)^2=-1$ and $(X/Y)^2=-r$ respectively. If -1 is a quadratic residue, then $-r$ is not. It follows that $X^2+Y^2=0$ has two solutions and $X^2+rY^2=0$ has none.

If -1 is a nonresidue, the situation is reversed: $X^2 + Y^2 = 0$ has no solutions and $X^2 + rY^2 = 0$ has two solutions.

4.2. **Total solutions.** Let r be a quadratic nonresidue in $\mathbb{F}_p$ as before. Just as in §4.1, we can rewrite (4.2) as one of the following:

(1) $X^2 = 0$ if two of a_2, c_2, f_2 are zero,
(2) $X^2 + Y^2 = 0$ if exactly one of a_2, c_2, f_2 is zero, and the product of the other two is a quadratic residue,
(3) $X^2 + rY^2 = 0$ if exactly one of a_2, c_2, f_2 is zero, and the product of the other two is a quadratic nonresidue,
(4) $X^2 + Y^2 + Z^2 = 0$ if $a_2c_2f_2$ is a nonzero quadratic residue, and
(5) $X^2 + Y^2 + rZ^2 = 0$ if $a_2c_2f_2$ is a nonzero quadratic nonresidue.

Now we count the number of solutions in each of these cases.

Rank 1 (first case). The equation $X^2 = 0$ has $p + 1$ solutions.

Rank 2 (second and third cases). The only solution with $Y = 0$ is $[0 : 0 : 1]$. So assume $Y \neq 0$, and rewrite the equations as $(X/Y)^2 = -1$ and $(X/Y)^2 = -r$ respectively.

Suppose -1 is a quadratic residue mod p. The equation $(X/Y)^2 = -1$ gives two possibilities for X/Y, and thus $2p$ solutions in $\mathbb{P}^2$. Hence $X^2 + Y^2 = 0$ has $2p + 1$ solutions in total. On the other hand, $(X/Y)^2 = -r$ has no solutions, meaning $[0 : 0 : 1]$ is the only solution to $X^2 + rY^2 = 0$.

If -1 is a nonresidue, the situation is reversed, and $X^2 + Y^2 = 0$ has one solution while $X^2 + rY^2 = 0$ has $2p + 1$ solutions.

Rank 3 (fourth and fifth cases). Suppose -1 is a quadratic residue mod p. If $Z = 0$, then we are in the setting of §4.1 case (3), which has two solutions. Otherwise, we can divide by Z and obtain

$$(X/Z)^2 + (Y/Z)^2 = -1$$
$$(X/Z)^2 + (Y/Z)^2 = -r$$

respectively. By Proposition 4.1 below, these each have $p - 1$ solutions. Therefore $X^2 + Y^2 + Z^2 = 0$ and $X^2 + Y^2 + rZ^2 = 0$ each have $p + 1$ solutions.

Suppose -1 is a nonresidue. There are no solutions with $Z = 0$, so rewrite the equations as above. By Proposition 4.1 again, they each have $p + 1$ solutions.[1]

Proposition 4.1. *For $a \neq 0$, the equation $x^2 + y^2 = a$ has $p - \left(\frac{-1}{p}\right)$ solutions over $\mathbb{F}_p$. usage of S_0 in this proof is conflicting notation; need to address*

Proof. Let $S_a \subset \mathbb{A}^2$ denote the solution set of $x^2 + y^2 = a$. First we will show the statement for $a = 1$.

Let T denote the square-roots of -1 in $\mathbb{F}_p$. In the case that -1 is a nonresidue, T is empty. Consider the maps $f\colon S_1 \setminus (1, 0) \to \mathbb{F}_p \setminus T$ and $g\colon \mathbb{F}_p \setminus T \to S_1 \setminus (1, 0)$ defined by

$$f(x, y) = \frac{y}{x - 1}$$
$$g(m) = \left(\frac{m^2 - 1}{m^2 + 1}, \frac{-2m}{m^2 + 1}\right).$$

It is easy to check that they are inverse to one another, from which it follows that $|S_1| = |\mathbb{F}_p| - |T| + 1 = p - \left(\frac{-1}{p}\right)$ as desired.

[1] add comment about isomorphism to $\mathbb{P}^1$

Note that if a, a' are both nonzero residues (or both nonresidues) then $|S_a| = |S_{a'}|$. From the preceding, we have the claim for all residues a. Observe that $S_0 \cup \cdots \cup S_{p-1}$ gives a partition of $\mathbb{A}^2$. Since

$$|S_0| = \begin{cases} 1 & \text{if } \left(\frac{-1}{p}\right) = -1, \\ 2p+1 & \text{if } \left(\frac{-1}{p}\right) = 1, \end{cases}$$

for a nonresidue a we have

$$|S_a| = \frac{2}{p-1}\left(p^2 - |S_0| - \frac{p-1}{2}|S_1|\right) = p - \left(\frac{-1}{p}\right). \qquad \square$$

Example 4.1 (A zoo of possibilities)**.** In the table below, the first two columns reflect the discussion immediately preceding. The remaining columns consider the number of extraneous solutions. The entries marked "N/A" are impossible and explanation is given afterwards. For all other entries, examples are given for the specific case $p = 3$.

		# soln. in $\{Z = 0\}$			
rank of proj.	# soln. in $\mathbb{P}^2$	0	1	2	$p+1$
1	$p+1$	N/A	x^2	N/A	1
2	1	x^2+y^2	x^2+1	N/A	N/A
2	$2p+1$	N/A	x^2+x	xy	x
3	$p+1$	x^2+y^2+1	$x+y^2$	x^2+2y^2+1	N/A

- When the projectivization has rank 1, it is a double line. If this line is distinct from $\{Z = 0\}$, they meet at exactly one point. Otherwise they are the same line, giving $p+1$ solutions in $\{Z = 0\}$.
- When the projectivization has rank 2 and has $2p+1$ solutions, it is the union of two intersecting lines. These lines cannot be disjoint from $\{Z = 0\}$.
- There are $p+1$ solutions in $\{Z = 0\}$ only when the coefficients a, b, c are all zero. In particular, such a conic cannot have a projectivization of rank 3.

5. Counting solutions of a conic in $\mathbb{A}^2$

Given a conic, we now have almost all of the necessary pieces to determine how many solutions it has in $\mathbb{A}^2$ over $\mathbb{F}_p$. The remaining case is that of a conic over $\mathbb{F}_2$.

Fortunately there are very few such conics, and the solutions to

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

are the same as the solutions to

$$bxy + (a+d)x + (c+e)y + f = 0.$$

At this point, one can simply list out all the possibilities. It can be checked that the number of solutions in each case can be concisely written as $2 + b(-1)^{(a+d)(c+e)+f}$, where b is either 0 or 1. I have temporarily put this here, but this might flow better if moved into the proof of the theorem below.

(remainder to be written)

Theorem 5.1. *main theorem determining* $F(a, b, c, d, e, f, p)$

get a reference for the following fact (which we'll probably need)?

Proposition 5.1. *For an odd prime* p*, the Legendre symbol* $\left(\frac{-1}{p}\right)$ *is given by*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \cong 1 \pmod 4 \\ -1 & \text{if } p \cong 3 \pmod 4. \end{cases}$$

6. To the p-adics via Hensel's lemma

(to be written)

7. To $\mathbb{Q}$ via Hasse-Minkowski

(to be written)