

# CONICS (TITLE TBD)

ABSTRACT. We count the number of solutions of any affine plane conic modulo a prime. We use this result to determine whether such a conic has rational solutions.

## CONTENTS

1. Introduction	1
2. Projectivization of the problem	1
3. Diagonalization of quadratic forms	2
4. Counting solutions of a conic in $\mathbb{P}^2$	4
4.1. Extraneous solutions	5
4.2. Total solutions	5
5. Counting solutions of a conic in $\mathbb{A}^2$	6
6. To the $p$ -adics via Hensel's lemma	7
6.1. The $p$ -adics	7
6.2. Hensel's lemma	7
6.3. Existence of solutions over $\mathbb{Z}_p$	7
7. To $\mathbb{Q}$ via Hasse-Minkowski	8
References	8

## 1. INTRODUCTION

### 2. PROJECTIVIZATION OF THE PROBLEM

Let us begin by fixing a conic

$$(2.1) \quad C: ax^2 + bxy + cy^2 + dx + ey + f = 0$$

and a choice of ground field  $\mathbb{F}_p$ . We further require that not all of  $a$ ,  $b$ , and  $c$  be zero, and that the coefficients have gcd 1. **Might be worth explaining why we've chosen to impose these conditions.** Unless otherwise specified, all primes are odd. (We defer treatment of the case  $p = 2$  to §5.)

**Definition 2.1.** Let  $\mathbb{A}_{\mathbb{F}_p}^n$  denote  $n$ -dimensional affine space over  $\mathbb{F}_p$ . Define  $n$ -dimensional projective space over  $\mathbb{F}_p$  as the quotient

$$\mathbb{P}_{\mathbb{F}_p}^n = (\mathbb{A}_{\mathbb{F}_p}^{n+1} \setminus \{0\}) / \sim,$$

where we declare that  $(x_1, \dots, x_{n+1}) \sim (\lambda x_1, \dots, \lambda x_{n+1})$  for  $\lambda$  a nonzero scalar. We will primarily work with  $n = 2$ , and suppress the ground field from the notation. We will write  $[X : Y : Z] \in \mathbb{P}^2$  to denote the equivalence class of  $(X, Y, Z) \in \mathbb{A}^3 \setminus \{0\}$ .

With this construction in mind, we can *projectivize* our conic (2.1) from  $\mathbb{A}^2$  to  $\mathbb{P}^2$ , by writing it as a homogenous equation:

$$(2.2) \quad \tilde{C}: aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0.$$

Note that homogeneity ensures it is well-defined to ask when this equation has a solution in  $\mathbb{P}^2$ .

Let  $C(\mathbb{F}_p)$  denote the solution set of (2.1) in  $\mathbb{A}^2$ . Our aim is to characterize  $|C(\mathbb{F}_p)|$  as a function of the coefficients  $a, b, c, d, e, f$  and the prime  $p$ . The solutions of (2.2) define a set  $\tilde{C}(\mathbb{F}_p) \subset \mathbb{P}^2$ .

There is an evident injection  $C(\mathbb{F}_p) \hookrightarrow \tilde{C}(\mathbb{F}_p)$  sending  $(x, y)$  to  $[x : y : 1]$ . However, elements of  $\tilde{C}(\mathbb{F}_p)$  of the form  $[X : Y : 0]$  do not correspond to elements of  $C(\mathbb{F}_p)$ . These are solutions “at infinity” in the projective plane. Thankfully, these extraneous solutions are easily characterized: they are the solutions to the equation

$$(2.3) \quad \tilde{C}_0: aX^2 + bXY + cY^2 = 0$$

on the projective line  $\mathbb{P}^1$ . Call this solution set  $\tilde{C}_0(\mathbb{F}_p) \subset \mathbb{P}^1$ .

**Lemma 2.1.**  $|\tilde{C}(\mathbb{F}_p)| = |C(\mathbb{F}_p)| + |\tilde{C}_0(\mathbb{F}_p)|$ .

*Proof.* A solution  $[X : Y : Z]$  of  $\tilde{C}$  corresponds to a solution  $(X/Z, Y/Z)$  of  $C$  when  $Z \neq 0$ , and to a solution  $[X : Y]$  of  $\tilde{C}_0$  when  $Z = 0$ .  $\square$

### 3. DIAGONALIZATION OF QUADRATIC FORMS

In this section, we aim to simplify the equation defining the homogenized conic  $\tilde{C}$  via coordinate-changes of  $\mathbb{P}^2$ . Regard this equation as a quadratic form in three variables over  $\mathbb{F}_p$  (where  $p \neq 2$ ), which may be represented by the symmetric matrix

$$A = \begin{bmatrix} a & b/2 & d/2 \\ b/2 & c & e/2 \\ d/2 & e/2 & f \end{bmatrix}.$$

Indeed, letting  $v = [X \ Y \ Z]^T$ , the equation defining  $\tilde{C}$  is given by  $v^T A v$ . Now, any  $P \in \text{GL}_3(\mathbb{F}_p)$  gives rise to a change of coordinates  $v \mapsto Pv$  in  $\mathbb{P}^2$ . After performing this change of coordinates, the quadratic form defining  $\tilde{C}$  is given by

$$(Pv)^T A (Pv) = v^T (P^T A P) v,$$

hence is represented by the matrix  $P^T A P$ . Since  $P$  is invertible, the projective conic corresponding to the quadratic form given by  $P^T A P$  has the same number of solutions over  $\mathbb{F}_p$  as  $\tilde{C}$ . The following result is well-known (see for instance [2, Prop. 42:1]):

**Theorem 3.1.** *There exists some  $P \in \text{GL}_3(\mathbb{F}_p)$  such that  $P^T A P$  is diagonal.*

This significantly simplifies the set of conics which we must consider: a diagonal matrix

$$\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}$$

corresponds to the conic defined by  $\lambda_1 x^2 + \lambda_2 y^2 + \lambda_3 z^2 = 0$  (note that we cannot have  $\lambda_1 = \lambda_2 = \lambda_3 = 0$  by our initial assumptions). By further scaling and permuting coordinates as appropriate, we immediately obtain the following:

**Corollary 3.1.** *Fix a quadratic nonresidue  $r \in \mathbb{F}_p$ . There exists some  $P \in \text{GL}_3(\mathbb{F}_p)$  such that  $P^T A P$  is equal to one of the following:*

$$\begin{array}{cccccc} (1) & (2) & (3) & (4) & (5) & (6) \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} r & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & r \end{bmatrix} \end{array}$$

In the next section, we determine how many solutions each of the corresponding conics has in  $\mathbb{P}^2$ . For now, we determine to which of these six matrices  $A$  corresponds; however, we do not distinguish between the matrices (1) and (2) as the corresponding conics  $X^2 = 0$  and  $rX^2 = 0$  have equivalent vanishing sets.

**Theorem 3.2.** *Let*

$$\begin{aligned}\alpha &= 4acf - ae^2 - b^2f + bde - cd^2, \\ \beta &= 4ac + 4af + 4cf - b^2 - d^2 - e^2,\end{aligned}$$

*and let  $\gamma$  be defined by permuting the coordinates of  $A$  so that  $4ac - b^2 \neq 0$ , and setting  $\gamma = 4ac - b^2$ . Then  $A$  corresponds via Corollary 3.1 to*

- (1) or (2) if  $\alpha = \beta = 0$ ;
- (3) if  $\alpha = 0$ ,  $\beta \neq 0$ , and  $\gamma$  is a nonzero quadratic residue;
- (4) if  $\alpha = 0$ ,  $\beta \neq 0$ , and  $\gamma$  is a nonzero quadratic nonresidue;
- (5) if  $\alpha$  is a nonzero quadratic residue;
- (6) if  $\alpha$  is a nonzero quadratic nonresidue.

*Proof.* Let  $P \in \text{GL}_3(\mathbb{F}_p)$  be such that  $P^TAP$  is one of the six matrices in Corollary 3.1; these six matrices are distinguished by their ranks and the products of their nonzero eigenvalues. Since  $P$  is invertible, the rank of  $P^TAP$  is equal to that of  $A$ . By the rank-nullity theory, the rank of  $A$  is given by subtracting the multiplicity of the eigenvalue 0 from 3; this multiplicity is given by the number of times the characteristic polynomial of  $A$  is divisible by  $t$ . A **Magma** [1] computation shows that the characteristic polynomial of  $A$  is given by

$$t^3 + (-a - c - f)t^2 + \frac{1}{4}(4ac + 4af - b^2 + 4cf - d^2 - e^2)t + \frac{1}{4}(-4acf + ae^2 + b^2f - bde + cd^2).$$

Thus,  $A$  has rank 3 when  $\alpha = 4 \det A$  is nonzero; since

$$\det P^TAP = \det P^T \cdot \det A \cdot \det P = \det A \cdot (\det P)^2,$$

the determinant of  $A$  is a quadratic residue if and only if that of  $P^TAP$  is. Cases (5) and (6) of the theorem are now immediate.

Likewise,  $A$  has rank 2 when  $\alpha = 0$  and  $\beta \neq 0$ . Since  $\beta$  is the sum of  $4ac - b^2$ ,  $4af - d^2$ , and  $4cf - e^2$ , these cannot all be zero; the latter two are obtained from  $4ac - b^2$  by permuting the coordinates of  $A$ , which justifies step (1) in computing  $\gamma$ . Thus, assume that step (1) has been performed. If  $a \neq 0$ , then the **Magma** method **DiagonalForm()** shows that  $A$  diagonalizes to

$$\begin{bmatrix} a & 0 & 0 \\ 0 & \frac{4ac-b^2}{4a} & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

via some  $P$ . Thus, the product of the nonzero eigenvalues of this matrix is  $\gamma = 4ac - b^2$ , up to a square; the case  $c \neq 0$  is similar. Next, if  $a = c = 0$  and  $f \neq 0$ , then a similar **Magma** computation shows that  $A$  diagonalizes to

$$\begin{bmatrix} f & 0 & 0 \\ 0 & -\frac{e^2}{4f} & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

The product of the nonzero eigenvalues of this matrix is  $\gamma = -1$ , up to a square. Note that in this case the diagonalizing matrix  $P$  is only well-defined if  $e$  is nonzero as well, but this is clear as the condition  $\alpha = 0$  is equivalent to  $bf = de$ , and  $b \neq 0$  as  $4ac - b^2 \neq 0$  (thus,  $4ac - b^2 = -b^2$  is also  $-1$  up to a square). Finally, if

$a = c = f = 0$ , then either  $d = 0$  or  $e = 0$ , and the same **Magma** computation shows that in either case  $A$  diagonalizes to

$$\begin{bmatrix} b & 0 & 0 \\ 0 & -b/4 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

The product of the nonzero eigenvalues of this matrix is again  $\gamma = -1$ , up to a square. Since the matrices (3) and (4) are obtained from these diagonalized forms of  $A$  by scaling coordinates, it is clear that  $A$  corresponds to (3) if  $\gamma$  is a quadratic residue and to (4) if it is not.

Finally,  $A$  has rank 1 when  $\alpha = \beta = 0$ , which establishes the first case.  $\square$

We will also need an analogous result for quadratic forms  $ax^2 + bxy + cy^2$  in two variables, which follows immediately from the previous theorem by setting  $d = e = f = 0$ :

**Corollary 3.2.** *The matrix  $\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$  diagonalizes (as in Corollary 3.1, though with  $P \in \mathrm{GL}_2(\mathbb{F}_p)$ ) to*

- $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$  if  $a = b = c = d = 0$ ;
- $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$  or  $\begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix}$  if  $4ac - b^2 = 0$ ;
- $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  if  $4ac - b^2$  is a nonzero quadratic residue;
- $\begin{bmatrix} 1 & 0 \\ 0 & r \end{bmatrix}$  if  $4ac - b^2$  is a nonzero quadratic nonresidue.

#### 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

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

is a homomorphism. If  $p$  divides  $x^2 - 1 = (x + 1)(x - 1)$ , we must have  $x = \pm 1 \pmod{p}$ , so the kernel is  $\{\pm 1\}$ . The cokernel  $\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2$  is also group of order two:

$$\mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \cong \{\pm 1\}.$$

**Definition 4.1.** The *Legendre symbol* is the quotient map

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \cong \{\pm 1\},$$

where  $\left(\frac{a}{p}\right)$  is  $-1$  if  $a$  is a nonresidue, and  $1$  if  $a$  is a nonzero residue. This map extends to a multiplication-respecting map

$$\mathbb{F}_p \rightarrow \{-1, 0, 1\}$$

with  $\left(\frac{0}{p}\right)$  defined as  $0$ .

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

Our goal is to count the number of solutions of a conic  $C$  in  $\mathbb{A}^2$ . In light of Lemma 2.1, it suffices to count the number of points on  $\tilde{C}$  and  $\tilde{C}_0$ . In the preceding section, we showed that conics in projective space are equivalent to certain representative forms.

Now we count the number of solutions that each representative has.

**4.1. Extraneous solutions.** Fix a quadratic nonresidue  $r \in \mathbb{F}_p$ . By Corollary 3.2,  $\tilde{C}_0$  is equivalent to one of the following:

- (1)  $0 = 0$ ,
- (2)  $X^2 = 0$ ,
- (3)  $X^2 + Y^2 = 0$ , and
- (4)  $X^2 + rY^2 = 0$ .

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. By Theorem 3.2,  $\tilde{C}$  is equivalent to one of the following:

- (1)  $X^2 = 0$ ,
- (2)  $rX^2 = 0$ ,
- (3)  $X^2 + Y^2 = 0$ ,
- (4)  $X^2 + rY^2 = 0$ ,
- (5)  $X^2 + Y^2 + Z^2 = 0$ , and
- (6)  $X^2 + Y^2 + rZ^2 = 0$ .

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

*Rank 1: (1) and (2).* The equations  $X^2 = 0$  and  $rX^2 = 0$  each have  $p + 1$  solutions.

*Rank 2: (3) and (4).* 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: (5) and (6).* 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

$$\begin{aligned} (X/Z)^2 + (Y/Z)^2 &= -1 \\ (X/Z)^2 + (Y/Z)^2 &= -r \end{aligned}$$

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. <sup>1</sup>

**Proposition 4.1.** *For  $a \neq 0$ , the equation  $x^2 + y^2 = a$  has  $p - \left(\frac{-1}{p}\right)$  solutions over  $\mathbb{F}_p$ .*

*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  $a = 1$ .

<sup>1</sup>add comment about isomorphism to  $\mathbb{P}^1$

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  $f: S_1 \setminus (1, 0) \rightarrow \mathbb{F}_p \setminus T$  and  $g: \mathbb{F}_p \setminus T \rightarrow S_1 \setminus (1, 0)$  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.

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  $S_0 \cup \dots \cup S_{p-1}$  gives a partition of  $\mathbb{A}^2$ . Since

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

for a nonresidue  $a$  we have

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

**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  $\mathbb{A}_{\mathbb{F}_p}^2$ . 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  $F(a, b, c, d, e, f, p)$*

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

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

## 6. TO THE $p$ -ADICS VIA HENSEL'S LEMMA

In the preceding, we have been concerned with the number of solutions our conic  $C$  has over  $\mathbb{F}_p$ . Now we will instead consider the question of existence of solutions over the  $p$ -adic integers, which we answer with a sufficient condition in Theorem 6.2. Despite only being concerned with existence, the classification and analysis of the preceding sections will still play a major role.

We begin by recalling the definition of the  $p$ -adic integers and then stating Hensel's lemma, which will be our primary tool for this section.

### 6.1. The $p$ -adics.

**Definition 6.1.** The ring of  $p$ -adic integers  $\mathbb{Z}_p$  is the inverse limit of

$$\cdots \rightarrow \mathbb{Z}/p^3 \rightarrow \mathbb{Z}/p^2 \rightarrow \mathbb{Z}/p.$$

In other words, elements of  $\mathbb{Z}_p$  can be thought of as sequences  $(a_1, a_2, a_3, \dots)$  where  $a_i \in \mathbb{Z}/p^i$  and  $a_{i-1}$  is the image of  $a_i$  under  $\mathbb{Z}/p^i \rightarrow \mathbb{Z}/p^{i-1}$ .

Such an element can alternatively be interpreted as the series

$$b_0 + b_1p + b_2p^2 + b_3p^3 + \cdots$$

where  $b_0 = a_1$  and  $b_i = (a_{i+1} - a_i)/p^i$  for  $i \geq 1$ . Addition and multiplication are done as expected with “rightwards carrying.”

**6.2. Hensel's lemma.** Hensel's lemma gives us a sufficient condition for the existence of roots over  $\mathbb{Z}_p$ . We refer the reader to [3] for a proof of the following.

**Theorem 6.1** (Multivariate Hensel's lemma). *Let  $f \in \mathbb{Z}_p[x_1, \dots, x_n]$  be a polynomial in  $n$  variables and let  $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{Z}_p^n$  be such that  $f(\gamma) \equiv 0 \pmod{p}$  and  $\frac{\partial f}{\partial x_i}(\gamma) \not\equiv 0 \pmod{p}$  for some  $i \in \{1, \dots, n\}$ . Then there exists  $\alpha \in \mathbb{Z}_p^n$  such that, for all  $i$ ,  $\alpha_i \equiv \gamma_i \pmod{p}$  and  $f(\alpha) = 0$ .*

**6.3. Existence of solutions over  $\mathbb{Z}_p$ .** Using the results of §4 and Hensel's lemma, we deduce the following result.

**Theorem 6.2.** *Let  $p$  be an odd prime. Let  $C$  denote the conic (2.1) and  $\tilde{C}$  its projectivization (2.2). Then if  $\tilde{C}$  is either full rank or the union of two distinct lines over  $\mathbb{F}_p$ , the original conic  $C$  has a solution over  $\mathbb{Z}_p$ .*

Explicitly,

- If  $-1$  is a residue mod  $p$  and  $\tilde{C}$  is equivalent to (3), (5), or (6) of §4.2, then  $C$  has a solution over  $\mathbb{Z}_p$ .
- If  $-1$  is a nonresidue mod  $p$  and  $\tilde{C}$  is equivalent to (4), (5), or (6) of §4.2, then  $C$  has a solution over  $\mathbb{Z}_p$ .

*Proof.* We need a point of  $C$  over  $\mathbb{F}_p$  where not all partial derivatives of the conic vanish, i.e. a *non-singular* point. A non-singular point of  $C$  corresponds to a non-singular point of  $\tilde{C}$  not lying in  $\{Z = 0\}$ .

If  $\tilde{C}$  has full rank, it is equivalent to

$$X^2 + Y^2 + Z^2 = 0 \text{ or } X^2 + Y^2 + rZ^2 = 0$$

where  $r$  is a nonresidue. In each case, the condition of having a non-vanishing partial derivative is precisely that one of the coordinates must be nonzero—but this is automatically satisfied in  $\mathbb{P}^2$ .

If  $\tilde{C}$  consists of two distinct lines, its only singular point is where the two lines intersect. We recall from §4 that  $\tilde{C}$  has  $2p + 1$  points in  $\mathbb{P}^2$ , at most  $p + 1$  of which are extraneous. It follows that  $C$  has a non-singular point.  $\square$

If  $\tilde{C}$  is a double line or has only a single solution, then Hensel’s lemma is inconclusive as we do not have a solution mod  $p$  satisfying the requisite condition.

## 7. TO $\mathbb{Q}$ VIA HASSE-MINKOWSKI

(to be written)

## REFERENCES

- [1] Wieb Bosma, John Cannon, and Catherine Playoust. [The Magma algebra system I: The user language](#). *Journal of Symbolic Computation*, 24:235–265, 1997.
- [2] O. Timothy O’Meara. [Introduction to quadratic forms](#). Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.
- [3] Will Sawin. Answer to <https://mathoverflow.net/questions/108687>.