Remark. Right now this is mostly a summary. I haven't padded it with much exposition.

Remark. I think in the problem statement we want to require that $\gcd(a_1, a_2, a_3) = 1$, a stronger statement than $\gcd(a_1, \dots, a_6) = 1$, to guarantee that the "conic" is always actually a conic? See Example 2.1

1. The case $p = 2$

We consider the even prime separately because the diagonalization process employed in the other cases does not work in characteristic 2.

Fortunately there are very few conics over $\mathbb{F}_2$, 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.

2. The case $p \geq 3$

Starting with the conic

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

we projectivize it to obtain the following homogeneous equation in $\mathbb{P}^2$:

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

In $\{Z = 0\} = \mathbb{P}^1 \subset \mathbb{P}^2$, this equation is

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

Lemma 2.1. *The number of solutions to* (2.2) *in* $\mathbb{P}^2$ *is the sum of the numbers of solutions to* (2.1) *in* $\mathbb{A}^2$ *and* (2.3) *in* $\mathbb{P}^1$.

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 $Z = 0$. □

2.1. Diagonalization of quadratic forms.

$$aX^2 + \frac{4ac - b^2}{4a}Y^2 + \frac{4acf - ae^2 - b^2 f + bde - cd^2}{4ac - b^2}Z^2 = 0$$

Transformation matrix:

$$\begin{bmatrix} 1 & 0 & 0 \\ -\frac{b}{2a} & 1 & 0 \\ \frac{be - 2cd}{4ac - b^2} & \frac{-2ae + bd}{4ac - b^2} & 1 \end{bmatrix}$$

In the following, let r denote a quadratic nonresidue in $\mathbb{F}_p$.

Lemma 2.2. *By a change of coordinates, the equation* $aX^2 + bXY + cY^2 = 0$ *can be transformed into one of the following:*

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

The first of these has one solution, namely $[0:1]$.

Evidently Y must be nonzero for the other 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.

Lemma 2.3. *Every conic in $\mathbb{P}^2$ can be brought to one of the following forms:*

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

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 Lemma 2.2, case (2), 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 A.1, 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 A.1 again, they each have $p + 1$ solutions.

Example 2.1 (A zoo of possibilities)**.** In the table below, the first two columns reflect the preceding discussion. The remaining columns consider how many solutions lie in $\{Z = 0\} = \mathbb{P}^1 \subset \mathbb{P}^2$, which do not give solutions to the affine equation. The entries marked "N/A" are impossible—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
1	$p + 1$	N/A	x^2	N/A
2	1	$x^2 + y^2$	$x^2 + 1$	N/A
2	$2p + 1$	N/A	$x^2 + x$	xy
3	$p + 1$	$x^2 + y^2 + 1$	$x + y^2$	$x^2 + 2y^2 + 1$

- When the projectivization has rank 1, it is a double line. This line is distinct from $\{Z = 0\}$ and thus meets it at exactly one point.

otherwise our original conic was a constant, but maybe this can happen if we're not careful about the problem setup... ask

- When the projectivization has rank 2 and has $2p+1$ points, it is the union of two intersecting lines, neither of which is $\{Z = 0\}$. If these two lines intersect in $\{Z = 0\}$, then there is just one solution in $\{Z = 0\}$. Otherwise, there are two. This corresponds geometrically to parallel lines versus intersecting lines in $\mathbb{A}^2$.

Likewise... what if the original "conic" was just x

Appendix A. Number theory

The nonzero elements $\mathbb{F}_p^\times \subset \mathbb{F}_p$ form a 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 $x = \pm 1 \bmod p$, thus the kernel is $\{\pm 1\}$. Let $(\mathbb{F}_p^\times)^2$ be the image of the homomorphism. Then,

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

This implies that the product of two nonresidues or two residues is a residue, while the product of a (nonzero) residue and nonresidue is a nonresidue. Moreover, each nonzero residue has exactly two square-roots.

Proposition A.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 $a = 1$.

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.

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

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

The proof of the following fact is omitted.

Proposition A.2. *For an odd prime p, the Legendre symbol $\left(\frac{-1}{p}\right)$ is given by*

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