POINTS ON CONICS MODULO p

TEAM 2: JONGMIN BAEK, ANAND DEOPURKAR,
AND KATHERINE REDFIELD

Abstract. We compute the number of integer points on conics modulo p, where p is an odd prime. We extend our results to conics on the projective plane modulo p, and then to conics on the projective plane modulo n, for an integer n. We relate the existence of solutions on the projective plane modulo n to the existence of rational solutions using the Hasse–Minkowski theorem.

1. Introduction

Consider the quadratic polynomial q given by

$$q(x, y) = ax^2 + by^2 + cxy + dx + ey + f, \tag{1.1}$$

where a, b, c, d, e and f are integers with no common divisor. We know that the set points $(x, y) \in \mathbb{R}^2$ such that $q(x, y) = 0$ forms an ellipse, a parabola, a hyperbola or—in degenerate cases—a pair of lines, a line, a point or an empty set. We call the set of solutions of $q(x, y) = 0$ the *affine conic* determined by q.

Although we understand conics in $\mathbb{R}^2$ quite well, it is much more challenging to find points on conics if we restrict (x, y) to $\mathbb{Z}^2$. Even the question of deciding whether the conic has any points in $\mathbb{Z}^2$ can be nontrivial. For example, it is unclear if the polynomial $x^2 + 5y^2 - 3$ has any zeros in $\mathbb{Z}^2$, although it has infinitely many zeros in $\mathbb{R}^2$.

Similarly, we can consider the homogeneous quadratic

$$Q(x, y, z) = ax^2 + by^2 + fz^2 + cxy + dxz + eyz. \tag{1.2}$$

As we shall see, the zeros of Q in $\mathbb{Z}^3$ are closely related to the zeros of q in $\mathbb{Q}^2$. We call the set of nonzero solutions of $Q(x, y, z) = 0$, up to constant multiples, the *projective conic* determined by Q. Again, the question of the existence of integer points on projective conics is difficult to answer. For example, it is not clear whether $x^2 + 5y^2 - 3z^2$ has any integer solutions other than $(0, 0, 0)$.

We note that the integer solutions of $q(x, y) = 0$ or $Q(x, y, z) = 0$ give us solutions modulo n, where n is a positive integer, in particular

Date: December 12, 2007.

a prime integer. Since integers modulo a prime p form a field, the question of finding zeros modulo p is much easier that the question of finding integer zeros. Thus, we may find the zeros of q or Q modulo p (and modulo n, if possible) and from this knowledge, try to extract some information about the integer zeros.

In this paper, we focus on finding the zeros of q modulo a prime p and the the zeros of Q modulo p and modulo an arbitrary positive integer n. The paper is organized as follows: In Section 2 we find the number of points on the affine conic $q(x, y) \equiv 0 \pmod{p}$. In Section 3 we find the number of points on the projective conic $Q(x, y, z) \equiv 0 \pmod{p}$. In Section 4, we look at the number of points on the projective conic $Q(x, y, z) \equiv 0 \pmod{n}$. Finally, in Section 5 we discuss the implications of the number of solutions of $Q(x, y, z) \equiv 0 \pmod{n}$ to the existence of integer solutions of $Q(x, y, z) = 0$.

2. Points on Affine Conics modulo p

Definition 2.1. *An* affine conic $C_q \subseteq \mathbb{Z}^2$ *is the set of solutions to* $q(x, y) = 0$ *where* q *has the form in Equation* (1.1)*. Similarly, we define* $C_q(n) \subseteq (\mathbb{Z}/n\mathbb{Z})^2$ *to be the set of solutions to* $q(x, y) \equiv 0 \pmod{n}$*.*

Given an arbitrary odd prime p and a quadratic polynomial $q(x, y)$, we are interested in finding the number of points in the affine conic $C_q(p)$. Because there are only a finite number of values in $\mathbb{Z}/p\mathbb{Z}$, we know that there are only finitely many such points.

To count the number of points in $C_q(p)$, we start by examining the equation these points satisfy:

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f \equiv 0 \pmod{p}. \tag{2.1}$$

Now, let X be the column vector $\langle x, y \rangle$, and let M be the symmetric matrix $M = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$ with entries in $\mathbb{Z}/p\mathbb{Z}$. We can then write Equation (2.1) in bilinear form as:

$$q(X) = X^T M X + \begin{bmatrix} d & e \end{bmatrix} X + f \equiv 0 \pmod{p}. \tag{2.2}$$

Once we start using the equation's bilinear form, we see that we can change the basis in $(\mathbb{Z}/p\mathbb{Z})^2$ to simplify the coefficients inside M:

Lemma 2.2. *There exists a change of basis* $A \in GL_2(p)$ *and some* $S \in (\mathbb{Z}/p\mathbb{Z})^2$ *such that*

$$q'(X) = q(AX + S) \equiv X^T D X + \begin{bmatrix} d' & e' \end{bmatrix} X + f' \pmod{p} \tag{2.3}$$

where D *is a diagonal matrix. Furthermore, if* M *is invertible, we can choose our* S *such that the linear term disappears. In this case, we can*

rewrite Equation (2.3) *to say:*

$$q'(X) \equiv X^T DX + f' \pmod{p}. \tag{2.4}$$

Equivalently, we can write Equation (2.3) *and Equation* (2.4) *in linear form as follows:*

$$q'(x,y) \equiv a'x^2 + b'y^2 + d'x + e'y + f' \pmod{p} \tag{2.5}$$

$$q'(x,y) \equiv a'x^2 + b'y^2 + f' \pmod{p}. \tag{2.6}$$

Proof. By Theorem A.1 in the appendix, there exists an invertible matrix A and a diagonal matrix D such that $D = A^T MA$. Then, after change of basis via A, letting S be the column vector $\langle 0, 0\rangle$, we see that

$$\begin{aligned} q'(X) &\equiv (AX+S)^T M(AX+S) + \begin{bmatrix} d & e \end{bmatrix}(AX+S) + f \\ &\equiv (AX)^T M(AX) + \begin{bmatrix} d & e \end{bmatrix}(AX) + f \\ &\equiv X^T(A^T MA)X + \begin{bmatrix} d & e \end{bmatrix}(AX) + f \\ &\equiv X^T DX + \begin{bmatrix} d & e \end{bmatrix}(AX) + f \\ &\equiv X^T DX + \begin{bmatrix} d' & e' \end{bmatrix} X + f \pmod{p}, \end{aligned}$$

as desired. Furthermore, if M is invertible, choosing

$$S = -\frac{1}{2}(M^{-1})^T \begin{bmatrix} d \\ e \end{bmatrix}$$

instead leads to

$$\begin{aligned} q'(X) &\equiv (AX+S)^T M(AX+S) + \begin{bmatrix} d & e \end{bmatrix}(AX+S) + f \\ &\equiv X^T(A^T MA)X + \left(2S^T MA + \begin{bmatrix} d & e \end{bmatrix} A\right) X + \left(S^T MS + f\right) \\ &\equiv X^T DX + \left(2\left(-\frac{1}{2}\begin{bmatrix} d & e \end{bmatrix} M^{-1}\right) MA + \begin{bmatrix} d & e \end{bmatrix} A\right) X \\ &\qquad + \left(S^T MS + f\right) \\ &\equiv X^T DX + \left(S^T MS + f\right) \\ &\equiv X^T DX + f' \pmod{p}, \end{aligned}$$

as desired. □

Definition 2.3. *Two quadratic polynomials q and q' related as in Lemma 2.2 are called* identical up to a linear change of coordinates.

Definition 2.4. *We say that the quadratic polynomial $q(x,y)$ as given by Equation* (2.1) *is* nondegenerate *modulo p if $b^2 - 4ac \not\equiv 0 \pmod{p}$.*

p	Possible value of $Z_q(p)$
3	$1, 2, 4, 5$
7	$1, 6, 8, 13$
17	$1, 16, 18, 33$
29	$1, 28, 30, 57$

TABLE 1. Possible values of $Z_q(p)$ in case $q(x, y)$ is nondegenerate modulo p, for small odd primes p.

Hence if $q(x, y)$ is nondegenerate modulo p, we can write its bilinear form as in Equation (2.2) using an invertible matrix M.

It is clear from Lemma 2.2 that if $q(x, y)$ is nondegenerate modulo p, there exists some

$$q'(x, y) = a'x^2 + b'y^2 + f' \equiv 0 \pmod{p} \tag{2.7}$$

which is identical to $q(x, y)$ up to a linear change of coordinates.

Corollary 2.5. If two polynomials $q(x, y)$ and $q'(x, y)$ are identical up to a linear change of coordinates, there are exaclty as many points in $C_q(p)$ as there are in $C_{q'}(p)$.

Proof. This fact follows almost directly from Lemma 2.2, because we can write $q(AX + S) = q'(X)$ where A is invertible there exists a bijection between the solutions of q' and the solutions of q. □

2.1. Number of points in $C_q(p)$ if q is nondegenerate modulo p.

Let us introduce a simple notation that represents the number of points in $C_q(p)$:

$$Z_q(p) = |C_q(p)|.$$

We empirically computed $Z_q(p)$ for small odd primes p and all unique nondegenerate quadratic polynomials $q(x, y)$, up to linear change of coordinates, by writing a program that manually tests all points in $(\mathbb{Z}/p\mathbb{Z})^2$. The output of our program can be seen in Table 1.

These results indicate that depending on the conic, $Z_q(p)$ can be either 1, $p - 1$, $p + 1$ or $2p - 1$.

The following theorems explain the results found by our program, and are based on the integral solutions of Equation (2.6). Below the expression $\left(\frac{x}{p}\right)$ refers to the Legendre symbol (See Appendix B).

Theorem 2.6. *Given an odd prime p and a nondegenerate quadratic polynomial $q'(x,y) \equiv a'x^2 + b'y^2 + 0 \pmod{p}$,*

$$\left(\frac{-a'b'}{p}\right) = +1 \quad \Longrightarrow \quad Z_{q'}(p) = 2p - 1.$$

Proof. We can rewrite the condition $q'(x,y) \equiv 0 \pmod{p}$ as

$$a'x^2 \equiv -b'y^2 \pmod{p} \tag{2.8}$$

Note that by hypothesis $a', b' \neq 0$ because q' is nondegenerate modulo p. If $y = 0$, then the only solution to this equation is $x = 0$. If $y \neq 0$, then there are just as many solutions to Equation (2.8) as there are to the equation:

$$(x/y)^2 \equiv -b'/a' \pmod{p}$$

The fact that $-a'b'$ is a nonzero quadratic residue implies that $-b'/a'$ is also a nonzero quadratic residue, so for each of the remaining $p-1$ possible values of $y \in (\mathbb{Z}/p\mathbb{Z})$, there are 2 possible values of $x \in (\mathbb{Z}/p\mathbb{Z})$ for which the equality holds, namely,

$$x \equiv \pm y\sqrt{-\frac{b'}{a'}} \pmod{p}. \tag{2.9}$$

Altogether, there are $1 + 2(p-1) = 2p-1$ solutions to Equation (2.8), meaning that $Z_{q'}(p) = 2p - 1$. □

Theorem 2.7. *Given an odd prime p and a nondegenerate quadratic polynomial $q'(x,y) \equiv a'x^2 + b'y^2 + 0 \pmod{p}$,*

$$\left(\frac{-a'b'}{p}\right) = -1 \quad \Longrightarrow \quad Z_{q'}(p) = 1.$$

Proof. If $-a'b'$ is a not a quadratic residue, then neither is $-b'/a'$. Hence, Equation (2.9) is not satisfiable in $(\mathbb{Z}/p\mathbb{Z})^2$ unless $y = 0$. Since setting $y = 0$ yields only one solution, $(x,y) = (0,0)$, it must be that $Z_{q'}(p) = 1$. □

Theorem 2.8. *Given an odd prime p and a nondegenerate quadratic polynomial $q'(x,y) \equiv a'x^2 + b'y^2 + f' \pmod{p}$ where $f' \neq 0$,*

$$\left(\frac{-a'b'}{p}\right) = +1 \quad \Longrightarrow \quad Z_{q'}(p) = p - 1.$$

Proof. We can rewrite the condition $q'(x,y) \equiv 0 \pmod{p}$ as

$$a'x^2 - (-b')y^2 \equiv -f' \pmod{p}. \tag{2.10}$$

The fact that $-a'b'$ is a quadratic residue implies that either $-b'$ and a' are both quadratic residues or both are not. If not, we can simply multiply the whole equation by another quadratic nonresidue

to make the coefficients of x^2 and $-y^2$ quadratic residues. Therefore, we can assume without loss of generality that a' and $-b'$ are quadratic residues. Let $\alpha^2 = a'$ and $\beta^2 = -b'$. Then we can factor Equation (2.10) to say:

$$(\alpha x - \beta y)(\alpha x + \beta y) \equiv -f' \pmod{p}. \tag{2.11}$$

Since $f' \neq 0$, we can consider the above equation as factoring $-f'$ into two terms:

k_1 and k_2. This can be done in $p-1$ ways for $x, y \in \mathbb{Z}/p\mathbb{Z}$. For each such factoring we are simultaneously solving:

$$\begin{aligned} \alpha x - \beta y &\equiv k_1 \pmod{p} \\ \alpha x + \beta y &\equiv k_2 \pmod{p}. \end{aligned}$$

This gives us a unique solution since (α, β) and $(\alpha, -\beta)$ are independent. Thus there are $p-1$ total ways to solve Equation (2.10) in $(\mathbb{Z}/p\mathbb{Z})^2$, and $Z_{q'}(p) = p - 1$. □

Theorem 2.9. *Given an odd prime p and a nondegenerate quadratic polynomial $q'(x, y) = a'x^2 + b'y^2 + f'$ where $f' \neq 0$,*

$$\left(\frac{-a'b'}{p}\right) = -1 \quad \Longrightarrow \quad Z_{q'}(p) = p + 1.$$

Proof. Starting with the same conditions as the proof for Theorem 2.8, assume without loss of generality that a' is a quadratic residue. Then the fact that $-a'b'$ is a nonresidue implies that $-b'$ is a nonresidue. Let $\alpha^2 = a'$. We have two cases:

Case (1): $\left(\frac{-f'}{p}\right) = +1$.

Let $\phi^2 = -f'$. We can factor Equation (2.10) to say

$$(\alpha x - \phi)(\alpha x + \phi) \equiv -b'y^2 \pmod{p} \tag{2.12}$$

Assuming that $y \neq 0$, we are factoring $-b'y^2$ into two terms, k_1 and k_2, which can be done in $p - 1$ ways as before with Equation (2.11). Once again, each factorization yields a unique solution. If $y = 0$, then there are two more solutions from $\alpha x \equiv \pm\phi \pmod{p}$, giving us a total of $p + 1$ solutions. Hence $Z_{q'}(p) = p + 1$.

Case (2): $\left(\frac{-f'}{p}\right) = -1$

First, let us note that there are $(p - 1)/2$ such values for $-f'$ in $\mathbb{Z}/p\mathbb{Z}$.

Let $-f'_1, -f'_2$ be two of these values, and let

$$q'_1(x, y) = a'x^2 + b'y^2 = -f'_1$$

$$q_2'(x,y) = a'x^2 + b'y^2 = -f_2'$$

.

For any given solution (x_1, y_1) to q_1', we see that we can find a unique solution $(\sqrt{\frac{f_2'}{f_1'}}x_1, \sqrt{\frac{f_2'}{f_1'}}y_1)$ for q_2'. Therefore if we can find the total number of solutions to

$$q'(x,y) = a'x^2 + b'y^2 \equiv C \pmod{p} \tag{2.13}$$

.

in $(\mathbb{Z}/p\mathbb{Z})^2$ where C is a nonzero quadratic nonresidue, we can easily compute the number of solutions for a specific $C = f'$ because the solutions are uniformly distributed.

We know that there are $p^2 - 1$ possible nonzero values of C, and by Case (1) we know that if C is a quadratic residue there are exactly $p+1$ solutions to Equation (2.13) . Since there are $(p-1)/2$ quadratic residues in $(\mathbb{Z}/p\mathbb{Z})$ we see that there are exactly

$$(p^2-1) - \frac{(p+1)(p-1)}{2} = \frac{(p+1)(p-1)}{2}$$

combinations of $x, y \in (\mathbb{Z}/p\mathbb{Z})$ for which Equation (2.13) produces a nonzero quadratic nonresidue. Therefore, for each of the $(p-1)/2$ possible nonzero, nonresidue values of $C = -f'$, Equation (2.13) has exactly $\frac{(p+1)(p-1)}{2} / \frac{(p-1)}{2} = p+1$ solutions, so $Z_{q'}(p) = p+1$. □

Theorems 2.6 through 2.9 account for all possible conditions on a', b', f', hence we have completely characterized $Z_q(p)$ for any nondegenerate quadratic polynomial $q(x,y)$ modulo p.

2.2. **Number of points in $C_q(p)$ if q is degenerate modulo p.** We next explored the properties of degenerate conics. Our findings allowed us to modify the program used for Section 2.1 so that we could calculate $Z_q(p)$ when $q(x,y)$ was degenerate modulo p. A key aspect of our original program depended upon the fact that there are a finite number of unique nondegenerate quadratic polynomials modulo p up to a linear change in coordinates. We therefore first set out to discover the unique degenerate quadratic polynomials modulo p.

Lemma 2.10. *If $q(x,y)$ is degenerate modulo p, there exists some q' of the form*

$$q'(x,y) = a'x^2 + e'y + f' \tag{2.14}$$

that is identical to $q(x,y)$ up to a linear change of coordinates.

p	Possible values of $Z_q(p)$
3	$0, 3, 6, 9$
7	$0, 7, 14, 49$
17	$0, 17, 34, 289$
29	$0, 29, 58, 841$

TABLE 2. Possible values of $Z_q(p)$ in case $q(x, y)$ is degenerate modulo p, for small odd primes p.

Proof. From Lemma 2.2, we know that there exists a change of basis A that diagonalizes the bilinear form. Since the quadratic is degenerate, either the first diagonal entry, a', or the second, b', in the diagonalized $q(AX)$ will be zero. Without loss of generality, let $b' = 0$. We have

$$q(AX) = X^T DX + \begin{bmatrix} d' & e' \end{bmatrix} X + f.$$

Where $D = \begin{bmatrix} a' & 0 \\ 0 & 0 \end{bmatrix}$. Adding a vector S to X, where $S = \langle \frac{-d'}{2a'}, 0 \rangle$, yields the further change of linear coordinates,

$$\begin{aligned} q'(X) &= q(A(X+S)) \\ &= (X+S)^T D(X+S) + \begin{bmatrix} d' & e' \end{bmatrix} (X+S) + f \\ &= X^T DX + \left(2S^T D + \begin{bmatrix} d' & e' \end{bmatrix}\right) X + \left(\begin{bmatrix} d' & e' \end{bmatrix} S + f\right) \\ &= X^T DX + \left(\begin{bmatrix} -d & 0 \end{bmatrix} + \begin{bmatrix} d' & e' \end{bmatrix}\right) X + \left(\begin{bmatrix} d' & e' \end{bmatrix} S + f\right) \\ &= X^T DX + \begin{bmatrix} 0 & e' \end{bmatrix} X + f', \end{aligned}$$

as desired. In the cases where $a', b' = 0$, the linear equation $q(AX) = \begin{bmatrix} d' & e' \end{bmatrix} X + f \equiv 0 \pmod{p}$. We see that by a simple further change of basis, $Z_q(p) = Z_{q'}(p)$ for some $q'(X) = \begin{bmatrix} d' & e' \end{bmatrix} X + f$. In linear form, this can be written as $q'(x, y) = e'x + f$ as desired.

In both cases, we see that $q(X)$ is identical to $q'(X)$ up to a linear change of coordinates. □

By Lemma 2.10 we see that for any quadratic polynomial $q(x, y)$ which is degenerate modulo prime p there exists a $q'(x, y) = a'x^2 + e'y + f'$ to which $q(x, y)$ is identical up to a linear change of coordinates.

We used this fact along with Corollary 2.5 to modify the earlier version of our program to manually compute $Z_q(p)$ for small odd primes p and all degenerate quadratic polynomials $q(x, y)$ unique up to a linear change of coordinates. The modified program produced the results seen in Table 2.

These results indicate that given a prime p and a quadratic polynomial q which is degenerate modulo p, the number of points $Z_q(p)$ can

be either 0, p, $2p$ or p^2. The following theorems explain these results and are based upon the integral solutions of Equation (2.14).

Theorem 2.11. *Given an odd prime p and a degenerate quadratic polynomial $q'(x,y) \equiv a'x^2 + e'y + f' \pmod{p}$,*

$$e' \neq 0 \quad \Longrightarrow \quad Z_{q'}(p) = p.$$

Proof. Since $e' \neq 0$, we can rearrange the terms in $q'(x,y) \equiv 0 \pmod{p}$ to the following:

$$y \equiv (-f' - a'x^2)/e' \pmod{p}. \tag{2.15}$$

This indicates that for any value of x, there exists a unique y such that (x,y) satisfies $q'(x,y) \equiv 0 \pmod{p}$. Hence there are as many solutions as the possible values of x. Because $x \in \mathbb{Z}/p\mathbb{Z}$, it must then be that $Z_{q'}(p) = p$. □

Since we have already analyzed the case in which $e' \neq 0$, we now examine the cases in which $e' = 0$.

Theorem 2.12. *Given an odd prime p and a degenerate quadratic polynomial $q'(x,y) \equiv a'x^2 + e'y + f' \pmod{p}$,*

$$a' = e' = f' = 0 \quad \Longrightarrow \quad Z_{q'}(p) = p^2.$$

Proof. All possible pairs in $(\mathbb{Z}/p\mathbb{Z})^2$ satisfy $q'(x,y) \equiv 0 \pmod{p}$, so $Z_{q'}(p) = p^2$. □

Theorem 2.13. *Given an odd prime p and a degenerate quadratic polynomial $q'(x,y) \equiv a'x^2 + e'y + f' \pmod{p}$,*

$$a' = e' = 0,\ f' \neq 0 \quad \Longrightarrow \quad Z_{q'}(p) = 0.$$

Proof. In this case, $q'(x,y) \equiv 0 \pmod{P}$ reads $f' \equiv 0 \pmod{p}$, which is not true by hypothesis. Hence, no pair in $(\mathbb{Z}/p\mathbb{Z})^2$ satisfies the equation, so $Z_{q'}(p) = 0$. □

Theorem 2.14. *Given an odd prime p and a degenerate quadratic polynomial $q'(x,y) \equiv a'x^2 + e'y + f' \pmod{p}$,*

$$a', f' \neq 0,\ e' = 0 \quad \Longrightarrow \quad Z_{q'}(p) = 2p \text{ or } 0.$$

Proof. If $a' \neq 0$ and $e' = 0$, we can rearrange the terms in $q'(x,y) \equiv 0 \pmod{p}$ to the following:

$$x^2 \equiv -f'/a' \pmod{p} \tag{2.16}$$

Case (1): $\left(\frac{-a'f'}{p}\right) = +1$.

In this case, the right-hand side of Equation (2.16) is a nonzero quadratic residue, so the equation has two solutions. Because y is free, there are a total of $2p$ points in $C_{q'}(p)$. Thus $Z_{q'}(p) = 2p$.

Case (2): $\left(\frac{-a'f'}{p}\right) = -1$.

If $-a'f'$ is a nonresidue, Equation (2.16) has no solutions, as the left-hand side is a residue while the right-hand side is not. Therefore $Z_{q'}(p) = 0$. □

Theorem 2.15. *Given an odd prime p and a degenerate quadratic polynomial $q'(x, y) \equiv a'x^2 + e'y + f' \pmod{p}$,*

$$a' \neq 0,\ e' = f' = 0 \quad \Longrightarrow \quad Z_{q'}(p) = p.$$

Proof. Now the equation $q'(x, y) \equiv 0 \pmod{p}$ reads $a'x^2 \equiv 0 \pmod{p}$, whose solutions are $(0, y)$ for all $y \in \mathbb{Z}/p\mathbb{Z}$. Hence $Z_{q'}(p) = p$. □

Theorems 2.11 through 2.15 account for all possible conditions on a', e', f', hence we have completely characterized $Z_q(p)$ in terms of $q(x, y)$ in case it is degenerate modulo p.

3. Points on Projective Conics modulo p

We are now interested in rational points on conics. To study rational points, we will make use of the projective plane, which is defined as follows:

Definition 3.1. *Let F be a field. The* projective plane *over F, denoted by $\mathbb{P}^2(F)$, is the set of equivalence classes in*

$$\{\langle a, b, c\rangle \in F^3 \mid \langle a, b, c\rangle \neq \langle 0, 0, 0\rangle\}$$

where scalar multiples are identified. In other words, the similarity relation is given by

$$\forall \langle a, b, c\rangle \in F^3 - 0,\ \forall \lambda \in F - 0, \qquad \langle a, b, c\rangle \sim \langle \lambda a, \lambda b, \lambda c\rangle.$$

If we let $F = \mathbb{Q}$, then members of $\mathbb{P}^2(\mathbb{Q})$ are triples of rational numbers unique up to scalar multiplication. By scaling appropriately, we can treat them as triples of integers unique up to scalar multiplication. Then, they correspond naturally to ordered pair of rational numbers, as shown in the next proposition.

Proposition 3.2. *There is a bijective correspondence between the set of points $\langle x, y, z\rangle$ in $\mathbb{P}^2(\mathbb{Q})$ with $z \neq 0$ and the set of rational points in $\mathbb{Q}^2$, given by*

$$\langle x, y, z\rangle \longleftrightarrow \langle x/z, y/z\rangle.$$

Proof. The correspondence above is injective. If $\langle x, y, z\rangle = \langle x', y', z'\rangle$ in $\mathbb{P}^2(\mathbb{Q})$, then it must be that $x' = \lambda x,\ y' = \lambda y,\ z' = \lambda z$, for some λ. Then

$$\begin{aligned}\langle x'/z', y'/z'\rangle &= \left\langle \frac{\lambda x}{\lambda z}, \frac{\lambda y}{\lambda z}\right\rangle \\ &= \langle x/z, y/z\rangle.\end{aligned}$$

It is also surjective: if $\langle q_1, q_2\rangle \in \mathbb{Q}^2$ is a rational point, the projective line $(q_1 z, q_2 z, z)$, where z is the least common multiple of the denominators of q_1, q_2, will map to (q_1, q_2). □

We can now relate the number of rational points on (2.1) to points on the projective plane. We begin by homogenizing (2.1):

$$Q(x, y, z) = ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0. \tag{3.1}$$

Using Proposition 3.2, we see that counting solutions to (3.1) in $\mathbb{P}^2(\mathbb{Q})$ tells us something about the number of nontrivial solutions to (2.1) in $\mathbb{Q}^2$. (To be exact, they are equal once projective points with $z = 0$ are omitted, according to Proposition 3.2.) Therefore, the number of solutions to (3.1) in $\mathbb{P}^2(\mathbb{Q})$ is of interest to us.

For the remainder of the section, p denotes an odd prime, and we will use $\mathbb{P}_p^2$ as a shorthand for $\mathbb{P}^2(\mathbb{F}_p)$. Note that Proposition 3.2 is still relevant because $\mathbb{P}_p^2$ can be interpreted as $\mathbb{P}^2(\mathbb{Q})$ modulo p.

More formally, we take the approach in Section 2 and attempt to characterize the number of solutions in $\mathbb{P}_p^2$ to an arbitrary quadratic polynomial $Q(x, y, z)$. In treating Equation (3.1), we can once again employ symmetric bilinear forms:

$$X^T \begin{bmatrix} a & b/2 & d/2 \\ b/2 & c & e/2 \\ d/2 & e/2 & f \end{bmatrix} X \equiv 0 \pmod{p}. \tag{3.2}$$

Here X denotes the column vector $\langle x, y, z\rangle$. We will be using Q to denote the matrix of the symmetric bilinear form as well. In that notation, the equation reads $X^T Q X \equiv 0 \pmod{p}$.

Definition 3.3. *A* projective conic $\widetilde{C}_Q(p)$ *is the set of solutions to* $Q(x, y, z) \equiv 0 \pmod{p}$ *in* $\mathbb{P}_p^2$ *where* Q *has the form in* (3.1).

We denote by $\widetilde{Z}_Q(p)$ the cardinality of $\widetilde{C}_Q(p)$. Our goal, then, is to compute values of $\widetilde{Z}_Q(p)$ for different symmetric bilinear forms Q.

3.1. **Counting equivalent classes of symmetric bilinear forms.** As in $(\mathbb{Z}/p\mathbb{Z})^2$, it is not necessary to count the number of solutions to all symmetric bilinear forms in $\mathbb{P}^2_p$. We exploit the fact that the numbers of solutions to two symmetric bilinear forms Q and Q' are the same if the two forms are similar under the equivalence relation defined in Section A of the appendix, i.e. there exists an $A \in GL_3(p)$ such that $Q' = A^TQA$. To see why, realize that the condition $Q' = A^TQA$ is the same as saying $Q'(X) = Q(AX)$. Thus A is simply a change of basis, and the number of solutions is preserved.

By Theorem A.1, all symmetric bilinear forms are similar to diagonal bilinear forms. In turn, we can prove that there are very few equivalence classes within diagonal bilinear forms.

Lemma 3.4. *Given an odd prime p, there exists a quadratic nonresidue η that can be written as the sum of two quadratic residues.*

Proof. Suppose the contrary that all sums of two quadratic residues are quadratic residues (or zero). This implies that quadratic residues are closed under addition. Note that $\mathbb{Z}/p\mathbb{Z}$ is generated by 1, which is a quadratic residue. So all nonzero elements of $\mathbb{Z}/p\mathbb{Z}$ would be residues, which is false. □

Lemma 3.5. *Two diagonal bilinear forms D and E over $\mathbb{P}^2_p$ are similar if the following two conditions hold:*

$$rk_p(D) = rk_p(E),$$

where rk_p denotes the rank modulo p, and

$$[\#\text{ of quadratic residues in entries of } D] \equiv [\#\text{ of quadratic residues in entries of } E] \pmod 2.$$

Proof. We begin by noting that D is similar to any diagonal matrix with its entries permuted, because we can pick row-switching elementary matrices as the change of basis. Also, picking an arbitrary nonsingular diagonal matrix as the change of basis has the effect of separately multiplying each entry by a square. Composing these operations, we see that D is similar to

$$D' = \begin{bmatrix} I_i & & \\ & \eta I_j & \\ & & 0 \end{bmatrix},$$

where i, j correspond to the numbers of residues and nonresidues along the diagonal of D, respectively. Note that $i + j = \mathrm{rk}_p(D)$.

In case $j \geq 2$, we perform the following additional operation: let η be the nonresidue written as the sum $\sigma_1^2 + \sigma_2^2$, which exists by Lemma

3.4. Take the identity matrix I_3 and replace a 2-by-2 square along the diagonal by $\frac{1}{\eta}\begin{bmatrix}\sigma_1 & \sigma_2\\ \sigma_2 & -\sigma_1\end{bmatrix}$. Here the 2-by-2 square in I_3 is chosen to correspond to a 2-by-2 subsquare of ηI_j sitting inside D'.

Denote the resulting matrix by J. We see that $J^T D' J$ looks exactly like D', except two η's along the diagonal are replaced by 1's. To check this, it suffices to examine only the rows corresponding to the nonidentity 2-by-2 subsquare of J:

$$\begin{aligned}\frac{1}{\eta}\begin{bmatrix}\sigma_1 & \sigma_2\\ \sigma_2 & -\sigma_1\end{bmatrix}^T\begin{bmatrix}\eta & 0\\ 0 & \eta\end{bmatrix}\frac{1}{\eta}\begin{bmatrix}\sigma_1 & \sigma_2\\ \sigma_2 & -\sigma_1\end{bmatrix} &= \frac{1}{\eta^2}\begin{bmatrix}\sigma_1\eta & \sigma_2\eta\\ \sigma_2\eta & -\sigma_1\eta\end{bmatrix}\begin{bmatrix}\sigma_1 & \sigma_2\\ \sigma_2 & -\sigma_1\end{bmatrix}\\ &= \frac{1}{\eta^2}\begin{bmatrix}\eta^2 & 0\\ 0 & \eta^2\end{bmatrix}\\ &= I_2.\end{aligned}$$

Applying this operation as necessary, we can show that D is similar to $\begin{bmatrix}I_i & & \\ & \eta I_j & \\ & & 0\end{bmatrix}$ where $j \in \{0, 1\}$. In summary, the "canonical form" of the equivalence relation depends only on the rank of D and the parity of the number of residues along the diagonal of D. Therefore, if the premise of the lemma holds, then D and E have the same canonical form, which indicates that they are similar. □

Corollary 3.6. A symmetric bilinear form Q over $\mathbb{P}_p^2$ is equivalent to one of the following:

$$\left\{I_3, \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0\\ 0 & \eta & 0\\ 0 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}, 0\right\},$$

where η is a quadratic nonresidue modulo p.

Proof. We list all possible simplified forms obtained in the proof of Lemma 3.5, dropping scalar multiples. We caution the reader that if the rank is odd, there is exactly one canonical form instead of two: the two matrices (one for each parity of the number of residues along the diagonal) are not similar, but when treated as bilinear forms over the projective plane, they are identified under scalar multiplication. For instance,

$$I^3 \sim \begin{bmatrix}\eta & 0 & 0\\ 0 & \eta & 0\\ 0 & 0 & \eta\end{bmatrix}.$$

When the rank is even, scaling does not flip the parity, so the two canonical forms are preserved. □

Corollary 3.6 tells us that there are at most five distinct equivalence classes. We ask if there are exactly five equivalence classes:

Theorem 3.7. *The diagonal forms in Corollary 3.6 are distinct under the equivalence relation.*

Proof. Let D be a diagonal form given in Corollary 3.6. First note that for any invertible matrix modulo A, both A and A^T have full ranks. Therefore, the rank of $A^T DA$ is equal to the rank of D. Hence the rank is invariant under the equivalence relation.

Next, the quadratic residuosity of the product of the nonzero diagonal entries in D is invariant as well. Suppose that $D \sim E$, where D and E are two different forms in Corollary 3.6 with the same rank k. We have

$$A^T DA = E$$

for some invertible matrix A. Now we take the submatrices of A, D, E corresponding to the k-by-k top-left corner, and denote them by $\widetilde{A}, \widetilde{D}, \widetilde{E}$ respectively. They are related as follows:

$$\widetilde{A}^T \widetilde{D} \widetilde{A} = \widetilde{E}.$$

Note that because $\widetilde{E}$ is nonsingular, $\widetilde{A}$ must also be nonsingular. Also,

$$\left(\frac{\det \widetilde{E}}{p}\right) = \left(\frac{\det \widetilde{A}^T \widetilde{D} \widetilde{A}}{p}\right) = \left(\frac{\det \widetilde{A}}{p}\right)^2 \left(\frac{\det \widetilde{D}}{p}\right) = \left(\frac{\det \widetilde{D}}{p}\right).$$

Since the determinants of $\widetilde{D}$ and $\widetilde{E}$ are simply the products of the nonzero diagonal entries of D and E, respectively, our claim of invariance is proven.

Inspecting the forms in Corollary 3.6, we see that any two diagonal matrices differ in either their ranks, or in the quadratic residuosity of the product of nonzero diagonal entries. Therefore, they cannot be similar. □

Remark: We did not use the fact that we are operating in $\mathbb{P}_p^2$ rather than in a higher-dimensional projective space $\mathbb{P}_p^n$, which consists of lines in $(\mathbb{Z}/p\mathbb{Z})^{n+1}$. Therefore, we expect that the number of equivalent symmetric bilinear forms over $\mathbb{P}_p^n$ to be similarly determined. We conjecture it to be $\lceil 3n/2 \rceil + 2$. This number is obtained by counting one equivalence class for each odd rank, two for each even rank, and one for the all-zero form.

p	Possible values of $\widetilde{Z}_Q(p)$
3	$1, 4, 7, 13$
5	$1, 6, 11, 31$
7	$1, 8, 15, 57$
11	$1, 12, 23, 133$
13	$1, 14, 27, 183$

TABLE 3. Possible values of $\widetilde{Z}_Q(p)$, for small odd primes p.

3.2. **Number of points in $\widetilde{C}_q(p)$.** Using Matlab, we computed $\widetilde{Z}_Q(p)$ for small odd primes p, and for several polynomials Q representing each of the five equivalence classes in Theorem 3.7. (In fact, it would suffice to only try the five canonical forms in Corollary 3.6.) The results are given in Table 3. We observe empirically that

$$\widetilde{Z}_Q(p) \in \{1,\ p+1,\ 2p+1,\ p^2+p+1\}$$

for all symmetric bilinear form Q. The following theorems explicitly characterize the possible values of $\widetilde{Z}_Q(p)$ we observe.

The simplest number to account for is p^2+p+1, which is the number of all elements in $\mathbb{P}_p^2$.

Theorem 3.8.

$$Q \equiv 0 \pmod{p} \quad \Longleftrightarrow \quad \widetilde{Z}_Q(p) = p^2+p+1.$$

Proof. If Q is the zero matrix modulo p, all elements of the form $X = \langle x, y, z \rangle$ satisfies Equation (3.2). Since $|\mathbb{P}_p^2| = p^2+p+1$, it follows that $\widetilde{Z}_Q(p) = p^2+p+1$. Conversely, if all elements of $\mathbb{P}_p^2$ satisfies the equation, then for all $X, Y \in P_p^2$, we have

$$X^T Q Y \equiv (X^T Q Y + Y^T Q X)/2 \equiv (X+Y)^T Q (X+Y)/2 \equiv 0.$$

Fixing X, we get $(X^T Q)$ is a trivial linear map on $GL_3(p)$. But since this holds for all X, it must be that $Q \equiv 0$. □

Theorem 3.9.

$$rk_p(Q) = 1 \quad \Longrightarrow \quad \widetilde{Z}_Q(p) = p+1.$$

Proof. If Q has rank 1, we know from Corollary 3.6 that Q must be equivalent to $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ after a change of basis. A solution $\langle x, y, z \rangle$ to this diagonal form obeys the equation $x^2 \equiv 0$. So $x \equiv 0$, while y, z are free. Counting triples in $(\mathbb{Z}/p\mathbb{Z})^3$ yields p^2 solutions. Subtracting the

all-zero solution and identifying scalar multiples, we obtain $\widetilde{Z}_Q(p) = p+1$. □

Theorem 3.10.

$$rk_p(Q) = 2 \quad \Longrightarrow \quad \widetilde{Z}_Q(p) = 1 \text{ or } 2p+1.$$

Proof. Using the same logic as in Theorem 3.9, the symmetric bilinear form Q must be similar to either $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \eta & 0 \\ 0 & 0 & 0 \end{bmatrix}$ where η is a nonresidue. In either case, the corresponding polynomial has the form $x^2 + b'y^2 \equiv 0 \pmod{p}$, where $b \not\equiv 0 \pmod{p}$.

Rearranging the terms, we have

$$-b' \equiv (y/x)^2, \text{ or } x \equiv y \equiv 0. \tag{3.3}$$

If $-b$ is a quadratic residue modulo p, then there exists β such that $\beta^2 \equiv -b'$. Then Equation (3.3) is equivalent to $y/x \equiv \pm\beta$. Counting solutions in $(\mathbb{Z}/p\mathbb{Z})^3$ yields $(2p-1)p$. Subtracting the all-zero solution and dividing by $p-1$ to account for scaling, we get $\widetilde{Z}_Q(p) = 2p+1$.

If $-b$ is not a quadratic residue, $-b' \equiv (y/x)^2$ has no solution, in which case we only count solutions with $x \equiv y \equiv 0$. Then there is exactly one solution in $\mathbb{P}^2_p$, namely $\langle 0, 0, 1\rangle$. So $\widetilde{Z}_Q(p) = 1$. □

Theorem 3.11.

$$rk_p(Q) = 3 \quad \Longrightarrow \quad \widetilde{Z}_Q(p) = p+1.$$

Proof. Because Q has rank 3, Q is similar to I_3. So we can count solutions to $x^2 + y^2 + z^2 \equiv 0$. Rearranging the terms yields

$$x^2 + y^2 \equiv -z^2 \pmod{p}. \tag{3.4}$$

In comparison, consider solutions to

$$x^2 + y^2 \equiv -\eta z^2 \pmod{p}, \tag{3.5}$$

where η is a nonresidue modulo p. We remark that exactly one of -1 and $-\eta$ is a quadratic residue modulo p, since their product is a nonresidue.

Let K_1 and K_2 be the number of nonzero solutions to (3.4) and (3.5), respectively, in $(\mathbb{Z}/p\mathbb{Z})^3$. Note that a nonzero pair (x, y) satisfies exactly one of the two equations, depending on the quadratic residuosity of $x^2 + y^2$. Therefore, $K_1 + K_2$ is equal to the number of possible nonzero pairs (x, y):

$$K_1 + K_2 = 2(p^2 - 1).$$

The factor of 2 arises from that there are two possible values of z for each equation. Now let β be such that $\beta^2 = -1$ or $\beta^2 = -\eta$, depending on which one is the quadratic residue. Then, one of the two equations above factors as

$$(x - \beta z)(x + \beta z) \equiv -y^2. \tag{3.6}$$

Solving (3.6) is equivalent to simultaneously solving

$$\begin{aligned} x - \beta z &\equiv k_1 \\ x + \beta z &\equiv k_2 \end{aligned}$$

where $k_1 k_2 \equiv -y^2$.

If $y \not\equiv 0$, there are $p - 1$ ways to factor $-y^2$ into $k_1 k_2$, and each system of equation yields a unique solution. Lastly, there are $p - 1$ ways to choose y. Counting all these yields $(p-1)^2$ solutions. If $y \equiv 0$, we require $x = \pm\beta z$, which has $2(p - 1)$ solutions. The total, then, is $(p - 1)^2 + 2(p - 1) = p^2 - 1$.

This tells us that either K_1 or K_2 is $p^2 - 1$. However, since they add up to $2(p^2 - 1)$, they must both be $p^2 - 1$. Then, in either case, we obtain $\frac{p^2-1}{p-1} = p + 1$ solutions to Equation (3.4) in $\mathbb{P}_p^2$. □

In summary, we conclude the following about the number of solutions to Equation (3.1) on the projective plane:

Theorem 3.12. *The number of solutions to Equation* (3.1) *in* $\mathbb{P}_p^2$ *is*

$$\widetilde{Z}_Q(p) = \begin{cases} p^2 + p + 1, & \text{if } rk_p(Q) = 0, \\ p + 1, & \text{if } rk_p(Q) = 1, \\ 1 \text{ or } 2p + 1, & \text{if } rk_p(Q) = 2, \\ p + 1, & \text{if } rk_p(Q) = 3. \end{cases}$$

3.3. **Relation to $C_q(p)$.** The numbers we observe differ somewhat from the numbers of integral solutions to $q(x, y)$ modulo p. This can be explained by the fact that we are counting *points at infinity*, or points on the projective plane with $z = 0$. After a linear change of coordinates, these correspond to an arbitrary 2-dimensional subspace $V \subseteq (\mathbb{Z}/p\mathbb{Z})^3$. Hence, the number of solutions on $\mathbb{P}_p^2$ that actually gives rise to a rational point are

$$\widetilde{Z}_Q(p) - \frac{\left|\{X \in V - \{0\} \mid X^T Q X \equiv 0 \pmod p\}\right|}{p - 1}.$$

3.4. **Implication of factoring.** We can ask how the condition of Q factoring over $\mathbb{F}_p$ relates to the number of solutions. If Q factors non-trivially, then for some nonzero $v = \langle v_1, v_2, v_3 \rangle$ and $w = \langle w_1, w_2, w_3 \rangle$,

$$\begin{aligned} Q(x,y,z) &\equiv (v_1x + v_2y + v_3z)(w_1x + w_2y + w_3z) \\ &\equiv (v^TX)^T(w^TX) \\ &\equiv X^T(vw^T)X \pmod{p}. \end{aligned}$$

If we treat Q as a symmetric bilinear form, then for all X, X',

$$\begin{aligned} X^TQX' &\equiv ((X+X')^TQ(X+X') - X^TQX - X'^TQX')/2 \\ &\equiv (X^T(vw^T)X' + X'^T(vw^T)X)/2 \\ &\equiv X^T\left(\frac{vw^T + wv^T}{2}\right)X' \pmod{p}. \end{aligned}$$

Thus $Q \equiv \frac{vw^T+wv^T}{2} \pmod{p}$.

A solution to Q here satisfies either $v^TX \equiv 0$ or $w^TX \equiv 0$. It is easy to see that $v^TX \equiv 0$ has $p+1$ solutions in $\mathbb{P}^2_p$, which are simply lines orthogonal to v. Similarly, $w^TX \equiv 0$ has $p+1$ solutions.

If we further assume that v, w are independent, there exists exactly one line orthogonal to both v and w. Hence, the total count of solutions is $(p+1) + (p+1) - 1 = 2p+1$. From Theorem 3.12, it follows that the rank of Q must be 2.

If v and w are dependent, we can write $w = kv$, so $Q = \frac{1}{2}kvv^T$. Since the rowspace of $\frac{1}{2}kvv^T$ is spanned by $\{v\}$, its rank is 1, and there are $p+1$ solutions total.

4. Points on projective conics modulo n

Let a,b,c be nonzero integers such that $\gcd(a,b,c) = 1$ and n be a positive integer. In this section, we look at the solutions of the equation

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{n}. \tag{4.1}$$

Observe that Equation (4.1) is trivially satisfied by $(0,0,0)$. However, there may be other trivial solutions. For example, if $n = p^2$, where p is a prime, then (p,p,p) is a nonzero trivial solution of Equation (4.1). Somehow we need to disregard these trivial solutions. We realize that we must look at solutions (x,y,z) where x, y and z do not share a common factor with n. This motivates the following definition.

Definition 4.1. *Let n be a positive integer. We define the set A_n^3 of* primitive triples *modulo n as follows:*

$$\mathrm{A}_n^3 := (\mathbb{Z}/n\mathbb{Z})^3 - \bigcup_{\substack{d>1 \\ d \mid n}} d \cdot (\mathbb{Z}/n\mathbb{Z})^3.$$

A triple $(x, y, z) \in \mathbb{Z}^3$ gives a triple in $(\mathbb{Z}/n\mathbb{Z})^3$ if we interpret x, y, z modulo n. Also, observe that (x, y, z) represents a triple in A_n^3 if and only if $\gcd(x, y, z, n) = 1$.

Before we look at the solutions of Equation (4.1) in A_n^3, let us examine the structure of A_n^3 for different n. Let n_1 and n_2 be positive integers and set $n = n_1 n_2$. We can interpret an element of $\mathbb{Z}/n\mathbb{Z}$ as an element of $\mathbb{Z}/n_1\mathbb{Z}$. In other words, we have a natural surjection from $\mathbb{Z}/n\mathbb{Z}$ onto $\mathbb{Z}/n_1\mathbb{Z}$. It is clear that this surjection applied to each coordinate yields a surjection $\pi : \mathrm{A}_n^3 \to \mathrm{A}_{n_1}^3$.

Proposition 4.2. *Let n_1 and n_2 be relatively prime positive integers and set $n = n_1 n_2$. Let $\pi_i : \mathrm{A}_n^3 \to \mathrm{A}_{n_i}^3$ be the natural surjections for $i = 1, 2$. Then we have a bijection*

$$\pi_1 \times \pi_2 : \mathrm{A}_n^3 \to \mathrm{A}_{n_1}^3 \times \mathrm{A}_{n_2}^3 .$$

Proof. Given triples $(x_i, y_i, z_i) \in \mathrm{A}_{n_i}^3$ for $i = 1, 2$, there is a unique element $(x, y, z) \in \mathbb{Z}/n\mathbb{Z}$ such that $\pi_i(x, y, z) = (x_i, y_i, z_i)$ by the Chinese remainder theorem. Since (x_i, y_i, z_i) are primitive tuples modulo n_i for $i = 1, 2$, it is easy to see that (x, y, z) is a primitive triple modulo n. □

Note that if $(x, y, z) \in \mathrm{A}_n^3$ is a solution of Equation (4.1), then so is $(\lambda x, \lambda y, \lambda z)$ for any λ in $(\mathbb{Z}/n\mathbb{Z})^*$. Hence, it is reasonable to count the number of solutions of Equation (4.1) up to multiplication by a unit of $\mathbb{Z}/n\mathbb{Z}$. To make this idea precise, we define a relation $\sim$ on A_n^3 by letting $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ for all $\lambda \in (\mathbb{Z}/n\mathbb{Z})^*$. Clearly, $\sim$ is an equivalence relation.

Definition 4.3. *Let n be a positive integer. The set of equivalence classes of A_n^3 under $\sim$ is called the* projective plane *modulo n and is denoted by $\mathbb{P}_n^2$. For an element $(x, y, z) \in \mathrm{A}_n^3$, we denote its equivalence class in $\mathbb{P}_n^2$ by $\overline{(x, y, z)}$.*

Note that every triple in A_n^3 has $\phi(n)$ elements in its equivalence class. Therefore,

$$\phi(n) \cdot |\mathbb{P}_n^2| = |\mathrm{A}_n^3|.$$

Also, if n is prime then the new definition of the projective plane agrees with the previous definition.

Let n_1, n_2 be positive integers and set $n = n_1 n_2$. Recall that we have a surjection $\pi : \mathrm{A}^3_n \to \mathrm{A}^3_{n_1}$. Note that if two elements of A^3_n are equivalent, then so are their images. Hence the projection π gives a projection $\widetilde{\pi} : \mathbb{P}^2_n \to \mathbb{P}^2_{n_1}$. We have a result analogous to Proposition 4.2.

Proposition 4.4. *Let n_1 and n_2 be relatively prime positive integers and set $n = n_1 n_2$. Consider the projections $\widetilde{\pi}_i : \mathbb{P}^2_n \to \mathbb{P}^2_{n_i}$ for $i = 1, 2$. We have a bijection*

$$\widetilde{\pi}_1 \times \widetilde{\pi}_2 : \mathbb{P}^2_n \to \mathbb{P}^2_{n_1} \times \mathbb{P}^2_{n_2}.$$

Proof. By Proposition 4.2, we have a bijection

$$\pi_1 \times \pi_2 : \mathrm{A}^3_n \to \mathrm{A}^3_{n_1} \times \mathrm{A}^3_{n_2}.$$

Let X, Y be two triples in A^3_n. Observe that $X \sim Y$ in A^3_n if and only if $\pi_i(X) \sim \pi_i(Y)$ in $\mathrm{A}^3_{n_i}$ for $i = 1, 2$. Hence $\widetilde{\pi}_1 \times \widetilde{\pi}_2$ is a bijection. □

We now have the necessary setup to discuss the solutions of Equation (4.1). As the reader may have guessed, some aspects of the discussion are not limited to equations like Equation (4.1), but can be extended to any homogeneous equation. In particular, if Q is a homogeneous polynomial in three variables with integer coefficients and $(x, y, z) \in \mathrm{A}^3_n$ is a zero of Q modulo n, then all elements of A^3_n equivalent to (x, y, z) are also zeros of Q modulo n.

We introduce some notation that extends the notation of the previous section.

Definition 4.5. *Let Q be a homogeneous polynomial in three variables with integer coefficients and n a positive integer. Define*

$$\begin{aligned}
C_Q(n) &:= \{(x, y, z) \in \mathrm{A}^3_n \mid Q(x, y, z) \equiv 0 \pmod{n}\},\\
\widetilde{C}_Q(n) &:= \{\overline{(x, y, z)} \in \mathbb{P}^2_n \mid Q(x, y, z) \equiv 0 \pmod{n}\},\\
Z_Q(n) &:= |C_Q(n)|,\\
\widetilde{Z}_Q(n) &:= |\widetilde{C}_Q(n)|.
\end{aligned}$$

Let $P : \mathrm{A}^3_n \to \mathbb{P}^2_n$ be the map

$$P : (x, y, z) \mapsto \overline{(x, y, z)}.$$

We clearly have the following:

Proposition 4.6.

(1) $P^{-1}(\widetilde{C}_Q(n)) = C_Q(n)$,
(2) $Z_Q(n) = \phi(n) \cdot \widetilde{Z}_Q(n)$.

We can prove the analogue of Proposition 4.2 and Proposition 4.4 for the zero sets C_Q and $\widetilde{C}_Q$.

Proposition 4.7. *Let n_1 and n_2 be relatively prime positive integers and set $n = n_1 n_2$. Let $\pi_i : \mathrm{A}^3_n \to \mathrm{A}^3_{n_i}$ and $\widetilde{\pi}_i : \mathbb{P}^2_n \to \mathbb{P}^2_{n_i}$ be the natural projections for $i = 1, 2$. Then, we have the commutative diagram:*

$$\begin{array}{ccc} C_Q(n) & \xrightarrow{\pi_1 \times \pi_2} & C_Q(n_1) \times C_Q(n_2) \\ \downarrow & & \downarrow \\ \widetilde{C}_Q(n) & \xrightarrow{\widetilde{\pi}_1 \times \widetilde{\pi}_2} & \widetilde{C}_Q(n_1) \times \widetilde{C}_Q(n_2) \end{array},$$

where the maps $\pi_1 \times \pi_2$ and $\widetilde{\pi}_1 \times \widetilde{\pi}_2$ are bijective.

Proof. We know that we have a commutative diagram

$$\begin{array}{ccc} \mathrm{A}^3_n & \xrightarrow{\pi_1 \times \pi_2} & \mathrm{A}^3_{n_1} \times \mathrm{A}^3_{n_2} \\ \downarrow & & \downarrow \\ \mathbb{P}^2_n & \xrightarrow{\widetilde{\pi}_1 \times \widetilde{\pi}_2} & \mathbb{P}^2_{n_1} \times \mathbb{P}^2_{n_2} \end{array},$$

where $\pi_1 \times \pi_2$ and $\widetilde{\pi}_1 \times \widetilde{\pi}_2$ are bijections. Since $\gcd(n_1, n_2) = 1$, we have $Q(x, y, z) \equiv 0 \pmod{n}$ if and only if $Q(x, y, z) \equiv 0 \pmod{n_i}$ for $i = 1, 2$. Hence we get a bijection

$$\pi_1 \times \pi_2 : C_Q(n) \to C_Q(n_1) \times C_Q(n_2).$$

This, along with Proposition 4.6 implies that $\widetilde{\pi}_1 \times \widetilde{\pi}_2$ gives a bijection

$$\widetilde{\pi}_1 \times \widetilde{\pi}_2 : \mathbb{P}^2_n \to \mathbb{P}^2_{n_1} \times \mathbb{P}^2_{n_2}.$$

□

As a direct corollary, we have the following:

Proposition 4.8. *Let n_1 and n_2 be relatively prime positive integers. Then,*

(1) $Z_Q(n_1 n_2) = Z_Q(n_1) Z_Q(n_2)$,

(2) $\widetilde{Z}_Q(n_1 n_2) = \widetilde{Z}_Q(n_1) \widetilde{Z}_Q(n_2)$.

For the rest of the section, we fix Q to be the quadratic form given by

$$Q(x, y, z) = ax^2 + by^2 + cz^2,$$

where a, b, c are nonzero integers such that $\gcd(a, b, c) = 1$. Recall that we are interested in the numbers $\widetilde{Z}_Q(n)$. Thanks to Proposition 4.8, we can compute the numbers $\widetilde{Z}_Q$ if we know them for powers of primes. In

other words, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where p_i are distinct primes and $\alpha_i > 0$, then

$$\widetilde{Z}_Q(n) = \widetilde{Z}_Q(p_1^{\alpha_1}) \cdots \widetilde{Z}_Q(p_k^{\alpha_k}).$$

Table 4 shows the values $\widetilde{Z}_Q$ for some forms Q and the first 8 powers of 3.

	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8
$x^2+y^2+z^2$	4	12	36	108	324	972	2916	8748
$x^2+2y^2-z^2$	4	12	36	108	324	972	2916	8748
$x^2+y^2-81z^2$	1	9	9	81	324	972	2916	8748
$27x^2+8y^2-5z^2$	7	27	99	270	810	2430	7290	21870

TABLE 4. $\widetilde{Z}_Q(3^k)$ for some Q.

The integer 2 often behaves differently in situations involving quadratic equations. Table 5 shows the values $\widetilde{Z}_Q$ for some forms Q and the first 8 powers of 2.

	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
$x^2+y^2+z^2$	3	0	0	0	0	0	0	0
$x^2+2y^2-z^2$	3	4	16	32	64	128	256	512
$x^2+y^2-81z^2$	3	8	16	32	64	128	256	512
$27x^2+8y^2-5z^2$	3	4	8	16	64	128	256	512

TABLE 5. $\widetilde{Z}_Q(2^k)$ for some Q and k

Observe in Table 4 and Table 5 that the numbers $\widetilde{Z}_Q(p^k)$ for $k = 1, 2, \ldots$ eventually form a geometric series with ratio p. This is not an accident.

Theorem 4.9. *Let p be a prime and $Q(x,y,z) = ax^2+by^2+cz^2$, where a, b, c are nonzero positive integers. Let N be a positive integer such that p^{N+1} does not divide any of a, b or c. Let $N_0 = N+1$ if p is odd and $N_0 = N+3$ if $p = 2$. Then, for $n \geq N_0$ we have*

$$\widetilde{Z}_Q(p^{n+1}) = p \cdot \widetilde{Z}_Q(p^n).$$

Proof. Since we know that $Z_Q(p^t) = \phi(p^t)\widetilde{Z}_Q(p^t)$ (Proposition 4.6) and $\phi(p^t) = p^{t-1}(p-1)$, we may prove $Z_Q(p^{n+1}) = p^2 Z_Q(p^n)$.

Recall that interpreting elements of $\mathbb{Z}/p^{n+1}\mathbb{Z}$ modulo p^n gives us a surjection $\pi : C_Q(p^{n+1}) \to C_Q(p^n)$. Let p^α, p^β and p^γ be the highest powers of p dividing $2a$, $2b$ and $2c$ respectively. For $(x,y,z) \in C_Q(p^n)$ such that $p \nmid x$, define

$$A_1(x,y,z) := \{(x + ip^{n-\alpha}, y, z) \mid 0 \leq i \leq p^\alpha - 1\}.$$

Notice that $|A_1(x,y,z)| = p^\alpha$. It is easy to prove that for $n \geq N_0$, we have

$$a(x + ip^{n-\alpha})^2 \equiv ax^2 \pmod{p^n}.$$

Therefore, we see that $A(x,y,z) \subset C_Q(p^n)$. Similarly, for an element $(x,y,z) \in C_Q(p^n)$ such that $p \nmid y$, we define

$$A_2(x,y,z) := \{(x, y + jp^{n-\beta}, z) \mid 0 \leq j \leq p^\beta - 1\},$$

and for $(x,y,z) \in C_Q(p^n)$ such that $p \nmid z$,

$$A_3(x,y,z) := \{(x, y, z + kp^{n-\gamma}) \mid 0 \leq n \leq p^\gamma - 1\}.$$

See that all $A_i(x,y,z)$ are subsets of $C_Q(p^n)$. Also, if $A_i(x_1,y_1,z_1)$ and $A_i(x_2,y_2,z_2)$ have an element in common, then $A_i(x_1,y_1,z_1) = A_i(x_2,y_2,z_2)$. Also, if (x,y,z) is an element of $C_Q(p^n)$, then at least one of x, y or z is not divisible by p, because (x,y,z) is a primitive triple. Thus, we see that we can write $C_Q(p^n)$ as a disjoint union of sets S_r, where each S_r has the form $A_i(x,y,z)$ for some $i \in \{1,2,3\}$ and $(x,y,z) \in C_Q(p^n)$. As a consequence, the proposition is proved if we prove that the number of elements in the preimage of $A_i(x,y,z)$ in $C_Q(p^{n+1})$ is $p^2|A_i(x,y,z)|$. Without loss of generality, we may prove this assertion for $A_1(x,y,z)$.

Choose integers x,y,z such that $p \nmid x$ and $(x,y,z) \in C_Q(p^n)$. Elements in $\mathrm{A}^3_{p^{n+1}}$ that map into $A_1(x,y,z)$ under π have the form $(x + ip^{n-\alpha}, y + jp^n, z + kp^n)$, where $0 \leq i \leq p^{\alpha+1} - 1$, $0 \leq j \leq p-1$ and $0 \leq k \leq p-1$. However, $(x + ip^{n-\alpha}, y + jp^n, z + kp^n)$ lies in $C_Q(p^{n+1})$ if and only if

$$a(x + ip^{n-\alpha})^2 + b(y + jp^n)^2 + c(z + kp^n)^2 \equiv 0 \pmod{p^{n+1}}. \tag{4.2}$$

Set $D := Q(x,y,z)/p^n$, which is an integer since $(x,y,z) \in C_Q(p^n)$. Set $a' = 2ax/p^\alpha$, $b' = 2by$ and $c' = 2cz$. Note that a' is an integer not divisible by p by our choice of α. Since $n \geq N_0$, the terms $ai^2p^{2(n-\alpha)}$, bj^2p^{2n} and ck^2p^{2n} are all divisible by p^{n+1}. Hence, Equation (4.2) is equivalent to

$$D + ia' + jb' + kc' \equiv 0 \pmod{p}. \tag{4.3}$$

Recall that $0 \leq i \leq p^{\alpha+1} - 1$ and $0 \leq j,k \leq p-1$. Since $\gcd(p,a') = 1$, we see that we can choose i in p^α ways for every choice of j and k. Therefore, $A_i(x,y,z)$ has $p^{\alpha+2}$ preimages in $C_Q(p^{n+1})$. Recall that $|A_i(x,y,z)| = p^\alpha$, and hence the proof is complete. □

Theorem 4.10 and Theorem 3.12 give us an explicit formula for $\widetilde{Z}_Q(p^n)$ if p is an odd prime and Q is nondegenerate modulo p.

Theorem 4.10. *Let p be an odd prime and $Q(x,y,z) = ax^2+by^2+cz^2$ be such that $p \nmid abc$. Then, $\widetilde{Z}_Q(p^n) = p^{n-1}(p+1)$.*

Proof. If $p \nmid abc$, then we may take $N = 0$ in the statement of Theorem 4.9. Then we have,

$$\widetilde{Z}_Q(p^n) = p^{n-1}\widetilde{Z}_Q(p).$$

Since none of a, b, c is divisible by p, we conclude from Theorem 3.12 that $\widetilde{Z}_Q(p) = p+1$. □

In particular, note that if Q is nondegenerate modulo p, then it has zeros modulo p^k for all $k \in \mathbb{N}$.

The number 2 behaves a bit differently. We have the following result.

Theorem 4.11. *Let $Q(x,y,z) = ax^2 + by^2 + cz^2$ be a quadratic form where a, b, c are odd integers. Then $\widetilde{Z}_Q(2^n) = 2^{n-3}\widetilde{Z}_Q(8)$ for $n \geq 3$.*

Proof. This follows from Theorem 4.9 since we can take $N = 1$. □

In particular, note that if Q is nondegenerate modulo 2, then it has zeros modulo 2^k for all $k \in \mathbb{N}$ if it has zeros modulo 8.

5. Integer points on projective conics

Let $a, b, c \in \mathbb{Z}$ be nonzero integers such that $\gcd(a,b,c) = 1$. Define a quadratic form Q by

$$Q(x,y,z) = ax^2 + by^2 + cz^2.$$

In the previous sections, we looked at the zeros of Q modulo n for different positive integers n. In this section, we see if zeros of Q modulo n for all positive integers n give any information about the integer zeros of Q.

Let $(x,y,z) \in \mathbb{Z}^3$ be such that $Q(x,y,z) = 0$ but $(x,y,z) \neq (0,0,0)$. Since Q is homogeneous, we can assume that $\gcd(x,y,z) = 1$. See that (x,y,z) gives us a zero of Q modulo n, for all positive integers n. In other words, $\overline{(x,y,z)}$ is an element of $\widetilde{C}_Q(n)$ for all positive integers n. Furthermore, (x,y,z) is also a real zero of Q. Hence, if Q has a nontrivial integer zero, then it must have a nontrivial zero modulo n for all n and also have a nontrivial real zero. One can ask if having a nontrivial real zero and a nontrivial zero modulo n for all n is sufficient to guarantee a nontrivial integer zero of Q. The celebrated Hasse–Minkowski theorem asserts that this is indeed the case.

Theorem 5.1 (Hasse–Minkowski)**.** [1, p.2] [1] *Let $Q(x, y, z) = ax^2 + by^2 + cz^2$, where a,b,c are nonzero integers. Then Q has a nontrivial zero in $\mathbb{Z}^3$ if and only if it has a nontrivial zero in $\mathbb{R}^3$ and a zero in $\mathbb{P}^2_n$ for all positive integers n.*

In fact, it turns out that the statement is true even if we drop the hypothesis of Q having real zeros ([2, Ch IV, §4, Corollary 3]). In other words, we have the following:

Theorem 5.2. *Q has a nontrivial zero in $\mathbb{Z}^3$ if and only if it has a zero in $\mathbb{P}^2_n$ for all positive integers n.*

By Proposition 4.8, we see that Q has zeros in $\mathbb{P}^2_n$ for all positive integers n if and only if it has zeros in $\mathbb{P}^2_{p^k}$ for all primes p and positive integers k. Theorem 3.12 shows that Q has zeros in $\mathbb{P}^2_p$ for all primes p. The two examples show that given an odd prime p and $k \geq 2$, we can construct a form Q that has zeros in $\mathbb{P}^2_{p^n}$ for $n < k$ but fails to have a zero in $\mathbb{P}^2_{p^k}$.

Example 5.3. Let $k \geq 2$ be even and p an odd prime. Choose $\alpha \in \mathbb{Z}$ such that α is a quadratic nonresidue modulo p. Consider the form

$$Q(x, y, z) = x^2 - \alpha y^2 - p^{k-1} z^2.$$

Clearly $(0, 0, 1)$ gives a primitive zero of Q in $\mathbb{P}^2_{p^n}$ for $n < k$. We claim that Q has no zero in $\mathbb{P}^2_{p^k}$.

Let $x, y, z \in \mathbb{Z}$ be such that $Q(x, y, z) \equiv 0 \pmod{p^k}$. Let p^u be the highest power of p dividing $x^2 - \alpha y^2$, and p^v the highest power of p dividing $p^{k-1} z^2$. Since α is a nonresidue modulo p, it follows that u is even. On the other hand, v is odd since $k - 1$ is odd. Therefore, for $Q(x, y, z) \equiv 0 \pmod{p^k}$, we must have $u \geq k$ and $v \geq k$. Hence p divides z and $x^2 - \alpha y^2$. Again, since α is a nonresidue, p divides x and y. Thus, (x, y, z) is not a primitive triple modulo p. It follows that Q has no zeros in $\mathbb{P}^2_{p^k}$.

Example 5.4. Let $k > 2$ be odd and p be an odd prime. Choose $\alpha \in \mathbb{Z}$ such that α is a nonresidue modulo p, as before. Consider the form

$$Q(x, y, z) = x^2 - p^{k-2} y^2 - \alpha p^{k-1} z^2.$$

Again, $(0, 0, 1)$ gives a zero of Q in $\mathbb{P}^2_{p^n}$ for $n < k$. We show that Q has no zero in $\mathbb{P}^2_{p^k}$.

[1] This is not the most common way to formulate the theorem. It is best phrased in terms of p-adic numbers. See [2, Ch IV, §3].

Let $x, y, z \in \mathbb{Z}$ be such that $Q(x, y, z) \equiv 0 \pmod{p^k}$. It follows that $p^{k-2} \mid x^2$. Since $k-2$ is odd, we see that $p^{k-1} \mid x^2$. This, in turn, implies that $p \mid y^2$, and hence $p^2 \mid y^2$. Thus, we have

$$Q(x, y, z) \equiv x^2 - \alpha p^{k-1} z^2 \equiv 0 \pmod{p^k}.$$

Letting $x^2 = p^{k-1} x_1^2$, we get

$$x_1^2 - \alpha z^2 \equiv 0 \pmod{p}.$$

Since α is a nonresidue, we see that $p \mid z$ and $p \mid x_1$. Thus, p divides x,y and z, which shows that (x, y, z) is not a primitive triple. It follows that Q has no zeros in $\mathbb{P}^2_{p^k}$.

Finally, the next example shows that given any $k \geq 2$, we can find an odd prime p and a form Q that satisfies the following:

(1) Q has zeros in $\mathbb{P}^2_{q^n}$ for all primes $q \neq p$ and all $n \in \mathbb{N}$.
(2) Q has zeros in $\mathbb{P}^2_{p^n}$ for all $n < k$,
(3) Q does not have a zero in $\mathbb{P}^2_{p^k}$.

Example 5.5. Let $k \geq 2$ and p be a prime congruent to 7 modulo 8. Consider the form

$$Q(x, y, z) = x^2 + p^{k-2} y^2 + p^{k-1} z^2.$$

Note that if k is even, then $(1, 0, 1)$ gives a zero of Q in $\mathbb{P}^2_8$. If k is odd, then $(1, 1, 0)$ gives a zero of Q in $\mathbb{P}^2_8$. By Theorem 4.11, we conclude that Q has zeros in $\mathbb{P}^2_{2^n}$ for all $n \in \mathbb{N}$.

Next, Q is nondegenerate modulo all primes $q \neq p$. By Theorem 4.10, we see that Q has zeros in $\mathbb{P}^2_{q^n}$ for all odd primes $q \neq p$ and $n \in \mathbb{N}$.

Clearly, $(0, 0, 1)$ gives a zero of Q in $\mathbb{P}^2_{p^n}$ for $n < k$. We claim that Q has no zero in $\mathbb{P}^2_{p^k}$. Let $x, y, z \in \mathbb{Z}$ be such that $Q(x, y, z) \equiv 0 \pmod{p^k}$. We see that $p^{k-1} \mid x^2 + p^{k-2} y^2$ and $p^{k-2} \mid x^2$. We have two cases:

Case (1) k is odd.

In this case, $k - 2 > 0$ is odd. Since $p^{k-2} \mid x^2$, we conclude that $p^{k-1} \mid x^2$, and hence $p \mid y$. Thus, we get $p^2 \mid y$, and hence $Q(x, y, z) \equiv x^2 + p^{k-1} z^2 \pmod{p^k}$. Letting $x^2 = p^{k-1} x_1^2$, we see that we have

$$x_1^2 + z^2 \equiv 0 \pmod{p}.$$

Since $p \equiv 3 \pmod{4}$, we see that $p \mid z$ and $p \mid x_1$. In particular, p divides x, y and z. Hence (x, y, z) is not a primitive triple.

Case (2) k is even.

Writing $x^2 = p^{k-2}x_1^2$, the equation $Q(x, y, z) \equiv 0 \pmod{p^k}$ gives

$$x_1^2 + y^2 + pz^2 \equiv 0 \pmod{p^2}.$$

In particular, $p \mid x_1^2 + y^2$. Since $p \equiv 3 \pmod 4$, we see that $p \mid x_1$ and $p \mid y$. Thus, $p^2 \mid x_1^2 + y^2$, which implies that $p \mid z$. Hence, p divides x, y and z. Hence (x, y, z) is not a primitive triple.

In any case, we see that we do not get a zero of Q in $\mathbb{P}^2_{p^k}$.

Appendix A. Equivalence of Symmetric Matrices mod p

Let p be a prime, and denote by $\mathcal{S}_p$ the set of n-by-n symmetric matrices over $\mathbb{F}_p$. Consider the operation on $\mathcal{S}_p$ that takes $M \in \mathcal{S}_p$ to $A^T M A$, where A is an n-by-n invertible matrix.

The operation gives rise to a natural relation $\sim$ over $\mathcal{S}_p$: for all $M_1, M_2 \in \mathcal{S}_p$, where the relation $M_1 \sim M_2$ holds if and only if there exists an invertible matrix A such that $M_1 \equiv A^T M_2 A \pmod p$. We note that $\sim$ is in fact an equivalence relation—it is reflexive, symmetric and transitive.

We show in the theorem below that a symmetric matrix modulo p must be similar to a diagonal matrix:

Theorem A.1. *For any $M \in \mathcal{S}_p$, there exists a diagonal matrix D and an invertible matrix $A \in GL_n(p)$ such that*

$$D \equiv A^T M A \pmod p$$

Proof. We will explicitly consturct a diagonal matrix D satisfying the theorem.

Consider M as a bilinear form. We begin by inductively showing that for each positive integer $k \leq n$, there exists a linearly independent set of vectors $\{v_1^*, \ldots, v_k^*\}$ such that

$$\forall i \neq j \in \{1, \ldots, k\}, \qquad (v_i^*)^T M (v_j^*) \equiv 0 \pmod p. \tag{A.1}$$

For $k = 1$, the condition in (A.1) is vacuous, so we can pick an arbitrary vector v_1^*. For the inductive case, assume that we already have a linearly independent set of vectors $\{v_1^*, \ldots, v_k^*\}$ satisfying (A.1). By extending the set as a basis, pick a vector v_{k+1} such that $v_1^*, \ldots, v_k^*, v_{k+1}$ are linearly independent. Then we let

$$v_{k+1}^* \equiv v_{k+1} - \sum_{i=1}^{k} v_i^* \frac{(v_i^*)^T M (v_{k+1})}{(v_i^*)^T M (v_i^*)} \pmod p.$$

First, for all $j \neq k+1$, we see that

$$\begin{aligned}(v_j^*)^T M(v_{k+1}^*) &\equiv (v_j^*)^T M(v_{k+1}) - \sum_{i=1}^{k} (v_j^*)^T M(v_i^*) \frac{(v_i^*)^T M(v_{k+1})}{(v_i^*)^T M(v_i^*)} \\ &\equiv (v_j^*)^T M(v_{k+1}) - (v_j^*)^T M(v_j^*) \frac{(v_j^*)^T M(v_{k+1})}{(v_j^*)^T M(v_j^*)} \\ &\equiv 0 \pmod{p},\end{aligned}$$

as desired. By symmetry of M, we also obtain $(v_{k+1}^*)^T M(v_j^*) \equiv 0 \pmod{p}$. Therefore, (A.1) still holds. In addition, we see that the vectors $v_1^*, \ldots, v_{k+1}^*$ are linearly independent, so the inductive hypothesis is satisfied.

The induction above yields a basis $\{v_1^*, \ldots, v_n^*\}$ satisfying (A.1). Now let A be the matrix formed by taking $v_1^*, \ldots, v_n^*$ as column vectors. A is nonsingular because the columns are linearly independent.

Pick $D = A^T M A \pmod{p}$. Note that the desired condition in the theorem is trivially satisfied. It remains to check that D is diagonal. From our choice of A, we see that $D_{ij} = (v_i^*)^T M(v_j^*)$, which is zero when $i \neq j$. Thus we have successfully shown that M is similar to a diagonal matrix. □

Appendix B. Quadratic residues

Quadratic residues are useful in treatments of quadratic equations modulo p, where p is a prime.

Definition B.1. *A number $q \in \mathbb{Z}/p\mathbb{Z}$ is called a* quadratic residue modulo p *(or* residue *for short) if there exists $x \not\equiv 0 \pmod{p}$ such that*

$$x^2 \equiv q \pmod{p}.$$

Zero is never a quadratic residue, since $x^2 \equiv 0$ implies $x \equiv 0$. It is also easy to see that there are exactly $(p-1)/2$ residues.

The condition of a number being a quadratic residue is called the *quadratic residuosity*, and is expressed commonly by the Legendre symbol:

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{if } a \equiv 0 \pmod{p}, \\ +1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{otherwise.} \end{cases}$$

An important property of Legendre symbols is that they are multiplicative, given a fixed prime p:

Proposition B.2. *For all $a, b \in \mathbb{Z}/p\mathbb{Z}$,*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right). \tag{B.1}$$

Proof. If a or b is zero, then both $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ and $\left(\frac{ab}{p}\right)$ are zero, so (B.1) is satisfied. So we may restrict our attention to cases where $a, b \not\equiv 0 \pmod{p}$.

If a and b are both residues, then there exist $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ such that $\alpha^2 = a$ and $\beta^2 = b$. Then ab is also a residue because $(\alpha\beta)^2 = ab$. Then both sides of (B.1) is 1, so it is satisfied.

If a is a residue with $\alpha^2 = a$ and b is not, then it cannot be that ab is a residue. Suppose the contrary, i.e. there exists $\delta \in \mathbb{Z}/p\mathbb{Z}$ such that $\delta^2 = ab$. Then $b = \left(\frac{\delta}{\alpha}\right)^2$, which contradicts the assumption. The same holds when a is not a residue and b is. In either case, both sides of (B.1) is -1.

The only remaining case is when a, b are both nonresidues. We can use the following counting argument: as a, b vary in $\{1, \ldots, p-1\}$ each, the product ab takes each value in $\{1, \ldots, p-1\}$ exactly $p-1$ times. Since half of $\{1, \ldots, p-1\}$ are residues, ab is a residue for exactly $(p-1)^2/2$ pairs of values of (a, b). We have already accounted for $(p-1)^2/4$ pairs where both a, b are residues. The remaining $(p-1)^2/4$ pairs then must come from pairs where both a, b are nonresidues. But there are exactly $(p-1)^2/4$ such pairs, so it must be the product of two nonresidue is always a residue, satisfying (B.1).

We have examined all possible cases for quadratic residuosity of a and b, and in all cases, (B.1) holds. □

Appendix C. Primary Authors

Section 2 was primarily authored by Katherine Redfield; Section 3 and the appendices (Section A and B) were primarily authored by Jongmin Baek; Section 1, Sections 4 and Section 5 were primarily authored by Anand Deopurkar.

References

[1] W. Aitken, F. Lemmermeyer: "Counterexamples to the Hasse Principle: An Elementary Introduction", `http://public.csusm.edu/aitken_html/m372/diophantine.pdf`

[2] J.-P. Serre: "A Course in Arithmetic", Springer-Verlag New York, 1973