TWO COMBINATORIAL GEOMETRIC PROBLEMS INVOLVING MODULAR HYPERBOLAS

Mizan R. Khan
Department of Mathematics and Computer Science, Eastern Connecticut State University, Willimantic, Connecticut
khanm@easternct.edu

Richard Magner[1]
Department of Mathematics and Computer Science, Eastern Connecticut State University, Willimantic, Connecticut
magnerri@my.easternct.edu

Steven Senger
Department of Mathematical Sciences, University of Delaware, Newark, Delaware
senger@math.udel.edu

Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria
arne.winterhof@oeaw.ac.at

Received: 6/25/13, Revised: 3/29/14, Accepted: 4/19/14, Published: 7/10/14

Abstract

For integers a and $n \geq 2$ with $\gcd(a,n) = 1$ let $\overline{\mathcal{H}}_{a,n}$ be the set of least residues of a modular hyperbola $\overline{\mathcal{H}}_{a,n} = \{(x,y) \in \mathbb{Z}^2 \, : \, xy \equiv a \pmod{n}, 1 \leq x,y \leq n-1\}$. In this paper we prove two combinatorial geometric results about $\overline{\mathcal{H}}_{a,p^m}$, where p^m is a prime power. Our first result shows that the number of ordinary lines spanned by $\overline{\mathcal{H}}_{1,p^m}$ is at least

$$(p-1)p^{m-1}\left(\frac{p^{m-1}(p-2)}{2} + c(p^m)\right),$$

where

(i) $c(p) = 0$, $c(4) = 1/2$, $c(8) = 0$, $c(49) = 6/7$;

(ii) $c(p^m) = 6/13$ if $m \geq 2$, p^m is small and $p^m \neq 4, 8, 49$;

(iii) $c(2^m) = 1/2$ if m is sufficiently large;

(iv) $c(p^m) = 3/4 + o(1)$ if $p > 2$, $m \geq 2$ and p^m is sufficiently large.

In the special case of $m = 1$ we have equality. The second result gives a partial answer to a question of Shparlinskion the cardinality of

$$\mathcal{F}_{a,n} = \{\sqrt{x^2+y^2} \, : \, (x,y) \in \overline{\mathcal{H}}_{a,n}\}.$$

[1]The second author was supported by an Eastern summer undergraduate research fellowship.

1. Introduction

For $n \geq 2$ let $\mathbb{Z}_n^*$ be the group of invertible elements modulo n and let $\mathcal{H}_{a,n}$ denote the *modular hyperbola* $xy \equiv a \pmod{n}$ where $x, y, a \in \mathbb{Z}$, with $\gcd(a, n) = 1$. (We insert the condition that a and n are relatively prime to ensure that $\mathcal{H}_{a,n} \subseteq \mathbb{Z}_n^* \times \mathbb{Z}_n^*$.) Following [6] we define $\overline{\mathcal{H}}_{a,n} = \mathcal{H}_{a,n} \cap [1, n-1]^2$, that is,

$$\overline{\mathcal{H}}_{a,n} = \{(x, y) \in \mathbb{Z}^2 \, : \, xy \equiv a \pmod{n}, 1 \leq x, y \leq n-1\}.$$

In the special case of $\overline{\mathcal{H}}_{1,n}$ we will simply drop the 1 and write $\overline{\mathcal{H}}_n$.

Given the simplicity of the congruence that defines a modular hyperbola and given the rich history of polynomial congruences, the reader may well feel that there is little or nothing left to say about this curve. But this is not the case. We refer the interested reader to the survey paper on modular hyperbolas by Shparlinski [6]. Shparlinski makes the following statement in the introduction — *our main goal is to show that although $\mathcal{H}_{a,m}$ is defined by one of the simplest possible polynomial congruences, it exhibits many mysterious properties and very surprising links with a wide variety of classical number theoretic questions and beyond.*

In this paper we answer two combinatorial geometric questions about modular hyperbolas. The first is to give a lower bound for the number of *ordinary lines* spanned by a modular hyperbola. The second is to give an estimate for the number of distinct distances of the points on a modular hyperbola to the origin. When the modulus is prime both questions have solutions that are *short and sweet*! But this does not extend to the composite case.

Let S be a finite set of points in the Euclidean space. A line that passes through exactly two distinct points of S is said to be an *ordinary line* spanned by S. The notion of an ordinary line arose in the context of the famous *Sylvester-Gallai* theorem in combinatorial geometry.

Theorem 1 (Sylvester-Gallai). *Let P be a finite set of points in the plane, not all on a line. Then there is an ordinary line spanned by P.*

We refer the reader to [4] and the references therein for an exposition of the history of this theorem and subsequent developments. We now give an application of the Sylvester-Gallai theorem to modular hyperbolas.

Lemma 2. *The only moduli for which the modular hyperbolas $\overline{\mathcal{H}}_n$ do* not *span an ordinary line are $n = 2, 8, 12$ and 24.*

Proof. We may assume that $n \neq 2, 3, 4, 6$, since for $n = 2$ the modular hyperbola consists of only one point, and in the case of $n = 3, 4$ or 6 the modular hyperbola consists of only two points. So for these 3 cases we have precisely one ordinary line.

The points $(1, 1)$ and $(n-1, n-1)$ are two distinct points of $\overline{\mathcal{H}}_n$, and consequently $\overline{\mathcal{H}}_n$ spans the line $y = x$. We now observe that the number of solutions of the

congruence $z^2 \equiv 1 \pmod{n}$ equals $\varphi(n)$ precisely when $n = 2, 3, 4, 6, 8, 12$ and 24. For all other values of n there exists $z \in \mathbb{Z}_n^*$ such that $z^2 \not\equiv 1 \pmod{n}$. Such a z gives a point in $\overline{\mathcal{H}}_n$ that does not lie on $y = x$. We now invoke the Sylvester-Gallai theorem to conclude our proof. □

For prime moduli it is easy to determine the precise number of ordinary lines.

Lemma 3. *Let p be a prime. Then the set $\overline{\mathcal{H}}_{a,p}$ spans $(p-1)(p-2)/2$ ordinary lines.*

Proof. We show that any line connecting 2 distinct points of $\overline{\mathcal{H}}_{a,p}$ is ordinary. Let $(x_1, y_1), (x_2, y_2)$ be two distinct points in $\overline{\mathcal{H}}_{a,p}$, and let $y = kx + d$ be the line in $\mathbb{R}^2$ passing through these two points. Since $x_1 \neq x_2$, x_1 and x_2 are distinct roots modulo p of the quadratic polynomial $kx^2 + dx - a$. By Lagrange's theorem $kx^2 + dx - a$ has no more than 2 roots modulo p. Hence, no other point of $\overline{\mathcal{H}}_{a,p}$ lies on $y = kx + d$. Since $\#\overline{\mathcal{H}}_{a,p} = p - 1$, $\overline{\mathcal{H}}_{a,p}$ spans $\binom{p-1}{2}$ ordinary lines. □

In Section 2 we determine a lower bound for the number of ordinary lines spanned by $\overline{\mathcal{H}}_{p^m}$ when $m \geq 2$ (see Theorem 6).

We now describe the second problem we study in this paper. Shparlinski in Section 4 of his survey paper [6] describes some geometric properties of $\mathcal{H}_{a,n}$. In Question 25 he asks for an estimate of the quantity $\#\mathcal{F}_{a,n}$, where $\mathcal{F}_{a,n}$ denotes the set of Euclidean distances from the origin to points on $\overline{\mathcal{H}}_{a,n}$, that is,

$$\mathcal{F}_{a,n} = \{\sqrt{x^2 + y^2} \,:\, (x, y) \in \overline{\mathcal{H}}_{a,n}\}.$$

We remark that a natural family of questions about finite point sets involves the various sets of distances they can determine. See for example [2]. Shparlinski's Question 25 is in this vein. Further motivation was provided by the following observation the fourth author (AW) had previously brought to Shparlinski's attention.

Lemma 4. *We have*

$$\#\mathcal{F}_{a,p} = \frac{1}{2}\left(p + \left(\frac{a}{p}\right)\right) \quad p > 2,$$

where p is prime, $\gcd(a, p) = 1$, and $(\cdot/p)$ is the Legendre symbol.

Proof. Let $(x, y) \in C \cap \overline{\mathcal{H}}_{a,p}$ where C is the circle with center the origin and radius $\sqrt{u}$. Since p is prime, the congruence $f(Z) = Z^4 - uZ^2 + a^2 \equiv 0 \pmod{p}$ has at most 4 roots and consequently $\#(C \cap \overline{\mathcal{H}}_{a,p}) \leq 4$. There are now 3 cases to consider.

1. $y \neq x, p - x$: We have the factorization

$$f(Z) \equiv (Z - x)(Z + x)(Z - y)(Z + y) \pmod{p}.$$

Since $x^2 + y^2 \neq (p - x)^2 + (p - y)^2$, $C \cap \overline{\mathcal{H}}_{a,p} = \{(x, y), (y, x)\}$.

2. $y = p - x$: We now have the factorization $f(Z) \equiv (Z-x)^2(Z+x)^2 \pmod{p}$, from which we conclude that $C \cap \overline{\mathcal{H}}_{a,p} = \{(x, p-x), (p-x, x)\}$.

3. $y = x$: We again have the factorization $f(Z) \equiv (Z-x)^2(Z+x)^2 \pmod{p}$. Since $x \neq (p-x)$, $C \cap \overline{\mathcal{H}}_{a,p} = \{(x, x)\}$.

On putting these 3 pieces together we obtain our conclusion. □

In Section 3 we answer Shparlinski's question for the case $n = p^2$ (see Theorem 15). Whilst the solution is an extension of the above proof, the details are more intricate. The reason for this is that unlike the prime case it is possible for a circle, centered at the origin, to intersect $\overline{\mathcal{H}}_{a,p^2}$ at more than 2 points. For example, for each prime $p \geq 5$, there is a circle, centered at the origin, that intersects $\overline{\mathcal{H}}_{p^2}$ at 4 points (see Corollary 18).

2. Ordinary lines in $\overline{\mathcal{H}}_{p^m}$, $m \geq 2$

In this section we focus on the case $a = 1$. We begin by observing that for prime powers p^m, with $m \geq 2$ (and $p^m \neq 4, 9$), $\overline{\mathcal{H}}_{p^m}$ spans lines that are not ordinary. In particular we have the following example.

Lemma 5. *Let p be a prime and let $m \in \mathbb{Z}$ with $m \geq 2$ and $p^m > 8$. Then $\overline{\mathcal{H}}_{p^m}$ spans a line with $\left(p^{\lfloor m/2 \rfloor} - 1\right)$ points.*

Proof. We include the hypothesis $p^m > 8$ to ensure that

$$\left(p^{\lfloor m/2 \rfloor} - 1\right) \geq 2.$$

Let l be the line $L : x + y = p^m + 2$. We will show that

$$\#\left(\overline{\mathcal{H}}_{p^m} \cap L\right) = p^{\lfloor m/2 \rfloor} - 1.$$

The lattice points on the line L that lie inside the first quadrant are of the form $(k, p^m + 2 - k)$ with $k = 1, 2, \ldots, p^m, p^m + 1$. If $(k, p^m + 2 - k) \in \overline{\mathcal{H}}_{p^m}$, then

$$k(2-k) \equiv 1 \pmod{p^m},$$

that is,

$$(k-1)^2 \equiv 0 \pmod{p^m}.$$

Therefore,

$$k - 1 = lp^{\lceil m/2 \rceil}$$

with $l = 1, 2, \ldots, \left(p^{\lfloor m/2 \rfloor} - 1\right)$. □

Since $\left(3^{\lfloor 3/2 \rfloor}-1\right)=2$, the above proof does not show that there are non-ordinary lines for the case $p^m=27$. For this case we note that the line $x+y=38$ contains 4 points of $\overline{\mathcal{H}}_{27}$. We now state the main result of this section.

Theorem 6. *Let p^m be a prime power and N the number of ordinary lines that $\overline{\mathcal{H}}_{p^m}$ spans. Then*

$$N \geq p^{m-1}(p-1)\left(\frac{p^{m-1}(p-2)}{2}+c(p^m)\right), \tag{1}$$

where

(i) $c(p)=0$, $c(4)=1/2$, $c(8)=0$, $c(49)=6/7$;

(ii) $c(p^m)=6/13$ *if* $m\geq 2$, p^m *is small and* $p^m \neq 4,8,49$;

(iii) $c(2^m)=1/2$ *if* m *is sufficiently large;*

(iv) $c(p^m)=3/4+o(1)$ *if* $p>2$, $m\geq 2$ *and* p^m *is sufficiently large.*

In the special case of $m=1$ *we have equality. (We also have equality when* $p^m=4,8,49$.*)*

Our proof does not include the special cases $p^m=4,8$ and 49. For these 3 cases we simply computed the value of $c(n)$ that gives equality. The basic idea of the proof of Theorem 6 is to decompose $\overline{\mathcal{H}}_{p^m}$ into $p-1$ distinct subsets $C_i, i=1,\ldots,p-1$, such that any line that connects a point in C_i to a point in C_j, with $i\neq j$, must be ordinary. We define the sets C_i as follows:

$$C_i=\left\{(x,y)\in \overline{\mathcal{H}}_{p^m} \,:\, x\equiv i \pmod p\right\},$$

where $1\leq i\leq p-1$. We note that $\#C_i=p^{m-1}$.

In several places we will need to invoke Hensel's lemma. Even though this lemma is a basic result in number theory, for the sake of completeness we state it.

Theorem 7 (Hensel's lemma). *Let p be a prime and let $f(x)\in\mathbb{Z}[x]$ be a polynomial whose leading coefficient is not divisible by p. If there exists $x_1\in\mathbb{Z}$ such that*

$$f(x_1)\equiv 0 \pmod p \text{ and } f'(x_1)\not\equiv 0 \pmod p,$$

then for every $k\geq 2$ there exists $x_k\in\mathbb{Z}$ such that

$$f(x_k)\equiv 0 \pmod{p^k} \text{ and } x_k\equiv x_{k-1} \pmod{p^{k-1}}.$$

Furthermore, x_k is uniquely determined modulo p^k.

We now state and prove the key lemma of this section.

Lemma 8. *Let $m \geq 2$ be an integer, $p > 2$ be a prime and let L be a line*

$$L : ax + by + c = 0, \text{ with } \gcd(a, b, c) = 1,$$

that is spanned by $\overline{\mathcal{H}}_{p^m}$. Then we have the following:

(i) $c^2 - 4ab \equiv 0 \pmod{p}$ *if and only if* $L \cap \overline{\mathcal{H}}_{p^m} \subseteq C_i$ *with* $i = -c(2a)^{-1} \bmod p$.

(ii) $\gcd(ab, p) = 1$.

(iii) If $\#(L \cap \overline{\mathcal{H}}_{p^m}) \geq 3$, *then* $L \cap \overline{\mathcal{H}}_{p^m} \subseteq C_i$ *for some* i.

(iv) If $\#(L \cap \overline{\mathcal{H}}_{p^m}) \geq 3$, *then* $\gcd(c, p) = 1$.

(v) If $c = 0$, *then* L *is the line* $y = x$.

Proof. Let $f(x)$ denote the polynomial $ax^2 + cx + b$.

(i) If $c^2 - 4ab \equiv 0 \pmod{p}$ then by the quadratic formula $2ax \equiv -c \pmod{p}$ for any $(x, y) \in L \cap \overline{\mathcal{H}}_{p^m}$. If $p|a$ then $p|c$. By considering the equation of L we conclude that $p|b$. This contradicts our hypothesis that $\gcd(a, b, c) = 1$. Thus, $\gcd(a, p) = 1$ and $x \equiv -c(2a)^{-1} \pmod{p}$ for every $(x, y) \in L \cap \overline{\mathcal{H}}_{p^m}$.

For the opposite direction, we show that if

$$(x_1, y_1), (x_2, y_2) \in L \cap \overline{\mathcal{H}}_{p^m}$$

with $x_1 \neq x_2$ (and thus $y_1 \neq y_2$) and $x_1 \equiv x_2 \pmod{p}$, then

$$2ax_1 \equiv -c \pmod{p} \text{ and } 2by_1 \equiv -c \pmod{p}.$$

The result then follows by multiplying these two congruences together.

We prove the first congruence. Now,

$$a(x + h)^2 + c(x + h) + b = (ax^2 + cx + b) + (2ax + c)h + ah^2.$$

Setting $x = x_1$ and $h = x_2 - x_1$ we obtain

$$ax_2^2 + cx_2 + b = (ax_1^2 + cx_1 + b) + (2ax_1 + c)(x_2 - x_1) + a(x_2 - x_1)^2.$$

Since $f(x_1) \equiv f(x_2) \equiv 0 \pmod{p^m}$, we get

$$(2ax_1 + c + a(x_2 - x_1))(x_2 - x_1) \equiv 0 \pmod{p^m}.$$

Since $x_1 \equiv x_2 \pmod{p}$, but $x_1 \not\equiv x_2 \pmod{p^m}$, we infer that

$$2ax_1 + c + a(x_2 - x_1) \equiv 0 \pmod{p^l}$$

for some $l, 0 < l < m$, and conclude that

$$2ax_1 + c \equiv 0 \pmod{p}.$$

A similar proof yields $2by_1 \equiv -c \pmod{p}$.

(ii) We argue by contradiction. Suppose $\gcd(ab, p) = p$. Without loss of generality we may assume that $p|a$. Let (x_1, y_1) and (x_2, y_2) be two distinct points in $L \cap \overline{\mathcal{H}}_{p^m}$. Therefore

$$f(x_1) \equiv f(x_2) \equiv 0 \pmod{p^m}.$$

Since $p|a$, $f(x)$ reduces modulo p to the linear polynomial $cx + b$. Since x_1 and x_2 are both zeros of the congruence $cx + b \equiv 0 \pmod{p}$, we conclude that $x_1 \equiv x_2 \pmod{p}$. By part (i) we now obtain

$$-c \equiv 2ax_1 \equiv 0 \pmod{p}.$$

Since $p|a$, we have that $p|c$ and consequently $p|b$. But this contradicts our hypothesis that $\gcd(a, b, c) = 1$.

(iii) Since $\gcd(ab, p) = 1$ the linear transformation $x = 2ax + c$ is invertible modulo p^m. Using this change of variable we transform the congruence

$$f(x) \equiv 0 \pmod{p^m}$$

to

$$z^2 \equiv (c^2 - 4ab) \pmod{p^m}.$$

If $\gcd(c^2 - 4ab, p) = 1$, then the congruence $z^2 \equiv (c^2 - 4ab) \pmod{p}$ would have precisely 2 solutions and by Hensel's lemma each one would lift to a unique solution of $z^2 \equiv (c^2 - 4ab) \pmod{p^m}$. This in turn would imply $f(x) \equiv 0 \pmod{p^m}$ has precisely 2 solutions. This contradicts our hypothesis that $f(x) \equiv 0 \pmod{p^m}$ has at least 3 solutions. Consequently, we must have that $(c^2 - 4ab) \equiv 0 \pmod{p}$, and the result follows from (i).

(iv) From (iii) and (i) we infer that $c^2 \equiv 4ab \pmod{p}$. Since $\gcd(ab, p) = 1$, $p \not| c$.

(v) By (iv) $\#(L \cap \overline{\mathcal{H}}_{p^m}) = 2$. Let (x_1, y_1) and (x_2, y_2) be the two elements of the intersection $L \cap \overline{\mathcal{H}}_{p^m}$. From the fact that x_1 and x_2 are the two distinct solutions of $x^2 \equiv -ba^{-1} \pmod{p^m}$ we conclude that $x_2 = p^m - x_1$ and $y_2 = p^m - y_1$. Furthermore the slope of L is

$$-\frac{b}{a} = \frac{y_1}{x_1} = \frac{p^m - y_1}{p^m - x_1}.$$

From the last equality we get that $x_1 = y_1$ and thus $b = -a$, that is, L is the line $y = x$. □

The next proposition gives an upper bound on the number of points of $\overline{\mathcal{H}}_{p^m}$ that can be collinear.

Proposition 9. *Let $p > 2$ be prime and L a line spanned by $\overline{\mathcal{H}}_{p^m}$. Then*

$$\#(L \cap \overline{\mathcal{H}}_{p^m}) \leq 2p^{\lfloor m/2 \rfloor}. \tag{2}$$

Proof. Any point $(x, y) \in L \cap \overline{\mathcal{H}}_{p^m}$ gives rise to a solution of the quadratic congruence

$$ax^2 + cx + b \equiv 0 \pmod{p^m}.$$

Thus we have that

$$\#(L \cap \overline{\mathcal{H}}_{p^m}) \leq N,$$

where N denotes the number of solutions of

$$ax^2 + cx + b \equiv 0 \pmod{p^m} \tag{3}$$

with $0 \leq x < p^m$.

Let $D = c^2 - 4ab$ be the discriminant of the quadratic equation. The change of variable $z = 2ax + c$ transforms congruence (3) to

$$z^2 \equiv D \pmod{p^m}. \tag{4}$$

We obtain the bound (2) by determining the solutions of congruence (4). There are three possibilities:

(i) $D \not\equiv 0 \pmod{p}$;

(ii) $D \equiv 0 \pmod{p^m}$;

(iii) $D \equiv 0 \pmod{p}$ but $D \not\equiv 0 \pmod{p^m}$.

(i) Since (4) has a solution and $D \not\equiv 0 \pmod{p}$, the congruence $z^2 \equiv D \pmod{p}$ has precisely 2 solutions. By Hensel's lemma each one lifts to a unique solution of $z^2 \equiv D \pmod{p^m}$. This in turn implies that $ax^2 + cx + b \equiv 0 \pmod{p^m}$ has precisely 2 solutions.

(ii) If $D \equiv 0 \pmod{p^m}$, then the solutions of (4) are of the form $kp^{\lceil m/2 \rceil}$ with $k = 0, 1, \ldots, p^{\lfloor m/2 \rfloor} - 1$, and consequently (4) has $p^{\lfloor m/2 \rfloor}$ solutions.

(iii) Since $p|D$, but $p^m \not| D$, there exists i with $1 \leq i < m$ such that $D \equiv 0 \mod p^i$, but $D \not\equiv 0 \mod p^{i+1}$. Since $\gcd(D/p^i, p) = 1$, we infer that $p^i | Z^2$, but $p^{i+1} \not| Z^2$, where Z is a solution of (4). It immediately follows that i is even.

We now rewrite (4) as

$$z^2 \equiv D/p^i \pmod{p^{m-i}}.$$

Since this congruence has a solution and $\gcd(D/p^i, p) = 1$, by the same argument as in (i) above we conclude there are exactly two integers k_1, k_2, with $0 < k_1, k_2 < p^{m-i}$, such that

$$k_1^2 \equiv k_2^2 \equiv D/p^i \pmod{p^{m-i}}.$$

Thus the solutions of the congruence (4) are of the form

$$(k_1 + lp^{m-i})p^{i/2} \text{ or } (k_2 + lp^{m-i})p^{i/2}$$

with $l = 0, 1, \ldots, p^{i/2} - 1$. Consequently, (4) has $2p^{i/2}$ solutions.

In all three cases we see that (4) has no more than $2p^{\lfloor m/2 \rfloor}$ solutions and so we obtain the bound (2). □

Bound (2) shows that for $m \geq 3$, the points of C_i are not collinear. We give a comprehensive proof of this fact to include the case $m = 2$.

Lemma 10. *Let $p > 2$ and $m \geq 2$. For each i, with $i = 1, 2, \ldots, p-1$, the points of C_i are not collinear.*

Proof. We argue by contradiction. Suppose there exists a line L and an $i, 1 \leq i \leq p-1$, such that $L \cap \overline{\mathcal{H}}_{p^m} = C_i$. By choosing the points on C_i whose x-coordinates are i and $i+p$ respectively, we infer that the slope of the line L is an integer. The line $y = x$ is a line of symmetry of $\overline{\mathcal{H}}_{p^m}$. If we reflect L along $y = x$, we get a line L' such that $L' \cap \overline{\mathcal{H}}_{p^m} = C_{i^{-1} \bmod p}$. By the same argument as before we get that the slope of L' is an integer. Furthermore $\text{slope}(L) \cdot \text{slope}(L') = 1$ and consequently $\text{slope}(L) = \pm 1$.

Suppose $\text{slope}(L) = -1$. Since $x = y$ is a line of symmetry of $\overline{\mathcal{H}}_{p^m}$, the reflection of L along $x = y$ is L itself. Consequently if $(s, t) \in C_i \cap L$, then $(t, s) \in C_i \cap L$. Since the number of points in C_i is odd it follows that there must be a point in $C_i \cap L$ lying on $x = y$. Now the only points of $\overline{\mathcal{H}}_{p^m}$ that lie on $x = y$ are $(1, 1)$ and $(p^m - 1, p^m - 1)$. Furthermore the line of slope -1 passing through $(1, 1)$ contains no other points of $\overline{\mathcal{H}}_{p^m}$. A similar observation holds for $(p^m - 1, p^m - 1)$. In either case we obtain a contradiction to our assumption that $C_i \subseteq L$.

So the last case to consider is $\text{slope}(L) = 1$. Let $(0, b)$ be the y-intercept of L. We have two possible cases: $i + b \geq p$ or $i + b < p$.

If $i + b \geq p$, then the point $(i + p^m - p, i + b + p^m - p)$ does not belong to $\overline{\mathcal{H}}_{p^m} \cap L$, and consequently the point of C_i with x-coordinate $i + p^m - p$ does not lie on L. If $i + b < p$, then $i \cdot (i + b) < p^2$. Since $i \cdot (i + b) \equiv 1 \pmod{p^m}$, it follows that $i \cdot (i + b) = 1$; that is, $(i, i + b) = (1, 1)$ and L is the line $x = y$. As noted earlier, this line contains only two points of $\overline{\mathcal{H}}_{p^m}$, and so once again we obtain a contradiction to our assumption that $C_i \subseteq L$. □

We are now in a position to prove Theorem 6. We will need the following results. For small p^m we will invoke the following weaker version of the Dirac-Motzkin conjecture proved by Csima and Sawyer [3].

Theorem 11. *Suppose P is a finite set of n points in the plane, not all on a line and $n \neq 7$. Then P spans at least $6n/13$ ordinary lines.*

The Dirac-Motzkin conjecture states that the lower bound for the number of ordinary lines is $n/2$ for sufficiently large n. Green and Tao [4, Theorem 2.2] have proved a more precise version of this conjecture which implies the following result.

Theorem 12. *Suppose P is a finite set of n points in the plane, not all on a line, and n is sufficiently large. Then P spans at least $(3/4 + o(1))n$ ordinary lines if n is odd and at least $n/2$ ordinary lines if n is even.*

Proof of Theorem 6. We first consider the case $p > 2$. If $(x_1, y_1) \in C_i$ and $(x_2, y_2) \in C_j$ with $i \neq j$, then Lemma 8 (iii) shows that the line through the points (x_1, y_1) and (x_2, y_2) is ordinary. There are $(p-2)(p-1)p^{2(m-1)}/2$ possible such pairs of points. Furthermore, since the points of C_i do not all lie on a line, by Theorem 11 or Theorem 12, respectively, each C_i gives rise to at least $c\,(p^m)\,p^{m-1}$ ordinary lines. From these observations we conclude that

$$N \geq p^{m-1}(p-1)\left(\frac{p^{m-1}(p-2)}{2} + c(p^m)\right),$$

where $c(n)$ is defined in Theorem 6. For $p = 2$, we have $C_1 = \overline{\mathcal{H}}_{2^m}$ and consequently, $N \geq c\,(2^m) \cdot \#C_1 = c\,(2^m)\,2^{m-1}$. This is the same as the RHS of (1) as the first term of the RHS of (1) is 0. □

We now give an application of Beck's theorem [1, Theorem 3.1] to obtain an estimate for the number of lines spanned by C_i when $m \geq 3$. We first state Beck's theorem in its original version.

Theorem 13 (Beck). *Let P be a set of n points in the plane. Then at least one of the following holds:*

(i) There exists a line containing at least $n/100$ points of P.

(ii) For some positive constant c, there exist at least $c \cdot n^2$ distinct lines containing two or more points of P.

Corollary 14. *If*

$$p^{\lceil m/2 \rceil - 1} > 200,$$

then the number of lines spanned by C_i with $i = 1, \ldots, p-1$, is at least $c \cdot p^{2(m-1)}$, where c is the constant in Beck's theorem.

Proof. We apply Beck's theorem with $P = C_i$. By (2) the first case of Beck's theorem does not hold. Hence C_i spans at least $c \cdot p^{2(m-1)}$ lines. □

3. A Partial Answer to Shparlinski's Question

The observation that the points of $\overline{\mathcal{H}}_{a,n}$ are symmetric along the line $y = x$ suggests the heuristic estimate that the cardinality of the set

$$\mathcal{F}_{a,n} = \{\sqrt{x^2 + y^2} \,:\, (x, y) \in \overline{\mathcal{H}}_{a,n}\}$$

is approximately $\varphi(n)/2$. The primary goal of this section is to adapt the proof of Lemma 4 to estimate the difference

$$\#\mathcal{F}_{a,n} - \frac{\varphi(n)}{2}$$

for $n = p^2$, p an odd prime.

To simplify the notation we introduce a map $d_{a,n} : \mathbb{Z}_n^* \to \mathbb{Z}$ via

$$d_{a,n}(x) = (x \bmod n)^2 + \left(\left(a \cdot x^{-1}\right) \bmod n\right)^2.$$

Clearly $\#\text{Image}(d_{a,n}) = \#\mathcal{F}_{a,n}$. We now focus on estimating $\#\text{Image}(d_{a,p^2})$.

We remark that determining the cardinality of the set

$$\{(x^2 + y^2) \mod n : (x, y) \in \overline{\mathcal{H}}_n\}$$

is easier and has been done in [5] using algebraic manipulations in conjunction with the Chinese Remainder Theorem.

3.1. Some Notation

We begin by defining a class of biquadratic polynomials and certain subsets of $\text{Image}(d_{a,p^2})$ and $\mathbb{Z}_{p^2}^*$. Let $f_u(Z)$ denote the polynomial

$$f_u(Z) = Z^4 - uZ^2 + a^2.$$

Let $A \subseteq \text{Image}(d_{a,p^2})$ be the set

$$A = \{u \in \text{Image}(d_{a,p^2}) : f_u(Z), f_u'(Z) \text{ have no common root modulo } p\}$$

and let B be the complement of A in $\text{Image}(d_{a,p^2})$.

Let B_1, B_2 be the following two subsets of $\text{Image}(d_{a,p^2})$:

$$B_1 = \{d_{a,p^2}(l) : l \in \mathbb{Z}_{p^2}^*, \ l^2 - a \equiv 0 \pmod p\},$$

$$B_2 = \{d_{a,p^2}(l) : l \in \mathbb{Z}_{p^2}^*, \ l^2 + a \equiv 0 \pmod p\}.$$

Finally if a is a quadratic residue modulo p, then there is an integer b, $0 < b < p$, such that $b^2 \equiv a \pmod p$. In this case we define the sets $C_1, C_2 \subseteq \mathbb{Z}_{p^2}^*$ via

$$C_1 = \{b + tp : 0 \le t \le p - 1\},$$

$$C_2 = \{p - b + tp : 0 \le t \le p - 1\}.$$

3.2. Main Result of Section 3 and Proof

Theorem 15. *Let $p > 2$ be a prime. Then*

$$\#\text{Image}(d_{a,p^2}) = \frac{1}{2}\left(\varphi(p^2) + 1 + \left(\frac{a}{p}\right)\right) - \#(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)).$$

Outline of proof of Theorem 15. The proof is encapsulated in the following sequence of statements.

(a) We can associate each $u \in \text{Image}(d_{a,p^2})$ with the congruence

$$f_u(Z) \equiv 0 \pmod{p^2}.$$

(b) Using properties of $f_u(Z)$ we show that for each $u \in A$, there are exactly two distinct elements $x_1, x_2 \in \mathbb{Z}_{p^2}^*$ such that

$$d_{a,p^2}(x_1) = d_{a,p^2}(x_2) = u.$$

(c) The cardinality of A is

$$\#A = \frac{\varphi(p^2) - \#d_{a,p^2}^{-1}(B)}{2}.$$

(d) The set B is the disjoint union of the sets B_1 and B_2. Consequently,

$$\#d_{a,p^2}^{-1}(B) = \#d_{a,p^2}^{-1}(B_1) + \#d_{a,p^2}^{-1}(B_2).$$

(e) If $B_2 \neq \emptyset$, then $\#d_{a,p^2}^{-1}(B_2) = 2p$ and $\#B_2 = p$.

(f) If $B_1 \neq \emptyset$, then $\#d_{a,p^2}^{-1}(B_1) = 2p$. Furthermore,

$$B_1 = d_{a,p^2}(C_1) \cup d_{a,p^2}(C_2)$$

with

$$\#d_{a,p^2}(C_i) = \frac{p-1}{2} + 1,$$

for $i = 1, 2$.

Proof of (a), (b) and (c). Let $u \in \text{Image}(d_{a,p^2})$. Then $u = r_u^2 + \left(ar_u^{-1}\right)^2$ for some $r_u \in \mathbb{Z}_{p^2}^*$ with $1 \leq r_u, ar_u^{-1} < p^2$. It immediately follows that r_u is a root of the congruence $f_u(Z) \equiv 0 \pmod{p}$.

We now turn to statements (b) and (c). Let $u \in A$ and let $r_u \in \mathbb{Z}_{p^2}^*$ such that $d_{a,p^2}(r_u) = u$. We claim that

$$d_{a,p^2}^{-1}(\{u\}) = \{r_u,\, ar_u^{-1}\}.$$

We first show $r_u \neq ar_u^{-1}$, by proving the contrapositive. Let $x = r_u \mod p$ and $y = ar_u^{-1} \mod p$. If $r_u = ar_u^{-1}$, then $x = y$, $x^2 \equiv a \pmod p$ and $u \equiv 2x^2 \pmod p$. It follows that $f_u(Z)$ factors as

$$f_u(Z) = Z^4 - uZ^2 + a^2 \equiv (Z-x)^2(Z+x)^2 \pmod p.$$

But this contradicts our assumption that $f_u(Z)$ and $f_u'(Z)$ do not have any roots in common modulo p. In a similar fashion we show that $ar_u^{-1} \neq p^2 - r_u$.

We now observe that $f_u(Z)$ has four distinct roots modulo p: $x, y, p-x$ and $p-y$. Furthermore each root lifts to a *unique* root modulo p^2, that is, x lifts to r_u, y to ar_u^{-1}, $p-x$ to $(p^2 - r_u)$ and $p-y$ to $(p^2 - ar_u^{-1})$. Consequently $d_{a,p^2}^{-1}(\{u\}) \subseteq \{r_u, ar_u^{-1}, p^2 - r_u, p^2 - ar_u^{-1}\}$. So to conclude the proof we need to prove that $d_{a,p^2}(r_u) \neq d_{a,p^2}(p^2 - r_u)$. If $d_{a,p^2}(r_u) = d_{a,p^2}(p^2 - r_u)$, then a simple calculation shows $ar_u^{-1} = (p^2 - r_u)$ which contradicts our earlier calculation that $ar_u^{-1} \neq p^2 - r_u$. □

Proof of (d). Let $d_{a,p^2}(r_u) = u$, where $u \in (\text{Image}(d_{a,p^2}) \cap B)$ and let $x = r_u \mod p$. Since $u \in B$, x is a common root modulo p of the polynomials $f_u(Z) = Z^4 - uZ^2 + a^2$ and $f_u'(Z) = 4Z^3 - 2uZ$. It follows that $2x^2 = u \pmod p$ and

$$(a - x^2)(a + x^2) \equiv 0 \pmod p.$$

Therefore

$$x^2 \equiv a \pmod p \text{ and } u \equiv 2a \pmod p$$

or

$$x^2 \equiv -a \pmod p \text{ and } u \equiv -2a \pmod p.$$

In the first case $u \in B_1$, and in the second $u \in B_2$. Finally $B_1 \cap B_2 = \emptyset$ since $2a \not\equiv -2a \pmod p$. □

Proof of (e). If $B_2 \neq \emptyset$, then there exists an integer c with $1 \leq c \leq p-1$ such that $c^2 \equiv -a \pmod p$. It follows that $d_{a,p^2}^{-1}(B_2)$ is the disjoint union of the sets D_1, D_2 where

$$D_1 = \{c + tp \,:\, 0 \leq t \leq p-1\},$$

$$D_2 = \{p - c + tp \,:\, 0 \leq t \leq p-1\}.$$

Consequently, $\#d_{a,p^2}^{-1}(B_2) = 2p$.

Now there exists a unique integer l_p, $0 \leq l_p \leq p-1$, such that

$$c \cdot (p - c + l_p p) \equiv a \pmod{p^2}.$$

It follows that for $t = 0, 1, \ldots, p-1$,

$$\left(a \cdot (c+tp)^{-1}\right) \mod p^2 = \begin{cases} p - c + (l_p + t)p, & l_p + t < p \\ p - c + (l_p + t - p)p, & l_p + t \geq p. \end{cases}$$

From this we see that $x \in D_1$ if and only if $a \cdot x^{-1} \in D_2$, and we can conclude that the sets $d_{a,p^2}(D_1)$ and $d_{a,p^2}(D_2)$ are equal, and consequently $B_2 = d_{a,p^2}(D_1)$. So we are done if we can show that d_{a,p^2} is one-to-one on D_1. To do this we define the functions

$$f(t) = (c + tp)^2 + (p - c + (l_p + t)p)^2$$

and

$$g(t) = (c + tp)^2 + (p - c + (l_p + t - p)p)^2.$$

That is,

$$d_{a,p^2}(c + tp) = \begin{cases} f(t), & l_p + t < p, \\ g(t), & l_p + t \geq p. \end{cases}$$

A simple calculation shows that $f(t) = f(s)$ if and only if $s = t$. Similarly, $g(t) = g(s)$ if and only if $s = t$. Finally, if we try to solve the equation $f(t) = g(s)$, we get the contradiction that $2|p$. Thus we get that d_{a,p^2} is one-to-one on D_1. □

Proof of (f). If $B_1 \neq \emptyset$, then there exists an integer b with $1 \leq b \leq p-1$ such that $b^2 \equiv a \pmod{p}$. It follows that $d^{-1}_{a,p^2}(B_1)$ is the disjoint union of the sets C_1, C_2, where (we remind the reader)

$$C_1 = \{b + tp : 0 \leq t \leq p-1\}, \text{ and } C_2 = \{p - b + tp : 0 \leq t \leq p-1\}.$$

Consequently, $\#d^{-1}_{a,p^2}(B_1) = 2p$.

The remaining part of the proof is trickier than the case for B_2. This is because d_{a,p^2} is not one-to-one on C_1, nor are $d_{a,p^2}(C_1)$ and $d_{a,p^2}(C_2)$ equal as sets. We will prove that

$$\#d_{a,p^2}(C_1) = \#d_{a,p^2}(C_2) = \frac{p-1}{2} + 1.$$

Now, there exists a unique integer j_p, $0 \leq j_p \leq p-1$, such that

$$b \cdot (b + j_p p) \equiv a \pmod{p^2}.$$

It follows that for $t = 0, 1, \ldots, p-1$,

$$\left(a \cdot (b + tp)^{-1}\right) \mod p^2 = \begin{cases} b + (j_p - t)p, & t \leq j_p \\ b + (p + j_p - t)p, & t > j_p. \end{cases}$$

We now define the functions

$$f(t) = (b + tp)^2 + (b + (j_p - t)p)^2 \text{ and } g(t) = (b + tp)^2 + (b + (p + j_p - t)p)^2.$$

That is,

$$d_{a,p^2}(b + tp) = \begin{cases} f(t), & t \leq j_p \\ g(t), & t > j_p. \end{cases} \tag{5}$$

A simple calculation shows that $f(t) = f(s)$ if and only if $s = t$ or $s = j_p - t$. Similarly, $g(t) = g(s)$ if and only if $s = t$ or $s = p + j_p - t$. Finally, if we try to

solve the equation $f(t) = g(s)$ we get the contradiction that $2|p$. These observations combined with the observation that either $(b+j_p p/2)$ or $(b+(j_p+p)p/2)$ is a solution of $x^2 \equiv a \pmod{p^2}$, give us the following:

(i) If j_p is even, then $\#f^{-1}(\{t\}) = 2$ for $t \leq j_p, t \neq j_p/2$; $\#g^{-1}(\{t\}) = 2$ for $t > j_p$; and $\#f^{-1}(\{j_p/2\}) = 1$.

(ii) If j_p is odd, then $\#f^{-1}(\{t\}) = 2$ for $t \leq j_p$; $\#g^{-1}(\{t\}) = 2$ for $t > j_p, t \neq (j_p + p)/2$; and $\#f^{-1}(\{(j_p + p)/2\}) = 1$.

We conclude that

$$\#d_{a,p^2}(C_1) = \frac{p-1}{2} + 1.$$

In a similar manner we show that $\#d_{a,p^2}(C_2) = (p-1)/2 + 1$.

In summary we see that if $(a/p) = 1$, then

$$\#B_1 = p + 1 - \#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right).$$

□

3.3. Bounding $\#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right)$

Thus the key difficulty to determining the cardinality $\#\text{Image}(d_{a,p^2})$ is determining the cardinality of the intersection $d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)$. We now identify $C_1 \times C_2$ with the set $\{0, 1, \ldots, p-1\}^2$ via

$$(t, s) \mapsto (b + tp, p - b + sp)$$

and then define the map

$$l : \{0, 1, \ldots, p-1\}^2 \to \mathbb{Z}^2$$

via

$$l\left((t, s)\right) = (d_{a,p^2}(b + tp), d_{a,p^2}(p - b + sp)).$$

Clearly,

$$\#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right) = \#\left(l\left([0, p-1]^2\right) \cap \{(x, x) \,:\, x \in \mathbb{Z}\}\right).$$

In (5) we gave the form of $(a \cdot x^{-1}) \mod p^2$ when $x \in C_1$, and then obtained the distance function associated with C_1. Specifically

$$d_{a,p^2}(b + tp) = \begin{cases} f(t), & t \leq j_p \\ g(t), & t > j_p \end{cases}$$

where

$$f(t) = (b + tp)^2 + (b + (j_p - t)p)^2, \text{ and } g(t) = (b + tp)^2 + (b + (p + j_p - t)p)^2.$$

We now state a similar form when $x \in C_2$. Put

$$k_p = \begin{cases} p - j_p - 2, & j_p \leq p-2, \\ -1, & j_p = p-1. \end{cases}$$

Since $x \in C_2$, $x = p-b+sp$ for some s with $0 \leq s \leq p-1$. An immediate calculation gives us the following:

$$\left(a \cdot x^{-1}\right) \mod p^2 = \begin{cases} p-b+(k_p-s)p, & s \leq k_p, \\ p-b+(p+k_p-s)p, & s > k_p. \end{cases}$$

Put

$$F(s) = (p-b+sp)^2 + (p-b+(k_p-s)p)^2,$$

and

$$G(s) = (p-b+sp)^2 + (p-b+(p+k_p-s)p)^2.$$

Then we have

$$d_{a,p^2}(p-b+sp) = \begin{cases} F(s), & s \leq k_p, \\ G(s), & s > k_p. \end{cases}$$

Proposition 16. *Let L_1, L_2 be the sets*

$$\begin{aligned} L_1 &= \{(t,s) \in [0, j_p/2] \times [k_p+1, (p+k_p)/2] \cap \mathbb{Z}^2 : \\ &\quad (s+t+1-p)(s-t+1+j_p-p) = 2b + j_p p - p^2\}, \end{aligned}$$

$$\begin{aligned} L_2 &= \{(t,s) \in [j_p+1, (p+j_p)/2] \times [0, k_p/2] \cap \mathbb{Z}^2 : \\ &\quad (s+t+1-p)(s-t+1+j_p) = 2b + j_p p\}. \end{aligned}$$

Then for $i = 1, 2$, if $L_i \neq \emptyset$, then l is injective on L_i. Furthermore,

$$l\left([0, p-1]^2\right) \cap \{(x,x) : x \in \mathbb{Z}\} = l(L_1) \cup l(L_2).$$

Proof. Let $(t,s) \in [0, p-1]^2 \cap \mathbb{Z}^2$ such that $d_{a,p^2}(b+tp) = d_{a,p^2}(p-b+sp)$. We consider two cases: (a) $j_p \leq p-2$; (b) $j_p = p-1$.

Case (a) $j_p \leq p-2$. In this case we are forced to consider four equations:

(i) $f(t) - F(s) = 0$: This has no solutions for integral s and t. (Otherwise we get the contradiction $2|p$.)

(ii) $g(t) - G(s) = 0$: Again this has no integer solutions for the same reason as above.

(iii) $f(t) - G(s) = 0$: We have that $f(t) - G(s)$ equals the expression

$$2p^2(-2p^2 + 2sp + 2pj_p + 2p - sj_p - tj_p - 1 + t^2 - j_p + 2b - 2s - s^2).$$

Consequently $f(t) - G(s) = 0$ simplifies to

$$p^2 - 2sp - pj_p - 2p + sj_p + tj_p + 1 - t^2 + j_p + 2s + s^2 = 2b + j_p p - p^2.$$

The LHS now factors to give

$$(s + t + 1 - p)(s - t + 1 + j_p - p) = 2b + j_p p - p^2. \tag{6}$$

(iv) $g(t) - F(s) = 0$: We have that $g(t) - F(s)$ equals the expression

$$2p^2(2pj_p - tp + sp + p - sj_p - tj_p - 1 + t^2 - j_p + 2b - 2s - s^2).$$

Consequently $g(t) - F(s) = 0$ simplifies to

$$-pj_p + tp - sp - p + sj_p + tj_p + 1 - t^2 + j_p + 2s + s^2 = 2b + j_p p.$$

The LHS now factors to give

$$(s + t + 1 - p)(s - t + 1 + j_p) = 2b + j_p p. \tag{7}$$

Case (b) $j_p = p - 1$. In this case we consider the equation $f(t) - G(s) = 0$. We have that

$$f(t) - G(s) = 2p^2(sp - tp - p + t^2 + t - s^2 + 2b - s).$$

Consequently $f(t) - G(s) = 0$ simplifies to

$$(-sp + tp - t^2 - t + s^2 + s) = 2b - p.$$

The LHS factors to give

$$(s - t)(s + t + 1 - p) = 2b - p,$$

which we note is the same as (6) with $j_p = p - 1$.

Thus we have proved that (t, s) satisfies either (6) or (7). Furthermore, it is easy to check that any point $(t, s) \in [0, p-1]^2 \cap \mathbb{Z}^2$ satisfying either (6) or (7) must give that $d_{a,p^2}(b+tp) = d_{a,p^2}(p-b+sp)$. Thus to complete the proof we need to restrict ourselves to sets where l is injective. We now note the following:

(I) $f(t_2) = f(t_1)$ if and only if $t_2 = j_p - t_1$.

(II) $G(s_2) = G(s_1)$ if and only if $s_2 = p - k_p - s_1$.

(III) $g(t_2) = g(t_1)$ if and only if $t_2 = p + j_p - t_1$.

(IV) $F(s_2) = F(s_1)$ if and only if $s_2 = k_p - s_1$.

The condition for equation (6) arose when we considered the equation $f(t) = G(s)$. If we restrict ourselves to values of t and s satisfying this equation to the intervals $0 \leq t \leq j_p/2$, $k_p + 1 \leq s \leq (p + k_p)/2$, we get that l is injective. The condition for equation (7) arose when we considered the equation $g(t) = F(s)$. If we restrict ourselves to values of t and s satisfying this equation to the intervals $j_p + 1 \leq t \leq (p + j_p)/2$, $0 \leq s \leq k_p/2$, we get that l is injective. We conclude that

$$l\left([0, p-1]^2\right) \cap \{(x, x) \,:\, x \in \mathbb{Z}\} = l(L_1) \cup l(L_2)$$

and consequently

$$\#\left(l\left([0, p-1]^2\right) \cap \{(x, x) \,:\, x \in \mathbb{Z}\}\right) = \#l(L_1) + \#l(L_2).$$

□

The interesting case of the previous proposition is the case for $j_p = 0$. By setting $m = (s + t + 1 - p)$ and $n = (s - t + 1)$, and then manipulating various inequalities we obtain the following corollary.

Corollary 17. *Let $j_p = 0$ and let S denote the set of lattice points $(m, n) \in \mathbb{Z}^2$ with $mn = 2b$ satisfying the additional conditions:*

$$-p + 2 \leq m < 0,\ -p/2 + 1 \leq n < 0,\ m \not\equiv n \pmod 2,\ m \leq n.$$

Then

$$\#S = \#l(L_2) = \#\left(d_{a,p^2}(C_1) \cap d_{a,p^2}(C_2)\right).$$

We now have the following two corollaries.

Corollary 18. *For $p \geq 5$, $\#\left(d_{1,p^2}(C_1) \cap d_{1,p^2}(C_2)\right) = 1$; consequently $\#\text{Image}(d_{1,p^2}) = \varphi(p^2)/2$.*

Proof. Since $a = 1$, we have $j_p = 0$. Invoking Corollary 17 we get that $S = \{(-2, -1)\}$. □

Corollary 19. *Let*

$$M_{p^2} = \max\left(\left\{\, \varphi(p^2)/2 - \#\text{Image}(d_{a,p^2}) \,:\, 1 \leq a < p^2,\, \gcd(a, p) = 1\right\}\right).$$

Then

$$\lim_{p \to \infty} (M_{p^2}) = \infty.$$

Proof. Let $a = p_1^2 p_2^2 \ldots p_n^2$, where p_i is the i-th odd prime, and let p be a prime larger than a. Now $b = p_1 p_2 \ldots p_n$ and $j_p = 0$, and therefore we can apply Corollary 17. The cardinality of S (the set defined in Corollary 17) equals 2^n. We now let p and n go to infinity to obtain our conclusion. □

3.4. The case $n = p^m$, $m \geq 3$

The reader should note for p^m with $m \geq 3$, the proofs of statements (a),(b),(c) and (d) extend automatically. The higher power case starts to diverge from our earlier work when we start to consider the counterparts of the sets B_1 and B_2, which we denote as B_{1,p^m}, B_{2,p^m}, that is,

$$B_{1,p^m} = \{d_{a,p^m}(l) : l \in \mathbb{Z}_{p^m}^*, \ \ l^2 - a \equiv 0 \pmod{p}\},$$

and

$$B_{2,p^m} = \{d_{a,p^m}(l) : l \in \mathbb{Z}_{p^m}^*, \ \ l^2 + a \equiv 0 \pmod{p}\}.$$

The proofs that $\#d_{a,p^2}^{-1}(B_1) = 2p$ when $B_1 \neq \emptyset$, and $\#d_{a,p^2}^{-1}(B_2) = 2p$ when $B_2 \neq \emptyset$, extend to the general case. So we have the following.

Theorem 20. *For $i = 1, 2$, if $B_{i,p^m} \neq \emptyset$, then*

$$\#d_{a,p^m}^{-1}(B_{i,p^m}) = 2p^{m-1}.$$

Consequently,

$$\begin{aligned} \#\text{Image}(d_{a,p^m}) - \frac{\varphi(p^m)}{2} &= \left(\#B_{1,p^m} - \frac{(1+(a/p))p^{m-1}}{4}\right) \\ &+ \left(\#B_{2,p^m} - \frac{(1+(-a/p))p^{m-1}}{4}\right). \end{aligned}$$

In particular when $(a/p) = (-a/p) = -1$, and consequently $B_{1,p^m} = B_{2,p^m} = \emptyset$, then

$$\#\text{Image}(d_{a,p^m}) = \frac{\varphi(p^m)}{2}. \tag{8}$$

Our final result provides a lower bound for $\#B_{i,p^m}, i = 1, 2$, when B_{i,p^m} is non-empty.

Proposition 21. *If $u \in B_{i,p^m}$, then*

$$\#d_{a,p^m}^{-1}(\{u\}) \leq 4p^{\lfloor m/2 \rfloor}. \tag{9}$$

Consequently, if $B_{i,p^m} \neq \emptyset$ then

$$\#B_{i,p^m} \geq p^{\lceil m/2 \rceil - 1}/2. \tag{10}$$

Sketch. Without loss of generality let $i = 1$. The proof of (9) is a minor variation on the proof of (2). Since $u \in B_{1,p^m}$, there exist $(x, y) \in \overline{\mathcal{H}}_{a,p^m}$ such that

$$x^2 + y^2 = u.$$

We can transform the equation into the congruence

$$z^2 \equiv (u^2 - 4a^2) \pmod{p^m},$$

where $z = (2x^2 - u)$. We now copy the proof of Proposition 9 to obtain (9). The only difference is that for each value of z there are two possible values of x. Since $\#d^{-1}_{a,p^m}(B_{1,p^m}) = 2p^{m-1}$, (10) follows immediately. □

Our preliminary computations suggest that the bound (9) is weak. Specifically, we have been unable to find a modular hyperbola for which there is a circle that intersects it at many points. Thus, unlike the case for B_1 and B_2, we are not satisfied with the bound for B_{i,p^m}.

3.5. Some Computed Values of $\#\mathcal{F}_{a,p^m}$

We conclude with the following tables of some small values of $\#\mathcal{F}_{a,p^m}$ computed directly. We point out that the lines corresponding to $\#\mathcal{F}_{2,5^m}$ and $\#\mathcal{F}_{3,5^m}$ are redundant. This is because $(2/5) = (3/5) = -1$, that is, neither 2 nor 3 is a quadratic residue modulo 5, and so we can simply invoke (8).

m	1	2	3	4	5	6	7	8	9	10
$\phi(3^m)/2$	1	3	9	27	81	243	729	2187	6561	19683
$\#\mathcal{F}_{1,3^m}$	2	4	10	26	81	243	728	2185	6560	19682
$\#\mathcal{F}_{2,3^m}$	1	3	9	27	81	243	729	2187	6561	19683
$\#\mathcal{F}_{4,3^m}$	2	4	10	27	81	243	729	2185	6559	19681

m	1	2	3	4	5	6	7
$\phi(5^m)/2$	2	10	50	250	1250	6250	31250
$\#\mathcal{F}_{1,5^m}$	3	10	51	249	1251	6248	31250
$\#\mathcal{F}_{2,5^m}$	2	10	50	250	1250	6250	31250
$\#\mathcal{F}_{3,5^m}$	2	10	50	250	1250	6250	31250
$\#\mathcal{F}_{4,5^m}$	3	11	51	249	1251	6249	31248

m	1	2	3	4	5	6	7
$\phi(7^m)/2$	3	21	147	1029	7203	50421	352947
$\#\mathcal{F}_{1,7^m}$	4	21	148	1027	7203	50421	352946
$\#\mathcal{F}_{2,7^m}$	4	22	147	1029	7204	50420	352943
$\#\mathcal{F}_{3,7^m}$	3	21	147	1029	7203	50421	352947
$\#\mathcal{F}_{4,7^m}$	4	21	148	1027	7204	50421	352946

Acknowledgements We thank the referee for some insightful suggestions to improve the exposition of this paper.

References

[1] J. Beck, On the lattice property of the plane and some problems of Dirac, Motzkin and Erdős in combinatorial geometry, *Combinatorica*, **3** (1983), no. 3-4, 281–297.

[2] P. Brass, W. Moser, and J. Pach, *Research Problems in Discrete Geometry,* Springer, 2005.

[3] J. Csima and E. T. Sawyer, There exist $6n/13$ ordinary points, *Discrete Comput. Geom.* **9** (1993), no. 2, 187–202.

[4] B. Green and T. Tao, On sets defining few ordinary lines, *Discrete Comput. Geom.* **50** (2013), no. 2, 409–468. (Also available at http://arxiv.org/abs/1208.4714)

[5] S. Hanrahan and M. R. Khan, The cardinality of the value sets of $\left(x^2 + x^{-2}\right) \mod n$ and $\left(x^2 + y^2\right) \mod n$, *Involve* **3** (2010), no. 2, 171–182.

[6] I. E. Shparlinski, Modular hyperbolas, *Jpn. J. Math.*, **7** (2012), no. 2, 235–294. (Also available at http://arxiv.org/abs/1103.2879)