Concentration points on two and three dimensional modular hyperbolas and applications

J. Cilleruelo
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas
Universidad Autónoma de Madrid
Madrid-28049, Spain
franciscojavier.cilleruelo@uam.es

M. Z. Garaev
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
garaev@matmor.unam.mx

Abstract

Let \( p \) be a large prime number, \( K, L, M, \lambda \) be integers with \( 1 \leq M \leq p \) and \( \gcd(\lambda, p) = 1 \). The aim of our paper is to obtain sharp upper bound estimates for the number \( I_2(M; K, L) \) of solutions of the congruence

\[ xy \equiv \lambda \pmod{p}, \quad K + 1 \leq x \leq K + M, \quad L + 1 \leq y \leq L + M \]

and for the number \( I_3(M; L) \) of solutions of the congruence

\[ xyz \equiv \lambda \pmod{p}, \quad L + 1 \leq x, y, z \leq L + M. \]  \hfill (1)

Using the idea of Heath-Brown from \([6]\), we obtain a bound for \( I_2(M; K, L) \), which improves several recent results of Chan and Shparlinski \([3]\). For instance, we prove that if \( M < p^{1/4} \), then \( I_2(M; K, L) \leq M^{o(1)} \).

The problem with \( I_3(M; L) \) is more difficult and requires a different approach. Here, we connect this problem with the Pell diophantine equation and prove that for \( M < p^{1/8} \) one has \( I_3(M; L) \leq M^{o(1)} \). Our results have applications to some other problems as well. For instance, it follows that if \( \mathcal{I}_1, \mathcal{I}_2, \mathcal{I}_3 \) are intervals in \( \mathbb{F}_p^* \) of length \( |\mathcal{I}_i| < p^{1/8} \), then

\[ |\mathcal{I}_1 \cdot \mathcal{I}_2 \cdot \mathcal{I}_3| = (|\mathcal{I}_1| \cdot |\mathcal{I}_2| \cdot |\mathcal{I}_3|)^{1-o(1)}. \]

MSC Classification: 11A07, 11B75
1 Introduction

In what follows, \( p \) denotes a large prime number, \( K, L, M, \lambda \) are integers with \( 1 \leq M \leq p \) and \( \gcd(\lambda, p) = 1 \). By \( x, y, z \) we denote variables that take integer values. The notation \( B^{\omega(1)} \) denotes such a quantity that for any \( \varepsilon > 0 \) there exists \( c = c(\varepsilon) > 0 \) such that \( B^{\omega(1)} < cB^{\varepsilon} \).

Let \( I_2(M; K, L) \) be the number of solutions of the congruence
\[
xy \equiv \lambda \pmod{p}, \quad K + 1 \leq x \leq K + M, \quad L + 1 \leq y \leq L + M
\]
and let \( I_3(M; L) \) be the number of solutions of the congruence
\[
xyz \equiv \lambda \pmod{p}, \quad L + 1 \leq x, y, z \leq L + M.
\]
Estimates of incomplete Kloosterman sums implies that
\[
I_2(M; K, L) = \frac{M^2}{p} + O(p^{1/2}(\log p)^2). \tag{2}
\]
In particular, if \( M/(p^{3/4}(\log p)^2) \to \infty \) as \( p \to \infty \), one gets that
\[
I_2(M; K, L) = (1 + o(1)) \frac{M^2}{p}.
\]
This asymptotic formula also holds when \( M/p^{3/4} \to \infty \) as \( p \to \infty \) (see [5]). The problem of upper bound estimates of \( I_2(M; K, L) \) for smaller values of \( M \) has been a subject of the work of Chan and Shparlinski [3]. Using Bourgain’s sum-product estimate [1], they have shown that there exists an effectively computable constant \( \eta > 0 \) such that for any positive integer \( M < p \), uniformly over arbitrary integers \( K \) and \( L \), the following bound holds:
\[
I_2(M; K, L) \ll \frac{M^2}{p} + M^{1-\eta}.
\]
In the present paper we obtain the following upper bound estimates for \( I_2(M; K, L) \).

**Theorem 1.** Uniformly over arbitrary integers \( K \) and \( L \), we have
\[
I_2(M; K, L) < \frac{M^{4/3+o(1)}}{p^{1/3}} + M^{o(1)}. \tag{3}
\]
When \( K = L \), we have
\[
I_2(M; L, L) < \frac{M^{3/2+o(1)}}{p^{1/2}} + M^{o(1)}. \tag{4}
\]
In particular, if \( M < p^{1/4} \) then \( I_2(M; K, L) < M^{o(1)} \).

Theorem [1] together with (2) easily implies the following consequence, which improves upon the mentioned result of Chan and Shparlinski.

**Corollary 1.** Uniformly over arbitrary integers \( K \) and \( L \), we have
\[
I_2(M; K, L) \ll \frac{M^2}{p} + M^{4/5+o(1)}.
\]
If \( K = L \), then
\[
I_2(M; L, L) \ll \frac{M^2}{p} + M^{3/4+o(1)}.
\]
The proof of Theorem 1 is based on an idea of Heath-Brown [6]. The problem with $I_3(M; L)$ is more difficult and requires a different approach. Here, we shall connect this problem with the Pell diophantine equation and establish the following statement.

**Theorem 2.** Let $M \ll p^{1/8}$. Then, uniformly over arbitrary integer $L$, we have

$$I_3(M; L) \ll M^{o(1)}. \quad (5)$$

From Theorem 2 we can easily derive a sharp bound for the cardinality of product of three small intervals in $\mathbb{F}_p^*$.

**Corollary 2.** Let $I_1, I_2, I_3$ be intervals in $\mathbb{F}_p^*$ of length $|I_i| < p^{1/8}$. Then

$$|I_1 \cdot I_2 \cdot I_3| = (|I_1| \cdot |I_2| \cdot |I_3|)^{1-o(1)}.$$

Theorems 1 and 2 have also applications to the problem on concentration points on exponential curves as well. Let $g \geq 2$ be an integer of multiplicative order $t$, and let $M < t$. Denote by $J_a(M; K, L)$ the number of solutions of the congruence

$$y \equiv a g^x \pmod{p}; \quad x \in [K + 1, K + M], \ y \in [L + 1, L + M].$$

Chan and Shparlinski [3] used a sum product estimate of Bourgain and Garaev [2] to prove that

$$J_a(M; K, L) < \max\{M^{10/11+o(1)}, M^{9/8+o(1)} p^{-1/8}\}$$

as $M \to \infty$. From our Theorem 1 we shall derive the following improvement on this result.

**Corollary 3.** Let $M < t$. Uniformly over arbitrary integers $K$ and $L$, we have

$$J_a(M; K, L) < (1 + M^{3/4} p^{-1/4}) M^{1/2+o(1)}.$$ 

In particular, if $M \leq p^{1/3}$, then we have $J_a(M; K, L) < M^{1/2+o(1)}$.

Theorem 2 allows to strength Corollary 3 when $M \ll p^{3/20}$.

**Corollary 4.** The following bound holds:

$$J_a(M; K, L) < (1 + M p^{-1/8}) M^{1/3+o(1)}.$$ 

In particular, if $M \ll p^{1/8}$, then we have $J_a(M; K, L) < M^{1/3+o(1)}$.

## 2 Proof of Theorem 1

We will need the following lemma which is a simple version of a more precise result about divisors in short intervals, see, for example, [4].

**Lemma 1.** For all positive integer $n$ and $m \geq \sqrt{n}$, the interval $[m, m + n^{1/6}]$ contains at most two divisors of $n$. 

Proof. Suppose that \( d_1, d_2, d_3 \in [m, m+L] \) are three divisors of \( n \). We claim that the number \( r = \frac{d_1d_2d_3}{(d_1, d_2)(d_1, d_3)(d_2, d_3)} \) is also a divisor of \( n \). To see this, for a given prime \( q \), let \( \alpha_1, \alpha_2, \alpha_3, \alpha \) such that \( q^{\alpha_i} | d_i \), \( i = 1, 2, 3 \) and \( q^\alpha | n \). Assume that \( \alpha_1 \leq \alpha_2 \leq \alpha_3 \leq \alpha \). The exponent of \( q \) in the rational number \( r \) is \( \alpha_1 + \alpha_2 + \alpha_3 - (\min(\alpha_1, \alpha_2) + \min(\alpha_1, \alpha_3) + \min(\alpha_2, \alpha_3)) = \alpha_3 - \alpha_1 \). Since \( 0 \leq \alpha_3 - \alpha_1 \leq \alpha \) we have that \( r \) is an integer divisor of \( n \).

On the other hand, since \( (d_i, d_j) \leq |d_i - d_j| \leq L \) we have

\[
n \geq r > \frac{m^3}{L^3} \geq \frac{n^{3/2}}{L^3},
\]

and the result follows. \( \square \)

Now we proceed to prove Theorem \( \text{H} \). Our approach is based on Heath-Brown’s idea from \( [5] \). We can assume that \( M \) is sufficiently large number. The congruence \( xy \equiv \lambda \pmod{p} \), \( K + 1 \leq x \leq K + M \), \( L + 1 \leq y \leq L + M \) is equivalent to

\[
xy + Kx + Ly \equiv b \pmod{p}, \quad 1 \leq x, y \leq M,
\]

where \( b = \lambda - K^2 \). From the pigeon-hole principle it follows that for any positive integer \( T < p \) there exists a positive integer \( t \leq T^2 \) and integers \( u_0, v_0 \) such that

\[
tK \equiv u_0 \pmod{p}, \quad tL \equiv v_0 \pmod{p}, \quad |u_0| \leq p/T, \quad |v_0| \leq p/T.
\]

From (5) we get that

\[
txy + u_0x + v_0y \equiv b_0 \pmod{p}, \quad 1 \leq x, y \leq M,
\]

for some \( |b_0| < p/2 \). We write this congruence as an equation

\[
txy + u_0x + v_0y = b_0 + zp, \quad 1 \leq x, y \leq M, \quad z \in \mathbb{Z}.
\]

Comparing the minimum and maximum value of the left hand side we can see that

\[
|z| \leq \left| \frac{txy + u_0x + v_0y - b_0}{p} \right| < \frac{T^2M^2}{p} + \frac{2M}{T} + \frac{1}{2}.
\]

We observe that for each given \( z \) the equation (7) is equivalent to the equation

\[
(tx + u_0)(ty + v_0) = n_z, \quad 1 \leq x, y \leq M
\]

for certain integer \( n_z \). If \( n_z = 0 \), then either \( tx + u_0 = 0 \) or \( ty + v_0 = 0 \). Since \( \lambda \neq 0 \pmod{p} \), in either case \( x \) and \( y \) are both determined uniquely. So, we can only consider those \( z \) for which \( n_z \neq 0 \).

- Case \( M < p^{1/4}/4 \). In this case we take \( T = 8M \). Then \( |z| < 1 \) and we have to consider only the integer \( n_z = n_0 \) in (5). Each solution of (5) produces two divisors of \( |n_0| \), \( |tx + u_0| \) and \( |ty + v_0| \), one of them is greater than or equal to \( \sqrt{|n_0|} \). If \( |n_0| \leq 2^{36}M^{18} \) the number of solutions of (5) is bounded by the number of divisors of \( n_0 \), which is \( M^{o(1)} \). If \( |n_0| > 2^{36}M^{18} \), the positive integers \( |tx + u_0| \) and \( |ty + v_0| \) lie in two intervals \( I_1 \) and \( I_2 \) of length \( T^2M \leq 2^6M^3 < |n_0|^{1/6} \). If there were five solutions, we would have three divisors greater of equal to \( \sqrt{|n_0|} \) in an interval of length \( \leq |n_0|^{1/6} \). We apply Lemma \( \text{I} \) to conclude that there are at most four solutions. Hence, in this case we have

\[
I_2(M; K, L) < M^{o(1)}.
\]
• Case \( M \geq p^{1/4}/4 \). In this case we take \( T \approx (p/M)^{1/3} \). Thus \( |z| \ll M^{4/3}/p^{1/3} \). For each \( z \) the number of solutions of (8) is bounded by the number of divisors of \( n_z \) which is \( p^{\omega(1)} = M^{\omega(1)} \). Hence, in this case we get

\[
I_2(M; K, L) < \frac{M^{4/3+\omega(1)}}{p^{1/3}}.
\]

Thus, we have proved that

\[
I_2(M; K, L) < \frac{M^{4/3+\omega(1)}}{p^{1/3}} + M^{\omega(1)}
\]

which proves the first part of Theorem 1.

The proof of the second part of Theorem 1 (corresponding to the case \( K = L \)) is similar, with the only difference that we simply take \( t \leq T \) (instead \( t \leq T^2 \)) satisfying

\[
tK \equiv u_0 \pmod{p}, \quad |u_0| \leq p/T.
\]

3 An auxiliary statement

To prove Theorem 2 we need the following auxiliary statement.

**Proposition 1.** Let \( |A|, |B|, |C|, |D|, |E|, |F| \leq M^{\omega(1)} \) and assume that \( \Delta = B^2 - 4AC \) is not a perfect square (in particular, \( \Delta \neq 0 \)). Then the diophantine equation

\[
Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0
\]

has at most \( M^{\omega(1)} \) solutions in integers \( x, y \) with \( 1 \leq |x|, |y| \leq M^{\omega(1)} \).

We shall need several lemmas.

**Lemma 2.** Let \( A \) be a positive integer that is not a perfect square and let \((x_0, y_0)\) be a solution of the equation the equation \( x^2 - Ay^2 = 1 \) in positive integers with the smallest value of \( x_0 \). Then for any other integer solution \((x, y)\) there exist a positive integer \( n \) such that

\[
|x| + \sqrt{A}|y| = (x_0 + \sqrt{A}y_0)^n.
\]

Lemma 2 is well-known from the theory of Pell’s equation.

**Lemma 3.** Let \( A \) be a squarefree integer, \( N \) is a positive integer. Then the congruence \( z^2 \equiv A \pmod{N} \), \( 0 \leq z \leq N - 1 \) has at most \( N^{\omega(1)} \) solutions.

**Proof.** Let \( J(N) \) be the number of solutions of the congruence in question and let \( N = p_1^{a_1} \cdots p_k^{a_k} \) be a canonical factorization of \( N \). Clearly, \( J(N) = J(p_1^{a_1}) \cdots J(p_k^{a_k}) \), where \( J(p^a) \) is the number of solutions of the congruence \( z^2 \equiv A \pmod{p^a} \), \( 0 \leq z \leq p^a - 1 \). Since \( A \) is squarefree, we have \( J(2^a) \leq 4 \) and \( J(p^a) \leq 2 \) for odd primes \( p \). The result follows.

**Lemma 4.** Let \( A, E \) be integers with \( |A|, |E| < M^{\omega(1)} \) such that \( A \) is not a perfect square. Then the equation

\[
x^2 - Ay^2 = E, \quad 1 \leq x, y < M^{\omega(1)}
\]

has at most \( M^{\omega(1)} \) solutions.
Proof. (1) We can assume that $A$ is also a squarefree number. Indeed, let $A = A_1B_1^2$, where $A_1, B_1$ are nonzero integers, $A_1$ is squarefree and is not a perfect square. Then our equation takes the form $x^2 - A_1(B_1y)^2 = E$, $1 \leq x, y < M^{O(1)}$. Since $B_1y < M^{O(1)}$, it follows that indeed we can assume that $A$ is squarefree.

(2) We can assume that in our equation $\gcd(x, y) = 1$. Indeed, if $d = \gcd(x, y)$, then $d^2 \mid E$. In particular, since $E$ has $M^{O(1)}$ divisors, we have $M^{O(1)}$ possible values for $d$. Besides, $(x/d)^2 + A(y/d)^2 = E/d^2$, where we have now $\gcd(x/d, y/d) = 1$. Thus, without loss of generality, we can assume that $\gcd(x, y) = 1$. In particular, it follows that $\gcd(y, E) = 1$.

(3) Since $A$ is not a perfect square, we have, in particular, that $E \neq 0$.

(4) For any $x, y \in \mathbb{Z}_+$ with $(y, E) = 1$ there exists $1 \leq z \leq |E|$ such that $x \equiv zy \pmod{E}$.

Given $1 \leq z \leq |E|$, let $K_z$ be the set of all pairs $(x, y)$ with

$$x^2 - Ay^2 = E, \quad 1 \leq x, y < M^{O(1)}, \quad (x, y) = 1$$

such that $x \equiv zy \pmod{E}$.

If $(x, y) \in K_z$, then $(zy)^2 - Ay^2 \equiv 0 \pmod{E}$. Since $(y, E) = 1$, it follows that $z^2 \equiv A \pmod{E}$. Due to Lemma 2, the number of solutions of this congruence is at most $|E|^{O(1)}$. Thus, we have at most $M^{O(1)}$ possible values for $z$. Therefore, it suffices to show that $|K_z| = M^{O(1)}$ for any such $z$.

Let $x_0$ be the smallest positive integer such that

$$x_0^2 - Ay_0^2 = E, \quad (x_0, y_0) \in K_z.$$

Let $(x, y)$ be any other solution from $K_z$. Then,

$$x_0^2 - Ay_0^2 = E, \quad x^2 - Ay^2 = E.$$ 

From this we derive that

$$(x_0x - Ay_0y)^2 - A(xy_0 - x_0y)^2 = (x_0^2 - Ay_0^2)(x^2 - Ay^2) = E^2. \quad (10)$$

On the other hand, from $(x_0, y_0), (x, y) \in K_z$ it follows that

$$x_0 \equiv zy_0 \pmod{E}, \quad x \equiv zy \pmod{E}.$$ 

Since $z^2 \equiv A \pmod{E}$, we get $xx_0 \equiv z^2 y_0y \pmod{E} \equiv Ay_0 \pmod{E}$. We also have $x_0y \equiv xy_0 \pmod{E}$, as both hand sides are $zy_0 \pmod{E}$. Therefore,

$$x_0x - Ay_0y \equiv 0 \pmod{E}, \quad xy_0 - x_0y \equiv 0 \pmod{E}. \quad (11)$$

From (11) and (11) we get that

$$
\left(\frac{x_0x - Ay_0y}{E}\right)^2 - A \left(\frac{xy_0 - x_0y}{E}\right)^2 = 1
$$

and the numbers inside of parenthesis are integers.

Now there are two cases to consider:

(1) $A > 0$. In view of Lemma 2

$$\left|\frac{x_0x - Ay_0y}{E}\right| + \sqrt{|A|}\left|\frac{xy_0 - x_0y}{E}\right| = (u_0 + \sqrt{|A|v_0})^n,$$
where \((u_0, v_0)\) is the smallest solution to \(X^2 - AY^2 = 1\) in positive integers, and \(n\) is some non-negative integer.

Since the left hand side is of the order of magnitude \(M^{O(1)}\), we have that \(n \ll \log M = M^{o(1)}\). Thus, there are \(M^{o(1)}\) possible values for \(n\) and, each given \(n\) produces at most 4 pairs \((x, y)\). This proves the statement in the first case.

(2) \(A < 0\). Then we get that

\[
\frac{x_0 x - Ay_0 y}{E} \in \{-1, 0, 1\}, \quad \frac{xy_0 - x_0 y}{E} \in \{-1, 0, 1\},
\]

and the result follows.

\[ \square \]

The proof of Proposition \(7\). Now we can deduce Proposition \(1\) from Lemma \(4\). Multiplying \(9\) by \(4\), we get

\[
(2Ax + By + D)^2 - \Delta y^2 + (4EA - 2BD)y + 4AF - D^2 = 0,
\]

where \(\Delta = B^2 - 4AC\). Multiplying by \(\Delta\) we get,

\[
(\Delta y + BD - 2EA)^2 - \Delta(2x + By + D)^2 = T,
\]

where \(T = (BD - 2EA)^2 + 4AF - D^2\). Now, since \(\Delta\) is not a full square, and since \(T, \Delta \leq M^{O(1)}\), we have, by Lemma \(4\) and the condition \(|A|, |B|, |C|, |D|, |E|, |F| \leq M\), that there are at most \(M^{o(1)}\) possible pairs \((\Delta y + BD - 2EA, 2x + By + D)\). Each such pair uniquely determines \(y\) (since \(\Delta \neq 0\)) and \(x\). This finishes the proof of Proposition \(1\). \[ \square \]

### 4 Proof of Theorem \(2\)

In what follows, by \(v^\star\) we denote the least positive integer such that \(vv^\star \equiv 1 \pmod{p}\). We rewrite our congruence in the form

\[
(L + x)(L + y)(L + z) \equiv \lambda \pmod{p}, \quad 1 \leq x, y, z \leq M
\]

which, in turn, is equivalent to the congruence

\[
L^2(x + y + z) + L(xy + xz + yz) + xyz \equiv \lambda - L^3 \pmod{p}, \quad 1 \leq x, y, z \leq M. \tag{12}
\]

Assume that \(M \ll p^{1/8}\) and that \(p\) is large enough to satisfy several inequalities through the proof. Let

\[
k = \max\{1, 2M^2/p^{1/4}\}. \tag{13}
\]

**Lemma 5.** If \(L = uv^\star\) for some integers \(u, v\) with \(|u| \leq M^3/k\) and \(1 \leq |v| \leq M^2/k\), then the number of solutions of the congruence \((12)\) is at most \(M^{o(1)}\).

**Proof.** The congruence \((12)\) is equivalent to

\[
v^2xyz + uv(xy + xz + yz) + u^2(x + y + z) \equiv \mu \pmod{p},
\]

where \(|\mu| < p/2\) and \(\mu \equiv \lambda v^2 - u^3v^\star\). The absolute value of the left hand side is bounded by

\[
(M^2/k)^2M^3 + (M^3/k)(M^2/k)(3M^2) + (M^3/k)^2(3M) \leq 7M^7/k^2 \leq 7M^7/(2M^2/p^{1/4})^2 = \frac{7}{4}M^3p^{1/2} < p/2.
\]
Hence, the congruence (12) is equivalent to the equality
\[ v^2xyz + uv(xy + xz + yz) + u^2(x + y + z) = \mu. \]

Multiplying by \( v \), we get
\[ (vx + u)(vy + u)(vz + u) = v\mu + u^3 \]

The absolute value of the right and the left hand sides is \( \leq M^{O(1)} \), and besides it is distinct from zero (since \( v\mu + u^3 \equiv \lambda v^3 \pmod{p} \), and \( \lambda v^3 \not\equiv 0 \pmod{p} \). Therefore, the number of solutions of the latter equation is bounded by \( M^{o(1)} \) and the lemma follows. \( \square \)

Due to this lemma, from now on we can assume that \( L \) does not satisfy the condition of Lemma 5, that is
\[ L \neq uv^*, \quad |u| \leq M^3/k, \quad |v| \leq M^2/k. \] (14)

For \( 0 \leq r, s \leq 3k - 1 \) and \( 0 \leq t \leq k - 1 \) let \( S_{rst} \) be the set of solutions \((x, y, z)\) such that
\[
\begin{aligned}
    x + y + z &\in (rM/k, (r+1)M/k) \\
    xy + xz + yz &\in (sM^2/k, (s+1)M^2/k) \\
    xyz &\in (tM^3/k, (t+1)M^3/k)
\end{aligned}
\]

Clearly, the number of solutions \( I_3(M; L) \) of our congruence satisfies
\[ I_3(M; L) \leq 9k^3 \max |S_{rst}|. \]

We fix one solution \((x_0, y_0, z_0)\) \(\in S_{rst}\). Any other solution \((x_i, y_i, z_i)\) \(\in S_{rst}\) satisfies the congruence
\[ A_iL^2 + B_iL + C_i \equiv 0 \pmod{p} \] (15)

where
\[
\begin{aligned}
    A_i &= x_i + y_i + z_i - (x_0 + y_0 + z_0), \\
    B_i &= x_iy_i + x_iz_i + y_iz_i - (x_0y_0 + x_0z_0 + y_0z_0), \\
    C_i &= x_iz_i - x_0y_0z_0.
\end{aligned}
\]

We have
\[ |A_i| \leq M/k, \quad |B_i| \leq M^2/k, \quad |C_i| \leq M^3/k. \] (16)

A solution \((x_i, y_i, z_i) \neq (x_0, y_0, z_0)\) we call degenerated if \( A_i = 0 \), and non-degenerated otherwise.

The set of non-degenerated solutions.

We shall show that there are at most \( M^{o(1)} \) non-degenerated solutions. So that, let us assume that there are at least several non-degenerated solutions. With this set of solutions we shall form a system of congruence with respect to \( L, L^2 \). Let us fix one solution \((A_1, B_1, C_1)\). Note that the condition \( A_i = 0 \) implies that \( A_i \not\equiv 0 \pmod{p} \).

Case (1). If \( A_1B_1 \neq A_iB_i \) for some \( i \), then in view of inequalities (16) we also have that \( A_1B_1 \neq A_1B_i \pmod{p} \). Solving the system of equations (15) corresponding to the indices \( i \) and 1, we obtain that
\[ L \equiv (C_iA_1 - A_iC_1)(A_iB_1 - A_iB_i)^* \pmod{p} \equiv uv^* \pmod{p}, \]

8
where
\[ u = C_iA_1 - A_iC_1, \quad v = A_iB_1 - A_1B_i, \quad u' = B_iC_1 - C_iB_1. \]

From this we derive that
\[ |u| \leq 2M^4/k^2, \quad |u'| \leq 2M^5/k^2, \quad |v| \leq 2M^3/k^2 \]
and \((uv^*)^2 \equiv L^2 \pmod{p}\). Hence, \(u^2 \equiv u'v^* \pmod{p}\). By using \((17), (13)\), we get \(|u|^2, |u'v^*| \leq 4M^8/k^4 \leq p/4\), so that we actually have the equality \(u^2 = u'v^* \).

Multiplying \((12)\) by \(v\), we get
\[ vxyz + u(xy + xz + yz) + u'(x + y + z) \equiv v(\lambda - L^3) \pmod{p} \] (18)

Since 1 \(\leq x, y, z \leq M\), the inequalities \((17)\) give
\[ |vxyz + u(xy + xz + yz) + u'(x + y + z)| \leq \frac{14M^6}{k^2} \leq \frac{14M^6}{(2M^2p^{-1/4})^2} = \frac{7M^2p^{1/2}}{2} < p/2. \]

This converts the congruence \((18)\) into the equality
\[ vxyz + u(xy + xz + yz) + u'(x + y + z) = \mu \]
for some \(\mu \preceq M^{O(1)}\) and \(\mu \equiv v(\lambda - L^3) \pmod{p}\). We multiply this equality by \(v^2\) and use \(u'v = u^2\); we get that
\[ (vx + u)(vy + u)(vz + u) = \mu v^2 + u^3. \]

Since \(\mu v^2 + u^3 \neq 0\), the total number of solutions of the latter equation is \(\ll M^{o(1)}\).

Case (2). If we are not in case (1), then for any index \(i\) one has \(A_iB_i = A_iB_1\), which, in turn, implies that we also have
\[ A_iC_i \equiv A_iC_1 \pmod{p}. \]

In view of inequalities \((16)\), we get that the latter congruence is also an equality, so that we have
\[ A_iB_i = A_iB_1, \quad A_iC_i = A_iC_1. \]

From the first equation and the definition of \(A_i, B_i, C_i\), we get
\[ z_i(A_1(x_i + y_i) - B_1) = B_1(x_i + y_i - a_0) - A_1x_iy_i + b_0A_1, \]
(21)
from the second equation we get
\[ z_i(A_1x_iy_i - C_1) = C_1(x_i + y_i - a_0) + c_0A_1, \]
(22)
where
\[ a_0 = x_0 + y_0 + z_0, \quad b_0 = x_0y_0 + y_0z_0 + z_0x_0, \quad c_0 = x_0y_0z_0. \]

Multiplying \((21)\) by \(A_1x_iy_i - C_1\), and \((22)\) by \(A_1(x_i + y_i) - B_1\), subtracting the resulting equalities, and making the change of variables \(x_i + y_i = u_i, \quad x_iy_i = v_i\), we obtain
\[ (B_1(u_i - a_0) - A_1v_i + b_0A_1)(A_1v_i - C_1) = (C_1(u_i - a_0) + c_0A_1)(A_1u_i - B_1). \]

We rewrite this equation in the form
\[ A_i v_i^2 + C_1 u_i^2 - B_1 u_i v_i - (a_0 C_1 - c_0 A_i) u_i - (b_0 A_1 - a_0 B_1 + C_1) v_i + b_0 C_1 - c_0 B_1 = 0. \]

If \( B_1^2 - 4A_1 C_1 \) is a full square (as a number), say \( R_1^2 \), then from (12) we obtain that \( L \equiv (-B_1 \pm R_1)(2A_1)^* = uv^* \) with \( |u| \leq |B_1| + |B_1| + \sqrt{|4A_1 C_1|} \leq 4M^2/k \), \( |v| \leq 2M/k \), which contradicts our condition (14).

If \( B_1^2 - 4A_1 C_1 \) is not a full square, then we are at the conditions of Proposition 4 and we can claim that the number of pairs \((u_i, v_i)\) is at most \( M^{o(1)} \). We now conclude the proof observing that each pair \( u_i, v_i \) produces at most two pairs \( x_i, y_i \), which, in turn, determines \( z_i \). Therefore, the number of non-degenerated solutions counted in \( S_{rst} \) is at most \( M^{o(1)} \).

The set of degenerated solutions.

We now consider the set of solutions for which \( A_i = 0 \). If \( B_i \neq 0 \), then \( B_i \not\equiv 0 \pmod{p} \) and thus we get \( L = -C_i B_i^* \) with \( |C_i| \leq M^3/k \), \( |B_i| \leq M^2/k \), which contradicts condition (14).

If \( B_i = 0 \) then together with \( A_i = 0 \) this implies that \( C_i = 0 \). Thus,
\[
\begin{align*}
    x_i + y_i + z_i &= a_0 = x_0 + y_0 + z_0, \\
    x_i y_i + x_i z_i + y_i z_i &= b_0 = x_0 y_0 + y_0 z_0 + z_0 x_0, \\
    x_i y_i z_i &= c_0 = x_0 y_0 z_0.
\end{align*}
\]
Hence,
\[
(L + x_i)(L + y_i)(L + z_i) = (L + x_0)(L + y_0)(L + z_0).
\]
The right hand side is not zero (since it is congruent to \( \lambda \pmod{p} \) and \( \gcd(\lambda, p) = 1 \)). Thus, the number of solutions of this equation is at most \( M^{o(1)} \). The result follows.

5 Proof of Corollaries

If \( M < p^{5/8} \) then
\[
\frac{M^{4/3+o(1)}}{p^{1/3}} + M^{o(1)} < M^{4/5+o(1)}
\]
and the statement of Corollary 4 for \( I_2(M; K, L) \) follows from Theorem 4. If \( M > p^{5/8} \) then, \( p^{1/2}(\log p)^2 < M^{4/5+o(1)} \) and the statement of Corollary 4 for \( I_2(M; K, L) \) follows from (5).

Analogously we deal with \( I_2(M; K, K) \) considering the cases \( M > p^{2/3} \) and \( M < p^{2/3} \).

In order to prove Corollary 3 let \( k = J_0(M; K, L) \) and let \((x_i, y_i), i = 1, \ldots, k\), be all solutions of the congruence \( y \equiv a g^z \pmod{p} \) with \( x_i \in [K+1, K+M] \) and \( y_i \in [L+1, L+M] \). Since \( M < t \), the numbers \( y_1, \ldots, y_k \) are distinct. Since \( y_i y_j \equiv a g^z \pmod{p} \) for some \( z \in [2K+2, 2K+2M] \), there exists a value \( \lambda \) such that for at least \( k^2/2M \) pairs \((y_i, y_j)\) we have \( y_i y_j \equiv \lambda \pmod{p} \). Hence, theorem 4 implies that
\[
\frac{k^2}{2M} < \frac{M^{3/2+o(1)}}{p^{1/2}} + M^{o(1)},
\]
and the result follows.

Corollary 4 is proved similar to Corollary 3. For any triple \((i, j, \ell)\) we have \( y_i y_j y_\ell \equiv a g^z \pmod{p} \) for some \( z \in [3K + 3, 3K + 3M] \). Hence, there exists \( \lambda \not\equiv 0 \pmod{p} \) such that the congruence \( y_i y_j y_\ell \equiv \lambda \pmod{p} \) has at least \( k^3/3M \) solutions. Thus,
\[
\frac{k^3}{3M} < M^{o(1)},
\]
and the result follows in this case. If $M > p^{1/8}$, then in the interval $[L + 1, L + M]$ we can find a subinterval of length $p^{1/8}$ which would contain at least $k/(2Mp^{-1/8})$ members from $y_1, \ldots, y_k$. Thus, the preceding argument gives that
\[
\left(\frac{k}{Mp^{-1/8}}\right)^3 < M^{o(1)},
\]
and the result follows.

Now we prove Corollary 2. Let $W$ be the number of solutions of the congruence
\[xyz \equiv x'y'z' \pmod{p}, \quad (x, x', y, y', z, z') \in \mathcal{I}_1 \times \mathcal{I}_1 \times \mathcal{I}_2 \times \mathcal{I}_2 \times \mathcal{I}_3 \times \mathcal{I}_3.\]
Then,
\[W = \frac{1}{p} \sum_{x} \left| \sum_{y} \chi(x) \right|^2 \left| \sum_{z} \chi(y) \right|^2 \left| \sum_{z} \chi(z) \right|^2.
\]
Applying the Holder’s inequality, we obtain
\[W \leq \left( \frac{1}{p} \sum_{x} \left| \sum_{y} \chi(x) \right|^6 \right)^{1/3} \left( \frac{1}{p} \sum_{y} \left| \sum_{z} \chi(y) \right|^6 \right)^{1/3} \left( \frac{1}{p} \sum_{z} \left| \sum_{x} \chi(z) \right|^6 \right)^{1/3}.
\]
Thus,
\[W \leq W_1^{1/3} \cdot W_2^{1/3} \cdot W_3^{1/3},
\]
where $W_j$ is the number of solutions of the congruence
\[xyz \equiv x'y'z' \pmod{p}, \quad x, y, z, x', y', z' \in \mathcal{I}_j.
\]
According to Theorem 2 for each given triple $(x', y', z')$ there are at most $|\mathcal{I}_j|^{o(1)}$ possibilities for $(x, y, z)$. Thus, we have that $W_i \leq |\mathcal{I}_j|^{3+o(1)}$. Therefore,
\[W \leq (|\mathcal{I}_1| \cdot |\mathcal{I}_2| \cdot |\mathcal{I}_3|)^{1+o(1)}.
\]
Now, using the well known relationship between the cardinality of a product set and the number of solutions of the corresponding equation, we get
\[|\mathcal{I}_1 \cdot \mathcal{I}_2 \cdot \mathcal{I}_3| \geq \frac{|\mathcal{I}_1|^2 \cdot |\mathcal{I}_2|^2 \cdot |\mathcal{I}_3|^2}{W} \geq (|\mathcal{I}_1| \cdot |\mathcal{I}_2| \cdot |\mathcal{I}_3|)^{1-o(1)}
\]
and the result follows.

6 Conjectures and Open problems

We conclude our paper with several conjectures and open problems.

Conjecture 1. For $M < p^{1/2}$ one has $I_2(M; K, L) < M^{o(1)}$

Conjecture 2. For $M < p^{1/3}$ one has $I_3(M; L) < M^{o(1)}$

Conjecture 3. For $M < p^{1/2}$ one has $J_a(M; K, L) < M^{o(1)}$. 

11
Conjecture 4. Let $I_1, I_2, I_3$ be intervals in $\mathbb{F}_p^*$ of length $|I_i| < p^{1/3}$. Then

$$|I_1 \cdot I_2 \cdot I_3| = (|I_1| \cdot |I_2| \cdot |I_3|)^{1-o(1)}.$$

Problem 1. From Theorem $\square$ it follows that if if $M < p^{1/4}$, then $I_2(M; K, L) < M^{o(1)}$. Improve the exponent $1/4$ to a larger constant.

Problem 2. From Theorem $\square$ it follows that if $M < p^{1/3}$, then $I_2(M; L, L) < M^{o(1)}$. Improve the exponent $1/3$ to a larger constant.

Problem 3. Theorem $\square$ claims that if $M < p^{1/8}$, then $I_3(M; L) < M^{o(1)}$. Improve the exponent $1/8$ to a larger constant.

References

[1] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory 1 (2005), 1-32.

[2] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Philos. Soc. 146 (2009), 1-21.

[3] T. H. Chan and I. Shparlinski, *On the concentration of points on modular hyperbolas and exponential curves*, Acta Arithmetica 142, no. 1 (2010) 59-66.

[4] J. Cilleruelo and J. Jiménez, *The hyperbola $xy = N$*, Journal of Théorie des Nombres of Bordeaux, vol 12, no. 1 (2000).

[5] M. Garaev, *On the logarithmic factor in error term estimates in certain additive congruence problems*, Acta Arithmetica 124, n 1 (2006) 27-39.

[6] D. R. Heath-Brown, *Almost-primes in arithmetic progressions and short intervals*, Math. Proc. Cambridge Philos. Soc. **83** (1978), no. 3, 357–375.