



CLOSE POINTS ON A MODULAR HYPERBOLA

Tsz Ho Chan

Department of Mathematics, Kennesaw State University, Marietta, Georgia

tchan4@kennesaw.edu

*Received: 6/4/25, Accepted: 12/1/25, Published: 9/28/26***Abstract**

In this paper, we continue the study of small squares containing two points of a modular hyperbola $xy \equiv c \pmod{p}$. We deduce a lower bound for its side length. Analogous to the study of smooth gaps between primes, we investigate what happens if the “distances” between two such points are smooth numbers, squarefree numbers, or primes, as well as in more general multiplicatively closed sets or almost dense sets.

– *Dedicated to Melvyn Nathanson and Carl Pomerance on their 80th birthday*

1. Introduction and Main Results

Let $p > 2$ be a prime number and c be any integer such that $\gcd(c, p) = 1$. Our main object of study is the modular hyperbola:

$$\mathcal{H}_p^c := \{(x, y) : xy \equiv c \pmod{p}\}.$$

We exclude $p = 2$ as the modular hyperbola $xy \equiv 1 \pmod{2}$ has only one point. Many people have studied the distribution of points on $\mathcal{H}_p^c$ using exponential, Kloosterman or character sum methods. Igor Shparlinski [12] wrote a very nice survey on the subject. Recently, the author [3] considered small squares in the plane

$$B_{X,Y}(H) := \{(x, y) : x \equiv X + i \pmod{p}, y \equiv Y + j \pmod{p} \text{ for some } 0 \leq i, j \leq H\}$$

containing two points on $\mathcal{H}_p^c$. It was proved that, given any $\epsilon > 0$ and any $\gcd(c, p) = 1$, there exists a constant $C_\epsilon > 0$ such that $H = C_\epsilon p^{1/4+\epsilon}$ is sufficient to give

$$|\mathcal{H}_p^c \cap B_{X,Y}(H)| \geq 2 \text{ for some } 0 \leq X, Y \leq p-1. \quad (1)$$

Moreover, the author drew a connection with the least positive quadratic non-residue $n_p \pmod{p}$, namely, for some constant $C_\epsilon > 0$, either

$$|\mathcal{H}_p^c \cap B_{X,Y}(C_\epsilon p^{1/6+\epsilon})| \geq 2 \text{ for some } 0 \leq X, Y \leq p-1,$$

or

$$n_p \leq C_\epsilon p^{1/(6\sqrt{\epsilon})+\epsilon}.$$

The above results bear some resemblance to the study of gaps between primes or other interesting arithmetic sequences. For example, Baker, Harman and Pintz [1] proved the existence of two primes in short intervals $[x, x + x^{21/40}]$ for sufficiently large x . Also, there have been much recent research activities on small and large gaps between consecutive primes, most noticeably [14], [10], [5], [11], and [6]. Here, we show that there is some gap between points on modular hyperbolas.

Theorem 1. *There exist infinitely many prime numbers $p \equiv 1 \pmod{4}$ such that, for some integer c_p with $\gcd(c_p, p) = 1$, we have*

$$|\mathcal{H}_p^{c_p} \cap B_{X,Y}(\sqrt{\lfloor 0.1 \log p \rfloor})| \leq 1$$

for all $0 \leq X, Y \leq p - 1$.

In response to a question posted by Kevin D. Boklan, Balog, Brüdern, and Wooley [2] studied smooth gaps between prime numbers. This was improved recently by Carol Wu [13] through the use of the Maynard-Tao sieve. Thus, we are interested in studying smooth (and other interesting types of) “gaps” or “distances” between close points on modular hyperbolas.

Question 1. Given any infinite set $\mathcal{A}$ of positive integers, what is the smallest H that guarantees the existence of $h, k \in \mathcal{A} \cap [1, H]$ such that

$$(x + h, y + k) \in \mathcal{H}_p^c \quad \text{for some } (x, y) \in \mathcal{H}_p^c ?$$

We present some results in this direction. First, we need some definitions.

Definition 1. A set $\mathcal{A}$ is *multiplicatively closed* if $a \cdot b \in \mathcal{A}$ whenever $a, b \in \mathcal{A}$.

Definition 2. An infinite set $\mathcal{A}$ of positive integers has *positive lower density* $\delta > 0$ if

$$\sum_{a \in \mathcal{A} \cap [1, X]} 1 \geq \delta X$$

for all sufficiently large X .

Definition 3. An infinite set $\mathcal{A}$ of positive integers is “almost dense” if, for any $\epsilon > 0$, there exists a constant $c_{\epsilon, \mathcal{A}} > 0$ such that

$$|\{X \leq n \leq 2X : n \in \mathcal{A}\}| \geq c_{\epsilon, \mathcal{A}} X^{1-\epsilon}$$

for all sufficiently large X (in terms of ϵ).

Theorem 2. *For any real number $\epsilon > 0$, prime number $p > 2$, and integer c with $\gcd(c, p) = 1$, let $\mathcal{M}$ be a multiplicative closed set with positive lower density δ . Then there exists a constant $C_{\delta, \epsilon} > 0$ such that*

$$(x + h, y + k) \in \mathcal{H}_p^c$$

for some $(x, y) \in \mathcal{H}_p^c$ and some $h, k \in \mathcal{M} \cap [1, C_{\delta, \epsilon} p^{1/4} \exp((\log p)^{1/2+\epsilon})]$.

Recall that an integer is y -smooth if all of its prime factors are less than or equal to y . It is well-known that p^ϵ -smooth numbers have positive density in intervals $[1, p^C]$ for any fixed $C > 0$. Thus, Theorem 2 applies to p^ϵ -smooth “distances” h, k , and improves on the previous result $H = C_\epsilon p^{1/4+\epsilon}$. Although squarefree numbers are not multiplicatively closed, we have a similar result.

Theorem 3. *For any real number $\epsilon > 0$, prime number $p > 2$, and integer c with $\gcd(c, p) = 1$, let $\mathcal{S}$ be the set of squarefree numbers. Then there exists a constant $C_\epsilon > 0$ such that*

$$(x + h, y + k) \in \mathcal{H}_p^c$$

for some $(x, y) \in \mathcal{H}_p^c$ and some $h, k \in \mathcal{S} \cap [1, C_\epsilon p^{1/4} \exp((\log p)^{1/2+\epsilon})]$.

Note: In Theorem 3, one can restrict h to be a prime number and k to be a product of two distinct prime numbers.

Theorem 4. *Given any real number $\epsilon > 0$, prime number $p > 2$, and integer c with $\gcd(c, p) = 1$, we have that for any “almost dense” set of positive integers $\mathcal{A}$, there exists a constant $C_{\epsilon, \mathcal{A}} > 0$ such that*

$$(x + h, y + k) \in \mathcal{H}_p^c$$

for some $(x, y) \in \mathcal{H}_p^c$ and some $h, k \in \mathcal{A} \cap [1, C_{\epsilon, \mathcal{A}} p^{11/34+\epsilon}]$.

Thus, Theorem 4 applies to prime “distances” h, k for example. The readers are encouraged to study other interesting integer “distances” or consider rectangles instead of squares.

The paper is organized as follows. First, we transform the problem into a character sum problem as in [3]. Then we prove Theorem 1 using Weil’s bound on character sums. Next, we prove Theorems 2 and 3 using Burgess’ method. Finally, we prove Theorem 4 by a double character sum estimate of Chang [4].

Throughout the paper, the symbol $|\mathcal{A}|$ stands for the cardinality of a set $\mathcal{A}$. The floor function $\lfloor x \rfloor$ denotes the largest integer less than or equal to x . We use $\exp(x)$ to denote the function e^x . When an integer a divides another integer b , we abbreviate that as $a \mid b$. Given a prime p and $\gcd(n, p) = 1$, we use $\bar{n}$ to denote the multiplicative inverse of $n \pmod{p}$ (i.e., $n \cdot \bar{n} \equiv 1 \pmod{p}$). The symbols $f(x) = O(g(x))$, $f(x) \ll g(x)$, and $g(x) \gg f(x)$ are equivalent to $|f(x)| \leq Cg(x)$ for some constant $C > 0$. Also, the symbols $f(x) = O_{\lambda_1, \dots, \lambda_r}(g(x))$, $f(x) \ll_{\lambda_1, \dots, \lambda_r} g(x)$, and $g(x) \gg_{\lambda_1, \dots, \lambda_r} f(x)$ mean that the implicit constant may depend on the parameters $\lambda_1, \dots, \lambda_r$.

2. Some Preliminaries

Suppose (x, y) and $(x + h, y + k)$ are two points on $\mathcal{H}_p^c$ for some $1 \leq h, k \leq H$. We have $(x + h)(y + k) \equiv xy \equiv c \pmod{p}$, which is equivalent to

$$\begin{cases} kx^2 + hc + hcx \equiv 0 \pmod{p}, \\ xy \equiv c \pmod{p}. \end{cases}$$

After completing the square of the first equation above, we get $(2kx + hc)^2 \equiv h^2k^2 - 4hkc \pmod{p}$. Hence, Equation (1) can be reduced to finding $1 \leq h, k \leq H$ such that

$$\left(\frac{hk(hk - 4c)}{p}\right) = 1 \quad \text{or} \quad \left(\frac{k}{p}\right)\left(\frac{k - 4c\bar{h}}{p}\right) = 1. \quad (2)$$

Here, $(\frac{\cdot}{p})$ is the Legendre symbol modulo p . Note that if h and k satisfy Equation (2), we can reverse the above process to find x and, hence, the two points (x, y) and $(x + h, y + k)$ on $\mathcal{H}_p^c$. A key tool we need is Weil's bound on character sums (see Theorem 11.23 in [8] for example).

Theorem 5 ([8]). *Let χ be a non-principal multiplicative character modulo p of order $d > 1$. Suppose $f \in \mathbb{F}_p[x]$ has m distinct roots and f is not a d -th power. Then, we have*

$$\left| \sum_{x \in \mathbb{F}_p} \chi(f(x)) \right| \leq (m - 1)\sqrt{p}. \quad (3)$$

3. Proof of Theorem 1

Proof. Suppose $p \equiv 1 \pmod{4}$. We want to find $L/4 < c < p - L/4$ such that

$$\left(\frac{l - 4c}{p}\right) = \left(\frac{l + 4c}{p}\right) = -1 \quad \text{for all } 1 \leq l \leq L \quad (4)$$

with some positive integer $L < n_p \ll p^{1/2} \log p$ by the Pólya–Vinogradov inequality. It then follows that

$$\left(\frac{hk}{p}\right)\left(\frac{hk - 4c}{p}\right) = -1 \quad \text{for all } 1 \leq |h|, |k| \leq \sqrt{L}.$$

This together with Equations (1) and (2) implies that $|\mathcal{H}_p^c \cap B(X, Y, \sqrt{L})| \leq 1$ for all $0 \leq X, Y \leq p - 1$. To deduce Equation (4), we consider the sum

$$\Sigma := \sum_{L/4 < c < p - L/4} \prod_{k=1}^L \left(\frac{1 - (\frac{k-4c}{p})}{2}\right) \cdot \prod_{l=1}^L \left(\frac{1 - (\frac{l+4c}{p})}{2}\right).$$

Note that the contribution from the missing terms $1 \leq c \leq L/4$ and $p - L/4 \leq c \leq p$ is at most L . Inserting these missing terms, expanding things out, and applying Equation (3), we get

$$\begin{aligned} \Sigma &= \frac{p}{2^{2L}} + \frac{1}{2^{2L}} \sum_{\substack{0 \leq r, s \leq L \\ r+s > 0}} (-1)^{r+s} \sum_{1 \leq k_1 < k_2 < \dots < k_r \leq L} \sum_{1 \leq l_1 < l_2 < \dots < l_s \leq L} \\ &\quad \sum_{c=1}^p \left(\frac{4c - k_1}{p} \right) \dots \left(\frac{4c - k_r}{p} \right) \cdot \left(\frac{4c + l_1}{p} \right) \dots \left(\frac{4c + l_s}{p} \right) + O(L) \\ &= \frac{p}{2^{2L}} + O(2^{2L} L p^{1/2}) \geq \frac{p}{2^{2L+1}} \geq p^{0.7} \end{aligned}$$

with $L = \lfloor 0.1 \log p \rfloor$ when p is sufficiently large. This shows that Equation (4) holds for some $L/4 < c < p - L/4$. Finally, we have $n_p \gg \log p \cdot \log \log \log p > L$ for infinitely many primes $p \equiv 1 \pmod{4}$ by a result of Graham and Ringrose [7]. Hence, we have Theorem 1. $\square$

4. Proof of Theorem 2

Proof of Theorem 2. Set

$$H := p^{1/4} \exp(0.5(\log p)^{1/2+\epsilon}), \quad T := \exp(0.25(\log p)^{1/2+\epsilon})(\log p)^{1/2-\epsilon}, \quad K := HT.$$

We want to find integers $h \in \mathcal{M} \cap [1, H]$ and $k \in \mathcal{M} \cap [1, K]$ satisfying

$$\left(\frac{k}{p} \right) \left(\frac{k - 4c\bar{h}}{p} \right) = 1. \quad (5)$$

Let $\mathcal{Q}_p$ be the set of quadratic residues modulo p . By the pigeonhole principle and the positive lower density of $\mathcal{M}$, we have

$$\left| [1, T] \cap \mathcal{Q}_p \right| \geq \frac{\delta T}{2} \quad \text{or} \quad \left| [1, T] \setminus \mathcal{Q}_p \right| \geq \frac{\delta T}{2}.$$

The larger of these two sets we denote by $\mathcal{Z}_0$. Next, we choose

$$\mathcal{A} = \mathcal{Z}_1 = \{1 \leq z_1 \leq H : z_1 \in \mathcal{M}\}.$$

Then $|\mathcal{A}|, |\mathcal{Z}_1| \geq \delta H$ by the positive lower density of $\mathcal{M}$.

Suppose Equation (5) is false for all numbers $h \in \mathcal{M} \cap [1, H]$ and $k \in \mathcal{M} \cap [1, K]$. We restrict our attention to $k = z_0 z_1$ where $z_0 \in \mathcal{Z}_0$ and $z_1 \in \mathcal{Z}_1$. Let r_{4c} denote the remainder of $4c$ after division by p . Then we have

$$\left(\frac{z_0 z_1}{p} \right) \left(\frac{z_0 z_1 - 4c\bar{h}}{p} \right) = 0 \quad \text{or} \quad \left(\frac{z_0 z_1}{p} \right) \left(\frac{z_0 z_1 - 4c\bar{h}}{p} \right) = -1. \quad (6)$$

The first case in Equation (6) consists of those tuples (h, z_0, z_1) with $hz_0z_1 = r_{4c}$ since $hz_0z_1 < p$. Apart from these tuples, the second case in Equation (6) yields

$$\left(\frac{z_0 - 4c\overline{hz_1}}{p}\right) = -\left(\frac{z_0}{p}\right)$$

which has the same value by the definition of $\mathcal{Z}_0$. Consequently, we have

$$S := \left| \sum_{\substack{h \in \mathcal{A} \\ z_0 \in \mathcal{Z}_0, z_1 \in \mathcal{Z}_1}} \left(\frac{z_0 - 4c\overline{hz_1}}{p}\right) \right| = |\mathcal{A}||\mathcal{Z}_0||\mathcal{Z}_1| - d_3(r_{4c}) \gg |\mathcal{A}||\mathcal{Z}_0||\mathcal{Z}_1| \gg_\delta H^2 T. \quad (7)$$

Here $d_3(n)$ stands for the number of ways to write n as a product of 3 positive integers, and we have the standard divisor bound $d_3(n) \ll n^{0.1}$ for example. Let

$$w(n) := \#\{(h, z_1) \in \mathcal{A} \times \mathcal{Z}_1 : hz_1n \equiv 4c \pmod{p}\}.$$

Clearly, we have $\sum_{n=1}^{p-1} w(n) = |\mathcal{A}||\mathcal{Z}_1|$. Define

$$W := \sum_{n=1}^{p-1} w(n)^2 = \#\{(h_1, h_2, z_1, z_2) : h_1, h_2 \in \mathcal{A}, z_1, z_2 \in \mathcal{Z}_1, h_1z_1 = h_2z_2\}.$$

Given h_1 and h_2 , any z_1 determines z_2 uniquely and vice versa. Also, observe that $\frac{h_1}{\gcd(h_1, h_2)}z_1 = \frac{h_2}{\gcd(h_1, h_2)}z_2$ which implies

$$\frac{h_1}{\gcd(h_1, h_2)} \Big| z_2 \quad \text{and} \quad \frac{h_2}{\gcd(h_1, h_2)} \Big| z_1.$$

Thus, we have

$$W = \sum_{h_1 \leq h_2 \in \mathcal{A}} \sum_{\substack{z_1 \in \mathcal{Z}_1 \\ \frac{h_2}{\gcd(h_1, h_2)} \Big| z_1}} 1 + \sum_{h_2 < h_1 \in \mathcal{A}} \sum_{\substack{z_2 \in \mathcal{Z}_1 \\ \frac{h_1}{\gcd(h_1, h_2)} \Big| z_2}} 1 =: W_1 + W_2.$$

By $\sum_{m \leq x, d|m} 1 \leq \frac{x}{d}$ and $\sum_{n \leq x} d(n) \ll x \log x$, we obtain

$$\begin{aligned} W_1 &\leq \sum_{h_1 \leq h_2 \in \mathcal{A}} \frac{H}{h_2 / \gcd(h_1, h_2)} \leq H \sum_{h_2 \in \mathcal{A}} \frac{1}{h_2} \sum_{\delta|h_2} \delta \sum_{h_1 \leq h_2, \delta|h_1} 1 \leq H \sum_{h_2 \in \mathcal{A}} d(h_2) \\ &\ll H^2 \log H. \end{aligned} \quad (8)$$

We have similar bounds for W_2 and W . By Hölder's inequality, Equations (8) and

(3), we get

$$\begin{aligned}
 S &= \left| \sum_n w(n) \sum_{z_0 \in \mathcal{Z}_0} \left(\frac{z_0 - n}{p} \right) \right| \\
 &\leq \left(\sum_n w(n)^{\frac{2R}{2R-1}} \right)^{\frac{2R-1}{2R}} \left(\sum_n \left(\sum_{z_0 \in \mathcal{Z}_0} \left(\frac{z_0 - n}{p} \right) \right)^{2R} \right)^{\frac{1}{2R}} \\
 &= \left(\sum_n w(n)^{\frac{2R}{2R-1}} \right)^{\frac{2R-1}{2R}} \left(\sum_{z_1, z_2, \dots, z_{2R} \in \mathcal{Z}_0} \sum_n \left(\frac{n - z_1}{p} \right) \left(\frac{n - z_2}{p} \right) \cdots \left(\frac{n - z_{2R}}{p} \right) \right)^{\frac{1}{2R}} \\
 &\leq \left(\sum_n w(n) \right)^{\frac{2R-2}{2R}} \left(\sum_n w(n)^2 \right)^{\frac{1}{2R}} \cdot \left(\frac{(2R)!}{2^R R!} |\mathcal{Z}_0|^R p + 2R |\mathcal{Z}_0|^{2R} \sqrt{p} \right)^{\frac{1}{2R}} \\
 &\ll (H^2)^{\frac{2R-2}{2R}} (H^2 \log H)^{\frac{1}{2R}} \cdot \left(\sqrt{R} \sqrt{T} \cdot p^{\frac{1}{2R}} + T \cdot (\sqrt{p})^{\frac{1}{2R}} \right). \tag{9}
 \end{aligned}$$

The term $\frac{(2R)!}{2^R R!} |\mathcal{Z}_0|^R p$ comes from the diagonal contributions when $z_1, z_2, \dots, z_{2R}$ can be partitioned into R distinct pairs z_i, z_j with $z_i = z_j$. Pick

$$R = \lfloor 2(\log p)^{1/2-\epsilon} + 1 \rfloor$$

and recall $T = \exp(0.25(\log p)^{1/2+\epsilon})(\log p)^{1/2-\epsilon}$. One can check that

$$T \cdot (\sqrt{p})^{\frac{1}{2R}} \gg_{\epsilon} \sqrt{R} \sqrt{T} p^{\frac{1}{2R}}.$$

Hence, Equation (9) yields

$$S \ll_{\epsilon} H^2 T \cdot \left(\frac{H^2}{p^{1/2} \log H} \right)^{-\frac{1}{2R}},$$

contradicting Equation (7) as $H = p^{1/4} \exp(0.5(\log p)^{1/2+\epsilon})$. This proves the existence of some solution to Equation (5), and hence completes the proof. $\square$

5. Proof of Theorem 3

Proof of Theorem 3. Since this proof is very similar to that of Theorem 2, we will highlight the necessary modifications only. We use the same choices for H and T but set $K := 2H \cdot T$. Let $\mathcal{P}$ be the set of prime numbers and

$$\mathcal{A} := \{1 \leq h \leq H : h \in \mathcal{P}\}.$$

We have $|\mathcal{A}| \gg H/\log H$ by Chebyshev's estimate. By the pigeonhole principle, we have

$$\left| \{1 \leq z_0 \leq T : z_0 \in \mathcal{P}\} \cap \mathcal{Q}_p \right| \gg \frac{T}{\log T} \quad \text{or} \quad \left| \{1 \leq z_0 \leq T : z_0 \in \mathcal{P}\} \setminus \mathcal{Q}_p \right| \gg \frac{T}{\log T},$$

and we let $\mathcal{Z}_0$ be the bigger of these two sets. Finally, set

$$\mathcal{Z}_1 := \{H < z_1 \leq 2H : z_1 \in \mathcal{P}\}$$

and $|\mathcal{Z}_1| \gg H/\log H$. Suppose Equation (5) is false for all squarefree numbers $1 \leq h \leq H$ and $1 \leq k = z_0 z_1 \leq K$. Then

$$\left(\frac{z_0 - 4ch\overline{z_1}}{p}\right) = -\left(\frac{z_1}{p}\right)$$

have the same value for all $h \in \mathcal{A}$, $z_0 \in \mathcal{Z}_0$, $z_1 \in \mathcal{Z}_1$ apart from those tuples (h, z_0, z_1) for which $hz_0 z_1 = r_{4c}$. Similar to Equation (7), we have

$$S := \left| \sum_{\substack{h \in \mathcal{A} \\ z_0 \in \mathcal{Z}_0, z_1 \in \mathcal{Z}_1}} \left(\frac{z_0 - 4ch\overline{z_1}}{p}\right) \right| \gg |\mathcal{A}| |\mathcal{Z}_0| |\mathcal{Z}_1| \gg \frac{H^2}{\log^2 H} \cdot \frac{T}{\log T}. \quad (10)$$

Recall that

$$w(n) = \#\{(h, z_1) \in \mathcal{A} \times \mathcal{Z}_1 : h z_1 n \equiv 4c \pmod{p}\},$$

and

$$\begin{aligned} W &= \sum_{n=1}^{p-1} w(n)^2 = \#\{(h_1, h_2, z_1, z_2) : h_1, h_2 \in \mathcal{A}, z_1, z_2 \in \mathcal{Z}_1, h_1 z_1 = h_2 z_2\} \\ &= \sum_{z_1 = z_2 \in \mathcal{Z}_1} \sum_{h_1 = h_2 \in \mathcal{A}} 1 \ll \frac{H^2}{\log^2 H}. \end{aligned}$$

Then, following the same argument as in Theorem 2, we obtain

$$S \ll_{\epsilon} \left(\frac{H^2}{\log^2 H}\right)^{\frac{2R-2}{2R}} \left(\frac{H^2}{\log^2 H}\right)^{\frac{1}{2R}} \cdot \frac{T}{\log T} \cdot (\sqrt{p})^{\frac{1}{2R}} \ll \frac{H^2}{\log^2 H} \cdot \frac{T}{\log T} \cdot \left(\frac{H^2}{\sqrt{p} \log^2 H}\right)^{-\frac{1}{2R}}$$

which contradicts Equation (10) with our choice of H . This completes the proof. $\square$

6. Proof of Theorem 4

Proof of Theorem 4. Karatsuba [9] studied double character sums and proved that, for some given $\epsilon > 0$, there exists $\epsilon' = \epsilon'(\epsilon) > 0$ such that

$$\sum_{x \in I} \left| \sum_{y \in S} \chi(y+x) \right| < p^{-\epsilon'} |I| |S| \quad (11)$$

for any interval $I \subseteq [1, p]$ with $|I| = p^{\beta}$ and any arbitrary subset $S \subseteq [1, p]$ with $|S| = p^{\alpha}$ satisfying

$$\alpha, \beta > \epsilon \quad \text{and} \quad \alpha + 2\beta > 1 + \epsilon. \quad (12)$$

Mei-Chu Chang [4] improved Equation (12) to

$$\epsilon < \beta \leq \frac{1}{k} \quad \text{and} \quad \left(1 - \frac{2}{3k}\right)\alpha + \frac{2}{3}\left(1 + \frac{2}{k}\right)\beta > \frac{1}{2} + \frac{1}{3k} + \epsilon \quad (13)$$

for any $\epsilon > 0$ and any integer $k > 0$.

Set $\alpha = \beta = 11/34 + \epsilon$. One can check that Equation (13) is satisfied with $k = 3$. Let $\mathcal{A}_\alpha = \mathcal{A} \cap [1, p^\alpha]$. By Equation (11), we have

$$\begin{aligned} \left| \sum_{k, h \in \mathcal{A}_\alpha} \left(\frac{k}{p}\right) \left(\frac{k - 4c\bar{h}}{p}\right) \right| &\leq \sum_{k \in \mathcal{A}_\alpha} \left| \sum_{h \in \mathcal{A}_\alpha} \left(\frac{k - 4c\bar{h}}{p}\right) \right| \\ &\leq \sum_{k \leq p^\alpha} \left| \sum_{h \in \mathcal{A}_\alpha} \left(\frac{-4c\bar{h} + k}{p}\right) \right| < p^{\alpha - \epsilon'} |\mathcal{A}_\alpha|. \end{aligned} \quad (14)$$

If $\left(\frac{k}{p}\right) \left(\frac{k - 4c\bar{h}}{p}\right) \neq 1$ for all $h, k \in \mathcal{A}_\alpha$, then $\left(\frac{k}{p}\right) \left(\frac{k - 4c\bar{h}}{p}\right) = 0$ for at most $|\mathcal{A}_\alpha|$ of the h 's, and the rest satisfy $\left(\frac{k}{p}\right) \left(\frac{k - 4c\bar{h}}{p}\right) = -1$. Thus, Equation (14) implies

$$|\mathcal{A}_\alpha|^2 - |\mathcal{A}_\alpha| < p^{\alpha - \epsilon'} |\mathcal{A}_\alpha|,$$

which contradicts

$$|\mathcal{A}_\alpha| \geq c_{\epsilon'/2, \mathcal{A}} \cdot p^{\alpha - \epsilon'/2}$$

as $\mathcal{A}_\alpha$ is “almost dense”. Therefore, $\left(\frac{k}{p}\right) \left(\frac{k - 4c\bar{h}}{p}\right) = 1$ for some $h, k \in \mathcal{A}_\alpha$ and hence, Theorem 4 is true. $\square$

Acknowledgement. The author would like to thank the anonymous referee for helpful suggestions.

References

- [1] R.C. Baker, G. Harman, and J. Pintz, The difference between consecutive primes, II, *Proc. London Math. Soc.* **83** (3) (2001), 532-562.
- [2] A. Balog, J. Brüdern, and T.D. Wooley, On smooth gaps between consecutive prime numbers, *Mathematika* **46** (1) (1999), 57-75.
- [3] T.H. Chan, Shortest distance in modular hyperbola and least quadratic non-residue, *Mathematika* **62** (2016), 860-865.
- [4] M.C. Chang, On a question of Davenport and Lewis and new character sum bounds in finite fields, *Duke Math. J.* **145** (3) (2008), 409-442.
- [5] K. Ford, B. Green, S. Konyagin, and T. Tao, Large gaps between consecutive prime numbers, *Ann. of Math.* **183** (2016), 935-974.

- [6] K. Ford, B. Green, S. Konyagin, J. Maynard, and T. Tao, Long gaps between primes, *J. Amer. Math. Soc.* **31** (1) (2018), 65-105.
- [7] S.W. Graham and C.J. Ringrose, Lower Bounds for Least Quadratic Non-Residues. In: *Berndt, B.C., Diamond, H.G., Halberstam, H., Hildebrand, A. (eds) Analytic Number Theory, Progress in Mathematics, vol 85*, Birkhäuser Boston, MA, 1990, pp. 269-309.
- [8] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, Providence, 2004.
- [9] A.A. Karatsuba, Distribution of values of Dirichlet characters on additive sequences, *Soviet Math. Dokl.* **44** (1) (1992), 145-148.
- [10] J. Maynard, Small gaps between primes, *Ann. of Math.* **181** (2015), 383-413.
- [11] J. Maynard, Large gaps between primes, *Ann. of Math.* **183** (2016), 915-933.
- [12] I.E. Shparlinski, Modular hyperbolas, *Japan J. Math.* **7** (2012), 235-294.
- [13] C. Wu, On smooth gaps between primes using the Maynard-Tao sieve, *Integers* **25** (2025), #A44, 6 pp.
- [14] Y. Zhang, Bounded gaps between primes, *Ann. of Math.* **179** (2014), 1121-1174.