ACTA ARITHMETICA
142.1 (2010)

On the concentration of points on modular hyperbolas and exponential curves

by

Tsz Ho Chan (Memphis, TN) and Igor E. Shparlinski (Sydney)

1. Introduction. For a prime p and an arbitrary integer a with $\gcd(a,p) = 1$, we consider the following set of points (x,y) on the modular hyperbola:

$$\mathcal{H}_{a,p} = \{(x,y) : xy \equiv a \pmod p\}.$$

There is an extensive literature where various questions concerning the distribution of points of $\mathcal{H}_{a,p}$ are studied (see the survey [14] and references therein). In particular, for a positive integer $H < p$ and arbitrary integers K and L, we denote by $N_{a,p}(H;K,L)$ the number of points $(x,y) \in \mathcal{H}_{a,p}$ which belong to the square $[K+1,K+H]\times[L+1,L+H]$. Using a standard technique and the Weil bound on incomplete Kloosterman sums one can easily obtain the asymptotic formula

$$N_{a,p}(H;K,L) = H^2/p + O(p^{1/2}(\log p)^2), \tag{1}$$

which has been slightly improved by Garaev [8].

We remark that (1) implies that $N_{a,p}(H;K,L) = (1+o(1))H^2/p$ if $Hp^{-3/4}(\log p)^{-1} \to \infty$ as $p \to \infty$ and also gives a nontrivial upper bound $N_{a,p}(H;K,L) = o(H)$ if $Hp^{-1/2}(\log p)^{-2} \to \infty$ and $H = o(p)$ as $p \to \infty$. These results seem to be the limit of what can be achieved within the standard exponential sum techniques and currently available estimates on incomplete Kloosterman sums. Here we show that a variant of the celebrated result of Bourgain, Katz & Tao [4] on the sum-product problem in finite fields, which is given by Bourgain [1, Theorem 4.1], allows us to obtain an upper bound on $N_{a,p}(H;K,L)$ which is nontrivial for any $H = o(p)$.

Furthermore, for a prime p, and arbitrary integers a and g with $\gcd(ag,p) = 1$, we consider the following set of points (x,y) on the modular exponential curves:

$$\mathcal{E}_{a,g,p} = \{(x,y) : y \equiv ag^x \pmod p\}.$$

2010 *Mathematics Subject Classification*: 11A07, 11B75, 11T23.
Key words and phrases: modular hyperbola, modular exponential curve, sum-product estimates, concentration function.

DOI: 10.4064/aa142-1-5

Accordingly, for a positive integer $H < p$ and arbitrary integers K and L, we denote by $M_{a,g,p}(H; K, L)$ the number of points $(x, y) \in \mathcal{E}_{a,g,p}$ which belong to the square $[K+1, K+H] \times [L+1, L+H]$. For $M_{a,g,p}(H; K, L)$ one has a full analogue of (1). More precisely, for $H \le t$, where t is the multiplicative order of g modulo p,

$$M_{a,g,p}(H; K, L) = H^2/p + O(p^{1/2}(\log p)^2). \tag{2}$$

Here we also obtain an upper bound $M_{a,g,p}(H; K, L)$, which is also non-trivial for any $H = o(t)$. In fact, in this case we are in the setting of the traditional sum-product problem and can use explicit estimates of Bourgain & Garaev [3], Garaev [9] and Katz & Shen [11] to get a more explicit estimate on $M_{a,g,p}(H; K, L)$ than the one we obtain for $N_{a,p}(H; K, L)$.

Although the proofs of our bounds are very simple, it seems that techniques from additive combinatorics have never been applied to questions of this kind. So, we hope this link may lead to some other new results.

We note that our results have a natural interpretation of upper bounds on the *concentration functions* of points on $\mathcal{H}_{a,p}$ and $\mathcal{E}_{a,g,p}$.

Finally, we discuss some possible ways to improve our results and further applications.

Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may occasionally depend, where obvious, on the parameter ε, but are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \le cV$ holds with some constant $c > 0$.

2. Sum-product and sum-reciprocal sum problems. Let $\mathbb{F}_p$ denote the finite field of p elements. For a set $\mathcal{A} \subseteq \mathbb{F}_p^*$ and a rational function $F(X_1, \dots, X_m) \in \mathbb{F}_p(X_1, \dots, X_m)$, we define the set

$$F(\mathcal{A}, \dots, \mathcal{A}) = \{F(a_1, \dots, a_m) : a_1, \dots, a_m \in \mathcal{A}\}.$$

We also use $E(\mathcal{A})$ to denote the *multiplicative energy* of $\mathcal{A}$, that is,

$$E(\mathcal{A}) = |\{(a_1, a_2, a_3, a_4) : a_1 a_2 = a_3 a_4,\ a_1, a_2, a_3, a_4 \in \mathcal{A}\}|.$$

Our bound on $N_{a,p}(H; K, L)$ depends on the following estimate of Bourgain [1, Theorem 4.1].

LEMMA 1. *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any set $\mathcal{A} \subseteq \mathbb{F}_p^*$ of cardinality $|\mathcal{A}| \le p^{1-\varepsilon}$,*

$$\max\{|\mathcal{A} + \mathcal{A}|, |\mathcal{A}^{-1} + \mathcal{A}^{-1}|\} \gg |\mathcal{A}|^{1+\delta}.$$

To estimate $M_{a,g,p}(H; K, L)$, we recall the following explicit version of the sum-product result of Bourgain, Katz & Tao [4], which is due to Bourgain & Garaev [3, Theorem 1.1].

LEMMA 2. *For any set* $\mathcal{A} \subseteq \mathbb{F}_p^*$,

$$E(\mathcal{A})^4 \ll \left(|\mathcal{A}-\mathcal{A}| + \frac{|\mathcal{A}|^3}{p}\right)|\mathcal{A}|^5|\mathcal{A}-\mathcal{A}|^4|\mathcal{A}+\mathcal{A}-\mathcal{A}-\mathcal{A}|(\log(|\mathcal{A}|+2))^4.$$

We also remark that by the Cauchy–Schwarz inequality,

$$E(\mathcal{A}) \ge \frac{|\mathcal{A}|^4}{|\mathcal{A}\cdot\mathcal{A}|}. \tag{3}$$

3. Main results. Here we show how Lemmas 1 and 2 imply upper bounds on $N_{a,p}(H;K,L)$ and $M_{a,g,p}(H;K,L)$, respectively.

THEOREM 3. *There exists some absolute constant* $\eta > 0$ *such that for any positive integer* $H < p$*, uniformly over arbitrary integers* K *and* L*, we have*

$$N_{a,p}(H;K,L) \ll H^2/p + H^{1-\eta}.$$

Proof. For large values of H, namely for $H \ge p^{2/3}$, the result is immediate from (1).

For small values of H, namely for $H < p^{2/3}$, we consider the set $\mathcal{A}$ of smallest nonnegative residues modulo p of $x \in [K+1, K+H]$ such that a times the inverse of x modulo p is congruent to some integer in the interval $[L+1, L+H]$.

Clearly,

$$|\mathcal{A}+\mathcal{A}| \le 2H \quad \text{and} \quad |\mathcal{A}^{-1}+\mathcal{A}^{-1}| \le 2H.$$

Applying Lemma 1 with $\varepsilon = 1/3$ we see that for some absolute constant $\delta > 0$ we have

$$H \gg |\mathcal{A}|^{1+\delta},$$

which concludes the proof. ∎

THEOREM 4. *For any positive integer* $H \le t$*, where* t *is the multiplicative order of* g *modulo* p*, uniformly over arbitrary integers* K *and* L*, we have*

$$M_{a,g,p}(H;K,L) \ll \max\{H^{10/11+o(1)}, H^{9/8+o(1)}p^{-1/8}\}$$

as $H \to \infty$.

Proof. We consider the set $\mathcal{A}$ of smallest nonnegative residues modulo p of $y \in [L+1, L+H]$ such that y is congruent to ag^x modulo p for some integer x in the interval $[K+1, K+H]$.

Clearly,

$$|\mathcal{A}-\mathcal{A}| \le 2H, \quad |\mathcal{A}\cdot\mathcal{A}| \le 2H, \quad |\mathcal{A}+\mathcal{A}-\mathcal{A}-\mathcal{A}| \le 4H.$$

Applying Lemma 2, we obtain

$$E(\mathcal{A})^4 \ll (H + |\mathcal{A}|^3/p)|\mathcal{A}|^5H^5(\log(H+2))^4,$$

while the bound (3) now implies

$$E(\mathcal{A}) \gg \frac{|\mathcal{A}|^4}{H}.$$

Comparing the previous estimates, we derive

$$|\mathcal{A}|^{11} \ll (H + |\mathcal{A}|^3/p)H^9(\log(H+2))^4$$

and the result follows. ∎

COROLLARY 5. *For any positive integers $H \le t$, where t is the multiplicative order of g modulo p, uniformly over arbitrary integers K and L, we have*

$$M_{a,g,p}(H; K, L) \ll H^2/p + H^{10/11+o(1)}$$

as $H \to \infty$.

Proof. For large values of H, namely for $H > p^{5/9}$, we deduce from (2) that

$$M_{a,g,p}(H; K, L) \ll H^2/p + p^{1/2}(\log p)^2 \le H^2/p + H^{9/10+o(1)}, \tag{4}$$

since $p < H^{9/5}$.

For small values of H, namely for $H \le p^{5/9}$, we have

$$H^{9/8}p^{-1/8} \le H^{9/10} \le H^{10/11}$$

and the result now follows from Theorem 4. ∎

4. Comments. It seems to be quite feasible to obtain an explicit form of Lemma 1 of the same type as Lemma 2, and thus obtain a concrete value of η in the bound of Theorem 3. Furthermore, for large sets $\mathcal{A} \subseteq \mathbb{F}_p^*$, the method of Garaev [9] gives such a bound right away:

$$|\mathcal{A} + \mathcal{A}|\,|\mathcal{A}^{-1} + \mathcal{A}^{-1}| \gg \min\left\{p|\mathcal{A}|, \frac{|\mathcal{A}|^4}{p}\right\}. \tag{5}$$

To establish (5) we first estimate exponential sums

$$S_{\lambda,p}(\mathcal{U}, \mathcal{V}) = \sum_{u\in\mathcal{U}} \sum_{\substack{v\in\mathcal{V}\\ v\ne u}} \mathbf{e}_p(\lambda(u-v)^{-1}),$$

where $\mathbf{e}_p(z) = \exp(2\pi i z/p)$, for any two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p$. We have

$$|S_{\lambda,p}(\mathcal{U}, \mathcal{V})| = \left| \sum_{t=1}^{p-1} \mathbf{e}_p(\lambda t^{-1}) \frac{1}{p} \sum_{b=0}^{p-1} \sum_{u\in\mathcal{U}} \sum_{\substack{v\in\mathcal{V}\\ v\ne u}} \mathbf{e}_p(b(t-u+v)) \right|$$

$$= \left| \frac{1}{p} \sum_{b=0}^{p-1} \sum_{t=1}^{p-1} \sum_{u\in\mathcal{U}} \sum_{v\in\mathcal{V}} \mathbf{e}_p(b(t-u+v) + \lambda t^{-1}) \right|$$

as the contribution from $v = u$ to the sum is

$$\sum_{b=0}^{p-1}\sum_{t=1}^{p-1} \mathbf{e}_p(bt + \lambda t^{-1}) = \sum_{t=1}^{p-1} \mathbf{e}_p(\lambda t^{-1}) \sum_{b=0}^{p-1} \mathbf{e}_p(bt) = 0.$$

Hence,

$$|S_{\lambda,p}(\mathcal{U},\mathcal{V})| \le \frac{1}{p}\sum_{b=0}^{p-1} \Big| \sum_{u\in\mathcal{U}} \mathbf{e}_p(bu)\Big| \Big| \sum_{v\in\mathcal{V}} \mathbf{e}_p(bv)\Big| \Big| \sum_{t=1}^{p-1} \mathbf{e}_p(bt + \lambda t^{-1})\Big|.$$

Now, using the Weil bound on Kloosterman sums (see [10, Theorem 11.11]) for the sum over t, and applying the Cauchy–Schwarz inequality to the sum over u and v, we obtain

$$\begin{aligned} |S_{\lambda,p}(\mathcal{U},\mathcal{V})| &\ll \frac{1}{p^{1/2}} \Big(\sum_{b=0}^{p-1} \Big| \sum_{u\in\mathcal{U}} \mathbf{e}_p(bu)\Big|^2\Big)^{1/2} \Big(\sum_{b=0}^{p-1} \Big| \sum_{v\in\mathcal{V}} \mathbf{e}_p(bv)\Big|^2\Big)^{1/2} \\ &= \frac{1}{p^{1/2}} \, (p|\mathcal{U}|)^{1/2} (p|\mathcal{V}|)^{1/2} = \sqrt{p|\mathcal{U}|\,|\mathcal{V}|} \end{aligned} \tag{6}$$

provided that $\gcd(\lambda, p) = 1$.

We now mimic the argument of Garaev [9] and consider the equation

$$a_1^{-1} + (b - a_2)^{-1} = c, \quad (a_1, a_2, b, c) \in \mathcal{A}\times\mathcal{A}\times\mathcal{B}\times\mathcal{C}, \tag{7}$$

where

$$\mathcal{B} = \mathcal{A} + \mathcal{A} \quad \text{and} \quad \mathcal{C} = \mathcal{A}^{-1} + \mathcal{A}^{-1}.$$

Let J be the number of solutions to (7).

For any triple $(a_1, a_2, a_3) \in \mathcal{A}\times\mathcal{A}\times\mathcal{A}$, we see that the vector

$$(a_1, a_2, a_2 + a_3, a_1^{-1} + a_3^{-1})$$

is a solution to (7), and different triples (a_1, a_2, a_3) give different solutions. Therefore

$$J \ge |\mathcal{A}|^3. \tag{8}$$

We can also express J via exponential sums

$$J = \sum_{a_1\in\mathcal{A}} \sum_{a_2\in\mathcal{A}} \sum_{\substack{b\in\mathcal{B}\\ b\ne a_2}} \sum_{c\in\mathcal{C}} \frac{1}{p} \sum_{\lambda=0}^{p-1} \mathbf{e}_p(\lambda(a_1^{-1} + (b - a_2)^{-1} - c)).$$

Changing the order of summation, separating the term $|\mathcal{A}|^2|\mathcal{B}|\,|\mathcal{C}|/p$ corresponding to $\lambda = 0$ and recalling (8), we obtain

$$|\mathcal{A}|^3 \le \frac{|\mathcal{A}|^2|\mathcal{B}|\,|\mathcal{C}|}{p} + \frac{1}{p}\sum_{\lambda=1}^{p-1} |S_{\lambda,p}(\mathcal{A},\mathcal{B})| \Big| \sum_{a_1\in\mathcal{A}} \sum_{c\in\mathcal{C}} \mathbf{e}_p(\lambda(a_1^{-1} - c))\Big|.$$

By (6) we obtain

$$|\mathcal{A}|^3 \ll \frac{|\mathcal{A}|^2|\mathcal{B}|\,|\mathcal{C}|}{p} + |\mathcal{A}|^{1/2}|\mathcal{B}|^{1/2}p^{-1/2}\sum_{\lambda=1}^{p-1}\Big|\sum_{a_1\in\mathcal{A}}\mathbf{e}_p(\lambda a_1^{-1})\Big|\,\Big|\sum_{c\in\mathcal{C}}\mathbf{e}_p(\lambda c)\Big|. \tag{9}$$

Applying the Cauchy–Schwarz inequality to the sum over λ, as in (6), we obtain the inequality

$$\sum_{\lambda=1}^{p-1}\Big|\sum_{a_1\in\mathcal{A}}\mathbf{e}_p(\lambda a_1^{-1})\Big|\,\Big|\sum_{c\in\mathcal{C}}\mathbf{e}_p(\lambda c)\Big| \le p\sqrt{|\mathcal{A}|\,|\mathcal{C}|},$$

which after inserting into (9) implies (5).

Note that the bound (5) is optimal when $|\mathcal{A}| > p^{2/3}$. In particular, take $N = [\sqrt{pH}]$. By the pigeon-hole principle, there is some k with $1 \le k \le p/N$ such that the set

$$\mathcal{A}_k = \{a \in [(k-1)N, kN] : a \equiv b^{-1} \pmod p \text{ for some } b \in [1, N]\}$$

has cardinality $|\mathcal{A}| \gg N^2/p \gg H$ while

$$|\mathcal{A}+\mathcal{A}|, |\mathcal{A}^{-1}+\mathcal{A}^{-1}| \le 2N \ll \sqrt{pH}.$$

Hence $|\mathcal{A}+\mathcal{A}|\,|\mathcal{A}^{-1}+\mathcal{A}^{-1}| \ll pH \ll p|\mathcal{A}|$.

The bound (5) can now be used in the scheme of the proof of Theorem 3 (and it leads to a nontrivial upper bound on $N_{a,p}(H; K, L)$), however it does not seem to improve the bound which follows from (1) (we also note that it is easy to get a version of (1) that gives the same upper bound but without $(\log p)^2$ in the error term). It seems that in order to be useful, a version of (5) is needed which is nontrivial for smaller sets $\mathcal{A}$ (of cardinality $|\mathcal{A}| = o(p^{1/2})$). Furthermore, one easily notices that in the scheme of the proof of Theorem 3 the set $\mathcal{A}+\mathcal{A}^{-1}$ can be used instead of $\mathcal{A}^{-1}+\mathcal{A}^{-1}$. Similarly, the set $\mathcal{A}-\mathcal{A}$ can be used instead of $\mathcal{A}+\mathcal{A}$. Thus it is enough to obtain an explicit lower bound on

$$\max\{|\mathcal{A}+\mathcal{A}|, |\mathcal{A}-\mathcal{A}|, |\mathcal{A}^{-1}+\mathcal{A}^{-1}|, |\mathcal{A}+\mathcal{A}^{-1}|\}.$$

Furthermore, one can consider longer expressions of the form

$$a_1 \pm \cdots \pm a_k \pm a_{k+1}^{-1} \pm \cdots \pm a_{k+m}^{-1}, \qquad a_1, \ldots, a_{k+m} \in \mathcal{A},$$

and try to show that at least one of them generates a sufficiently large set.

Probably using the extension of the result of Bourgain & Garaev [3], given by Shen [13], one can study the concentration function of solutions to some other congruences.

Another possible direction of research is to study the concentration functions of points on the multidimensional generalisations of $\mathcal{H}_{a,p}$ such as

$$\{(x, y_1, \ldots, y_s) : (x + j)y_j \equiv a_j \pmod p,\ j = 1, \ldots, s\},$$

see [7] for some results for the case $s = 2$, $a_1 = a_2 = 1$; or

$$\{(x_1, \ldots, x_s) : x_1 \ldots x_s \equiv a \pmod p\},$$

see [15, 16, 17], where multiplicative character sums are shown to be a more appropriate tool to study such sets for $s \geq 3$.

Multidimensional analogues of the set $\mathcal{E}_{a,g,p}$, such as

$$\{(x, y_1, \ldots, y_s) : y_j \equiv a_j g_j^x \pmod p,\ j = 1, \ldots, s\},$$

are also of interest.

Finally, we remark that using the technique introduced in [12] and then refined in [6] (see also [2, 5]) one can obtain results about the distribution of residues of g^x which go beyond the results of the type of (2). However, this technique has only been developed in the case when x runs through the full period $x = 1, \ldots, t$, where, as before, t is the multiplicative order of g modulo p. It is certainly an interesting question to extend these results to the case of x running through shorter intervals of length $H < t$ and obtain new upper bounds on $M_{a,g,p}(H; K, L)$. It is not clear whether this technique may lead to new results on $N_{a,p}(H; K, L)$ but this is definitely worth studying.

Acknowledgements. The authors would like to thank the referee for useful comments leading to the improvement of the bound in (5). The second author was supported in part by ARC grant DP0556431.

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, K. Ford, S. V. Konyagin and I. E. Shparlinski, *On the divisibility of Fermat quotients*, preprint, 2008, 21 pp.

[3] 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.

[4] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields and applications*, Geom. Funct. Anal. 14 (2004), 27–57.

[5] J. Bourgain, S. V. Konyagin, C. Pomerance and I. E. Shparlinski, *On the smallest pseudopower*, Acta Arith. 140 (2009), 43–55.

[6] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, *Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm*, Int. Math. Res. Notices 2008, art. ID rnn090, 29 pp.; corrigenda, ibid. 2009, no. 16, 3146–3147.

[7] T. H. Chan, *Distribution of difference between inverses of consecutive integers modulo p*, Integers 4 (2004), A3, 11 pp.
[8] M. Z. Garaev, *On the logarithmic factor in error term estimates in certain additive congruence problems*, Acta Arith. 124 (2006), 27–39.
[9] —, *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc. 136 (2008), 2735–2739.
[10] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.
[11] N. H. Katz and C.-Y. Shen, *A slight improvement to Garaev's sum product estimate*, Proc. Amer. Math. Soc. 136 (2008), 2499–2504.
[12] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge Univ. Press, Cambridge, 1999.
[13] C.-Y. Shen, *An extension of Bourgain and Garaev's sum-product estimates*, Acta Arith. 135 (2008), 351–356.
[14] I. E. Shparlinski, *Distribution of points on modular hyperbolas*, in: Sailing on the Sea of Number Theory, Proc. 4th China-Japan Seminar on Number Theory, Weihai, 2006, World Sci., 2007, 155–189.
[15] —, *On the distribution of points on multidimensional modular hyperbolas*, Proc. Japan Acad. Ser. A Math. Sci. 83 (2007), no. 2, 5–9.
[16] —, *On a generalisation of a Lehmer problem*, Math. Z. 263 (2009), 619–631.
[17] I. E. Shparlinski and A. Winterhof, *Visible points on multidimensional modular hyperbolas*, J. Number Theory 128 (2008), 2695–2703.

Tsz Ho Chan
Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152, U.S.A.
E-mail: tchan@memphis.edu

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
E-mail: igor@comp.mq.edu.au

Received on 7.4.2009
and in revised form on 11.6.2009 (5997)