BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 56, No. 1, 2008

NUMBER THEORY

On the Euler Function on Differences Between the Coordinates of Points on Modular Hyperbolas

by

Igor E. SHPARLINSKI

Presented by Andrzej SCHINZEL

Summary. For a prime $p > 2$, an integer a with $\gcd(a, p) = 1$ and real $1 \le X, Y < p$, we consider the set of points on the modular hyperbola

$$\mathcal{H}_{a,p}(X, Y) = \{(x, y) : xy \equiv a \pmod p,\ 1 \le x \le X,\ 1 \le y \le Y\}.$$

We give asymptotic formulas for the average values

$$\sum_{\substack{(x,y)\in\mathcal{H}_{a,p}(X,Y)\\ x\ne y}} \frac{\varphi(|x-y|)}{|x-y|} \quad \text{and} \quad \sum_{\substack{(x,y)\in\mathcal{H}_{a,p}(X,X)\\ x\ne y}} \varphi(|x-y|)$$

with the Euler function $\varphi(k)$ on the differences between the components of points of $\mathcal{H}_{a,p}(X, Y)$.

1. Introduction. For a prime $p > 2$, an integer a with $\gcd(a, p) = 1$ and real X and Y with $1 \le X, Y < p$ we consider the set

$$\mathcal{H}_{a,p}(\mathcal{B}) = \mathcal{H}_{a,p} \cap \mathcal{B}$$

of points on the modular hyperbola

$$\mathcal{H}_{a,p} = \{(x, y) : xy \equiv a \pmod p,\ 1 \le x < p,\ 1 \le y < p\}.$$

inside of the half-open box

$$\mathcal{B} = [U, U + X) \times [V, V + Y) \tag{1}$$

with some integers $0 \le U < U + X \le p$, $0 \le V < V + Y \le p$.

Various properties, such as largest value and the number of distinct values, of the differences $x - y$ for points $(x, y) \in \mathcal{H}_{a,p}(\mathcal{B})$ have recently been considered (see [2, 4, 6] and references therein).

2000 *Mathematics Subject Classification*: 11A07, 11K38, 11N25.
Key words and phrases: modular hyperbola, Euler function, discrepancy.

Here we continue to investigate arithmetic properties of these differences and obtain asymptotic formulas for the average values

$$S_{a,p}(\mathcal{B}) = \sum_{\substack{(x,y)\in\mathcal{H}_{a,p}(\mathcal{B})\\ x\neq y}} \frac{\varphi(|x-y|)}{|x-y|} \quad \text{and} \quad T_{a,p}(\mathcal{B}) = \sum_{\substack{(x,y)\in\mathcal{H}_{a,p}(\mathcal{B})\\ x\neq y}} \varphi(|x-y|)$$

where, as usual, $\varphi(k)$ denotes the Euler function of $k \geq 1$.

We remark that it would be interesting to extend our results to solutions of congruences $xy \equiv a \pmod m$ modulo arbitrary integers m, as well as to solutions of more general polynomial congruences. It seems that both such extensions need some additional ideas.

Throughout the paper, all the implied constants are absolute.

2. Background on the discrepancy. Let $\mathcal{I}$ be the family of half-open aligned boxes $I = [0,\alpha) \times [0,\beta) \subseteq [0,1)^2$. For a set $W \subseteq [0,1)^2$ of N points we define the *discrepancy* as

$$D(W) = \sup_{I\in\mathcal{I}} \left| \frac{\#(W \cap I)}{N} - |I| \right|$$

where $|I| = \alpha\beta$ is the area of I.

We use the *Erdős–Turán–Koksma inequality* (see [1, Theorem 1.21]) for the discrepancy of a set of points of $[0,1)^2$, which we present in the following form.

LEMMA 1. *For any integer $L \geq 1$, for the discrepancy of a set*

$$W = \{(u_1, v_1), \ldots, (u_N, v_N)\} \subseteq [0,1)^2$$

of N points the bound

$$D(W) = O\left(\frac{1}{L} + \frac{1}{N} \sum_{0<|r|+|s|\leq L} \frac{1}{(|r|+1)(|s|+1)} \left|\sigma_{r,s}(W)\right|\right)$$

holds, where the sum is taken over all integer points $(r,s) \in \mathbb{Z}^2$ with $0 < |r| + |s| \leq L$ and

$$\sigma_{r,s}(W) = \sum_{n=1}^{N} \exp\left(2\pi i(ru_n + sv_n)\right).$$

3. Sum $S_{a,p}(\mathcal{B})$

THEOREM 2. *For $\gcd(a,p) = 1$ and a box $\mathcal{B}$ given by (1), we have*

$$S_{a,p}(\mathcal{B}) = \frac{6}{\pi^2}\,\frac{XY}{p} + O(p^{1/2}(\log p)^2 + \min\{X,Y\}p^{-1/4}\log p).$$

Proof. Without loss of generality we assume that $X \le Y$.

We recall that

$$\frac{\varphi(k)}{k} = \sum_{d|k} \frac{\mu(d)}{d},$$

where $\mu(d)$ is the Möbius function (see [3, Equation (1.36)]).

Therefore,

$$S_{a,p}(\mathcal{B}) = \sum_{\substack{(x,y)\in\mathcal{H}_{a,p}(\mathcal{B})\\ x\ne y}} \sum_{d|x-y} \frac{\mu(d)}{d} = \sum_{d=1}^{p} \frac{\mu(d)}{d}\, N_{a,p}(d,\mathcal{B}), \tag{2}$$

where

$$N_{a,p}(d,\mathcal{B}) = \sum_{\substack{(x,y)\in\mathcal{H}_{a,p}(\mathcal{B})\\ d|x-y\\ x\ne y}} 1.$$

Writing $y = x + zd$ we see that $N_{a,p}(d,\mathcal{B})$ is the number of solutions (x,z) to the congruence

$$x(x+dz) \equiv a \pmod p \tag{3}$$

with

$$U \le x < U + X \quad \text{and} \quad \frac{V-x}{d} \le z < \frac{V+Y-x}{d}. \tag{4}$$

We fix some positive integer K, put $Z = X/K$ and split the interval $[U, U+X)$ into K smaller intervals

$$J_k = [(k-1)Z, kZ),$$

where $k = 1, \dots, K$.

Let $N_{a,p}(k,d,\mathcal{B})$ be the number of solutions to (3) with

$$x \in J_k \quad \text{and} \quad \frac{V-x}{d} \le z < \frac{V+Y-x}{d}.$$

Thus

$$N_{a,p}(d,\mathcal{B}) = \sum_{k=1}^{K} N_{a,p}(k,d,\mathcal{B}). \tag{5}$$

Moreover,

$$L_{a,p}(k,d,\mathcal{B}) \le N_{a,p}(k,d,\mathcal{B}) \le U_{a,p}(k,d,\mathcal{B}), \tag{6}$$

where $L_{a,p}(k,d,\mathcal{B})$ and $U_{a,p}(k,d,\mathcal{B})$ are the numbers of solutions to (3) with

$$x \in J_k \quad \text{and} \quad \frac{V-(k-1)Z}{d} \le z < \frac{V+Y-kZ}{d}$$

and

$$x \in J_k \quad \text{and} \quad \frac{V - kZ}{d} \le z < \frac{V + Y - (k-1)Z}{d},$$

respectively.

Let W be the set of fractions $(x/p, z/p)$ taken over all solutions (x, z) to (3) with $0 \le x, z < p$. We note that (3) can be written as

$$z \equiv d^{-1}(ax^{-1} - x) \pmod p.$$

Clearly the rational functions $f(x) = x$ and $g(x) = d^{-1}(ax^{-1} - x)$ are linearly independent modulo p. Hence the Weil bound on Kloosterman sums (see [3, Theorem 11.11]) applies to their nontrivial linear combinations modulo p, that is, we have

$$\sum_{x=1}^{p-1} \exp\left(2\pi i \, \frac{rx + sd^{-1}(ax^{-1} - x)}{p}\right) = \sum_{x=1}^{p-1} \exp\left(2\pi i \, \frac{(r - d^{-1}s)x + ad^{-1}sx^{-1}}{p}\right) = O(p^{1/2})$$

uniformly over all integers r and s with $\gcd(r, s, p) = 1$. Hence, by Lemma 1, we get the bound $D(W) = O(p^{-1/2}(\log p)^2)$ on the discrepancy of W.

Therefore,

$$L_{a,p}(k, d, \mathcal{B}) = \frac{(Y - Z)Z}{dp} + O(p^{1/2}(\log p)^2),$$
$$U_{a,p}(k, d, \mathcal{B}) = \frac{(Y + Z)Z}{dp} + O(p^{1/2}(\log p)^2).$$

Substituting these bounds in (6), we get

$$N_{a,p}(k, d, \mathcal{B}) = \frac{YZ}{dp} + O(p^{1/2}(\log p)^2 + Z^2 d^{-1} p^{-1}) = \frac{XY}{Kdp} + O(p^{1/2}(\log p)^2 + X^2 K^{-2} d^{-1} p^{-1}).$$

Thus, from (5), we get

$$N_{a,p}(d, \mathcal{B}) = \frac{XY}{dp} + O(Kp^{1/2}(\log p)^2 + X^2 K^{-1} d^{-1} p^{-1}).$$

We now put $K = \lceil Xp^{-3/4} d^{-1/2} (\log p)^{-1} \rceil$, which leads to the bound

$$N_{a,p}(d, \mathcal{B}) = \frac{XY}{dp} + O(p^{1/2}(\log p)^2 + Xp^{-1/4} d^{-1/2} \log p).$$

Finally, using (2), we deduce

$$\begin{aligned} S_{a,p}(\mathcal{B}) &= \frac{XY}{p}\sum_{d=1}^{p}\frac{\mu(d)}{d^2} + O\left(p^{1/2}(\log p)^2\sum_{d=1}^{p}\frac{1}{d} + Xp^{-1/4}\log p\sum_{d=1}^{p}\frac{1}{d^{3/2}}\right) \\ &= \frac{XY}{p}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + O\left(p^{1/2}(\log p)^3 + Xp^{-1/4}\log p\right) \\ &= \zeta^{-1}(2)\,\frac{XY}{p} + O(p^{1/2}(\log p)^3 + Xp^{-1/4}\log p) \\ &= \frac{6}{\pi^2}\,\frac{XY}{p} + O(p^{1/2}(\log p)^3 + Xp^{-1/4}\log p), \end{aligned}$$

where $\zeta(s)$ is the Riemann zeta-function (see [3, Equation (1.15)]). ∎

COROLLARY 3. *For* $\gcd(a,p)=1$ *and a box* $\mathcal{B}$ *given by* (1), *we have*

$$S_{a,p}(\mathcal{B}) = \frac{6}{\pi^2}\frac{XY}{p} + O(X^{1/2}Y^{1/2}p^{-1/4}(\log p)^{3/2}).$$

Proof. Since $\#\mathcal{H}_{a,p}(\mathcal{B}) = XY/p + O\left(p^{1/2}(\log p)^2\right)$ (which can be derived similarly to the bounds on $L_{a,p}(k,d,\mathcal{B})$ and $U_{a,p}(k,d,\mathcal{B})$ in the proof of Theorem 2) we see that for $XY \le p^{3/2}(\log p)^3$ the result is trivial. Assuming that $XY > p^{3/2}(\log p)^3$ and also using the inequalities

$$\min\{X,Y\} \le X^{1/2}Y^{1/2} \le X^{1/2}Y^{1/2}(\log p)^{1/2},$$

we see that

$$p^{1/2}(\log p)^3 + Xp^{-1/4}\log p = O(X^{1/2}Y^{1/2}p^{-1/4}(\log p)^{3/2}),$$

which concludes the proof. ∎

4. Sum $T_{a,p}(\mathcal{B})$. For simplicity we only consider the case $U = V = 0$ and $X = Y$, that is, when $\mathcal{B}$ is a cube with the origin as one of the vertices. The general case can be considered along the same lines, but the elementary part of evaluation of the main term becomes more tedious and leads to a more cluttered expression.

THEOREM 4. *For* $\gcd(a,p)=1$ *and a box* $\mathcal{B}$ *given by* (1) *with* $U = V = 0$ *and* $X = Y$, *we have*

$$T_{a,p}(\mathcal{B}) = \frac{2}{\pi^2}\,\frac{X^3}{p} + O(X^{8/3}p^{-3/4}(\log p)^{1/2}).$$

Proof. We fix some positive integer K, put $Z = X/K$ and split $\mathcal{B}$ into K^2 smaller aligned cubes

$$\mathcal{B}_{h,k} = [(h-1)Z, hZ) \times [(k-1)Z, kZ),$$

where $h, k = 1, \ldots, K$. In particular,

$$T_{a,p}(\mathcal{B}) = \sum_{h,k=1}^{K} T_{a,p}\left(\mathcal{B}_{h,k}\right). \tag{7}$$

For $(x, y) \in \mathcal{B}_{h,k}$, we have

$$x - y = hZ - kZ + O(Z) = (h-k)Z + O(Z).$$

Thus, applying Corollary 2, we derive

$$\begin{aligned}
T_{a,p}(\mathcal{B}_{h,k}) &= \sum_{\substack{(x,y)\in\mathcal{H}_{a,p}\left(\mathcal{B}_{h,k}\right)\\ x\neq y}} \frac{\varphi(|x-y|)}{|x-y|}|x-y| \\
&= (|h-k|Z + O(Z))S_{a,p}(\mathcal{B}_{h,k}) \\
&= (|h-k|Z + O(Z))\left(\frac{6}{\pi^2}\frac{Z^2}{p} + O(Xp^{-1/4}(\log p)^{3/2})\right) \\
&= \frac{6}{\pi^2}\frac{|h-k|Z^3}{p} + O(Z^3p^{-1} + X^2p^{-1/4}(\log p)^{3/2}).
\end{aligned}$$

Substituting this bound in (7), we obtain

$$\begin{aligned}
T_{a,p}(\mathcal{B}) &= \frac{6}{\pi^2}\frac{Z^3}{p}\sum_{h,k=1}^{K}|h-k| + O(K^2Z^3p^{-1} + X^2p^{-1/4}(\log p)^{3/2}) \\
&= \frac{12}{\pi^2}\frac{Z^3}{p}\sum_{h=1}^{K}\sum_{k=1}^{h-1}(h-k) + O(X^3K^{-1}p^{-1} + K^2X^2p^{-1/4}(\log p)^{3/2}) \\
&= \frac{6}{\pi^2}\frac{Z^3}{p}\sum_{h=1}^{K}h(h-1) + O(X^3K^{-1}p^{-1} + K^2X^2p^{-1/4}(\log p)^{3/2}) \\
&= \frac{2}{\pi^2}\frac{Z^3}{p}(K^3 + O(K^2)) + O(X^3K^{-1}p^{-1} + K^2X^2p^{-1/4}(\log p)^{3/2}) \\
&= \frac{2}{\pi^2}\frac{X^3}{p} + O(X^3K^{-1}p^{-1} + K^2X^2p^{-1/4}(\log p)^{3/2}).
\end{aligned}$$

Taking $K = \lceil X^{1/3}p^{-1/4}(\log p)^{-1/2}\rceil$, we conclude the proof. ∎

5. Final remarks. It is clear that Theorems 2 and 4 are nontrivial whenever $XY \geq p^{3/2+\varepsilon}$ and $X \geq p^{3/4+\varepsilon}$, respectively, where $\varepsilon > 0$ is arbitrary and p is large enough. We remark that beyond this range even that $\mathcal{H}_{a,p}(\mathcal{B}) \neq \emptyset$ is unknown (see [4]) and thus it can be hard to improve the range of applicability of Theorems 2 and 4 without getting principally new insight on the distribution of points on $\mathcal{H}_{a,p}$. On the other hand, it is quite

possible that using the approach of [5] one can get better results "on average" over a.

Studying average values of other arithmetic functions on the points of $\mathcal{H}_{a,p}(\mathcal{B})$ is of interest as well. For example, it would be interesting to obtain bounds or asymptotic formulas for the sums

$$\sum_{(x,y)\in\mathcal{H}_{a,p}(\mathcal{B})} \mu(xy), \qquad \sum_{(x,y)\in\mathcal{H}_{a,p}(\mathcal{B})} \left(\frac{x}{y}\right), \qquad \sum_{(x,y)\in\mathcal{H}_{a,p}(\mathcal{B})} \omega(|x-y|),$$

where $\mu(k)$ is the Möbius function, (k/m) is the *Jacobi symbol* of k modulo m, which we also extend to even values of m by simply putting $(k/m) = 0$, and $\omega(k)$ is the number of distinct prime divisors of k.

References

[1] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications*, Springer, Berlin, 1997.

[2] K. Ford, M. R. Khan, I. E. Shparlinski and C. L. Yankov, *On the maximal difference between an element and its inverse in residue rings*, Proc. Amer. Math. Soc. 133 (2005), 3463–3468.

[3] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

[4] M. R. Khan and I. E. Shparlinski, *On the maximal difference between an element and its inverse modulo n*, Period. Math. Hungar. 47 (2003), 111–117.

[5] I. E. Shparlinski, *Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average*, Michigan Math. J., to appear.

[6] I. E. Shparlinski and A. Winterhof, *Distances between the points on modular hyperbolas*, J. Number Theory, to appear.

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

Received December 31, 2007 (7635)