BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 54, No. 3-4, 2006

NUMBER THEORY

Primitive Points on a Modular Hyperbola

by

Igor E. SHPARLINSKI

Presented by Andrzej SCHINZEL

Summary. For positive integers m, U and V, we obtain an asymptotic formula for the number of integer points $(u,v) \in [1,U] \times [1,V]$ which belong to the modular hyperbola $uv \equiv 1 \pmod m$ and also have $\gcd(u,v) = 1$, which are also known as primitive points. Such points have a nice geometric interpretation as points on the modular hyperbola which are "visible" from the origin.

1. Introduction. For a positive integer m we consider the *modular hyperbola*

$$\mathcal{H}_m = \{(u,v) : uv \equiv 1 \pmod m,\ 1 \le u,v < m\}.$$

Various properties of the points $(u,v) \in \mathcal{H}_m$ have been considered in the literature. For example,

- the question about the joint distribution of parity of u and v is known as the *Lehmer problem* and has attracted a lot of attention (see [27]–[29]);
- the distribution of the distances $|u - v|$ for $(u,v) \in \mathcal{H}_m$ has been addressed in the literature as well (see [5, 14, 30]);
- some geometric properties of the convex hull of $\mathcal{H}_m$ have been studied in [15].

Here we consider an apparently new question of estimating the number of points $(u,v) \in \mathcal{H}_m$ with $\gcd(u,v) = 1$ which belong to a given box $(u,v) \in [1,U] \times [1,V]$. These points have an attractive geometric interpretation as points on $\mathcal{H}_m$ which are "visible" from the origin (see [2, 12, 18, 26] and references therein for several other aspects of distribution of "visible" points in various regions).

2000 *Mathematics Subject Classification*: 11A07, 11K38, 11L40.
Key words and phrases: modular hyperbola, primitive point.
This work was supported in part by ARC grant DP0556431.

More precisely, for positive real numbers U and V we consider the set

$$\mathcal{H}_m(U,V) = \{(u,v) \in \mathcal{H}_m : 1 \le u \le U,\ 1 \le v \le V\}$$

and we define

$$N_m(U,V) = \sum_{\substack{(u,v)\in\mathcal{H}_m(U,V)\\ \gcd(u,v)=1}} 1.$$

We obtain an asymptotic formula for $N_m(U,V)$ which is nontrivial whenever

$$UV \ge m^{3/2+\varepsilon} \tag{1}$$

for any fixed $\varepsilon > 0$ and sufficiently large m.

We recall that the notations $U \ll V$ and $U = O(V)$ are both equivalent to the statement that $|U| \le cV$ with some constant $c > 0$. Throughout the paper, $o(1)$ denotes a quantity which tends to zero as $m \to \infty$.

2. Preparation. We need the following bound on the distribution of inverses of squares in residue rings which could be of independent interest.

For an integer d with $\gcd(d,m) = 1$, we use $\overline{d}$ to denote the modular inverse of d modulo m, that is, $d\overline{d} \equiv 1 \pmod m$, $1 \le \overline{d} < m$.

For a real R and integers K and L with $1 \le K, R < m$ we denote by $T_m(R;K,L)$ the number of integers $d \in [L, L+K-1]$ with $\gcd(d,m) = 1$ and such that $\overline{d^2} \equiv r \pmod m$ for some integer r with $1 \le r \le R$.

Lemma 1. *For any real R and integers K and L with $1 \le K, R < m$, we have*

$$T_m(R;K,L) = \frac{R}{m} \sum_{\substack{d=L\\ \gcd(d,m)=1}}^{L+K-1} 1 + O(m^{1/2+o(1)}).$$

Proof. The proof uses very standard arguments so we give only the main ingredients.

Our basic ingredient is the following bound on complete exponential sums:

$$\max_{b=1,\dots,m} \Bigg| \sum_{\substack{d=1\\ \gcd(d,m)=1}}^{m} \exp\left(2\pi i\, \frac{a\overline{d^2} + bd}{m}\right)\Bigg| \le (m\gcd(a,m))^{1/2+o(1)},$$

which holds for any integer a and is a very special case of the more general bound of [20] for exponential sums with monomials. Now, using the standard reduction between complete and incomplete sums (see [13, Section 12.2]), we obtain

$$\Bigg| \sum_{\substack{d=L\\ \gcd(d,m)=1}}^{L+K-1} \exp\left(2\pi i\, \frac{a\overline{d^2}}{m}\right)\Bigg| \le (m\gcd(a,m))^{1/2+o(1)}.$$

Combining this with the Erdős–Turán inequality (see [17, Corollary 1.1, Chapter 1]), after simple calculations we obtain the desired result. ∎

We also remark that the Weil and Salié bounds of complete Kloosterman sums together imply that

$$\Bigg| \sum_{\substack{u=1\\ \gcd(u,m)=1}}^{m} \exp\left(2\pi i\, \frac{au+b\overline{u}}{m}\right)\Bigg| \le (m\gcd(a,m))^{1/2+o(1)}$$

(see [13, Corollary 11.12]). Now, the above mentioned reduction between complete and incomplete sums (see [13, Section 12.2]) leads to the following well known bound on incomplete Kloosterman sums.

LEMMA 2. *For any integer a and real Z with $1 \le Z \le m$, we have*

$$\sum_{\substack{(u,v)\in\mathcal{H}_m\\ 1\le u\le Z}} \exp\left(2\pi i\, \frac{av}{m}\right) \le (m\gcd(a,m))^{1/2+o(1)}.$$

3. Main result. As usual, $\varphi(m)$ denotes the Euler function.

THEOREM 3. *For all integers m and real U, V with $1 \le U, V < m$, we have*

$$N_m(U,V) = \frac{6}{\pi^2}\cdot\frac{UV}{m}\prod_{p\mid m}\left(1+\frac{1}{p}\right)^{-1} + O(U^{1/2}V^{1/2}m^{-1/4+o(1)}),$$

where the product is taken over all prime numbers $p \mid m$.

Proof. For an integer d, we let

$$M_m(d;U,V) = \sum_{\substack{(u,v)\in\mathcal{H}_m(U,V)\\ d\mid\gcd(u,v)}} 1$$

be the number of pairs $(u,v) \in \mathcal{H}_m(U,V)$ with $d \mid \gcd(u,v)$.

Let $\mu(d)$ denote the Möbius function. We recall that $\mu(1) = 1$, $\mu(d) = 0$ if $d \ge 2$ is not square-free and $\mu(d) = (-1)^{\omega(d)}$ otherwise, where $\omega(d)$ is the number of distinct prime divisors of d. By the inclusion-exclusion principle, we write

$$N_m(U,V) = \sum_{d=1}^{\infty}\mu(d)M_m(d;U,V). \tag{2}$$

Clearly

$$M_m(d;U,V) = 0 \tag{3}$$

if $\gcd(d,m) > 1$ or $d > m$.

For $\gcd(d,m)=1$, writing

$$u = ds \quad \text{and} \quad v = dt, \tag{4}$$

we have

$$M_m(d;U,V) = \#\{(s,t) : st \equiv \overline{d^2} \pmod m,\ 1 \le s \le U/d,\ 1 \le t \le V/d\}$$

where as before, $\overline{d}$ denotes the modular inverse of d modulo m.

Lemma 2, combined with the Erdős–Turán inequality (see [17, Corollary 1.1, Chapter 1]), immediately implies that

$$M_m(d;U,V) = \frac{UV\varphi(m)}{d^2m^2} + O(m^{1/2+o(1)}) \tag{5}$$

(see, for example, [2, Lemma 1.7]; similar results are also obtained in [14, 29]).

We also note that for each d, the product $r = st \le UV/d^2$, where s and t are given by (4), belongs to a fixed residue class modulo m and thus can take at most UV/d^2m+1 possible values. Denoting by $\tau(k)$ the number of positive integer divisors of $k \ge 1$, we see that for each fixed $r \le UV/d^2 \le UV \le m^2$, there are $\tau(r) = m^{o(1)}$ pairs (s,t) of integers s and t with $r = st$ (see [24, Section I.5.2]). Therefore, we also have

$$M_m(d;U,V) \le \left(\frac{UV}{d^2m} + 1\right)m^{o(1)}. \tag{6}$$

Finally, we note that for any integer $\Delta \ge \sqrt{UV/m}$ we have

$$\sum_{2\Delta > d \ge \Delta} M_m(d;U,V) \le T_m(UV/\Delta^2;\Delta,\Delta)m^{o(1)}$$

since $\overline{d^2} \equiv r \pmod m$ where, as before, $r = st \le UV/d^2 \le UV/\Delta^2 \le m$ (thus for every d the value of r is uniquely defined and for every r there are at most $\tau(r) = m^{o(1)}$ possible pairs (s,t)). Therefore,

$$\begin{aligned}\sum_{m \ge d \ge \Delta} M_m(d;U,V) &\le \sum_{\nu=0}^{\lceil 2\log m\rceil} \sum_{2^{\nu+1}\Delta > d \ge 2^\nu\Delta} M_m(d;U,V)\\ &\le \sum_{\nu=0}^{\lceil 2\log m\rceil} T_m(UV/(2^\nu\Delta)^2;2^\nu\Delta,2^\nu\Delta)m^{o(1)}.\end{aligned}$$

Hence, by Lemma 1 we obtain

$$\begin{aligned}\sum_{m \ge d \ge \Delta} M_m(d;U,V) &\le \sum_{\nu=0}^{\lceil 2\log m\rceil} \left(\frac{2^\nu\Delta UV}{(2^\nu\Delta)^2m^{1+o(1)}} + m^{1/2+o(1)}\right)\\ &\ll \frac{UV}{\Delta m^{1+o(1)}} + m^{1/2+o(1)}.\end{aligned} \tag{7}$$

Therefore, for arbitrary integers $\Delta > \delta > 1$, using the asymptotic formula (5) for $d \le \delta$, the bound (6) for $\delta < d \le \Delta$, and the bound (7) for $d \ge \Delta$, we derive from (2) and (3) that

$$N_m(U,V) = \frac{UV\varphi(m)}{m^2} \sum_{\substack{1\le d\le \delta \\ \gcd(d,m)=1}} \frac{\mu(d)}{d^2} + E, \tag{8}$$

where

$$\begin{aligned} E &\ll \delta m^{1/2+o(1)} + \sum_{\delta \le d \le \Delta} \left(\frac{UV}{d^2 m} + 1\right) m^{o(1)} + U^{1/2}V^{1/2}\Delta^{-1} m^{o(1)} \\ &\ll \delta m^{1/2+o(1)} + UV\delta^{-1}m^{-1} + \Delta m^{o(1)} + UV\Delta^{-1}m^{-1}. \end{aligned} \tag{9}$$

We also have

$$\sum_{\substack{1\le d\le \delta \\ \gcd(d,m)=1}} \frac{\mu(d)}{d^2} = \sum_{\substack{d\ge 1 \\ \gcd(d,m)=1}} \frac{\mu(d)}{d^2} + O(\delta^{-1}) = \prod_{p\nmid m}\left(1 - \frac{1}{p^2}\right) + O(\delta^{-1}),$$

where the product is taken over all prime numbers $p \nmid m$. Recalling that

$$\prod_{p}\left(1 - \frac{1}{p^2}\right) = \sum_{d\ge 1} \frac{\mu(d)}{d^2} = \zeta(2)^{-1} = \frac{6}{\pi^2}$$

and

$$\prod_{p\mid m}\left(1 - \frac{1}{p^2}\right) = \prod_{p\mid m}\left(1 - \frac{1}{p}\right)\prod_{p\mid m}\left(1 + \frac{1}{p}\right) = \frac{\varphi(m)}{m}\prod_{p\mid m}\left(1 + \frac{1}{p}\right),$$

we obtain

$$\sum_{\substack{1\le d\le \delta \\ \gcd(d,m)=1}} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}\,\frac{m}{\varphi(m)}\prod_{p\mid m}\left(1 + \frac{1}{p}\right)^{-1} + O(\delta^{-1}). \tag{10}$$

We now substitute (9) and (10) in (8), which yields

$$\begin{aligned} N_m(U,V) = {} & \frac{6}{\pi^2}\cdot\frac{UV}{m}\prod_{p\mid m}\left(1 + \frac{1}{p}\right)^{-1} \\ & + O(\delta m^{1/2+o(1)} + UV\delta^{-1}m^{-1} + \Delta m^{o(1)} + UV\Delta^{-1}m^{-1}). \end{aligned}$$

Taking

$$\delta = \lceil U^{1/2}V^{1/2}m^{-3/4}\rceil \quad \text{and} \quad \Delta = \lceil U^{1/2}V^{1/2}m^{-1/2}\rceil,$$

we derive the desired result. ■

It is easy to see that

$$\prod_{p\mid m}\left(1 + \frac{1}{p}\right) \ll \prod_{p\mid m}\left(1 - \frac{1}{p}\right)^{-1} = \frac{m}{\varphi(m)} \ll \log\log m.$$

In particular, we conclude that Theorem 3 is nontrivial under the condition (1).

Corollary 4. *For all integers m and real U, V with $1 \le U, V < m$ and $UV \ge m^{3/2+\varepsilon}$, we have*

$$N_m(U,V) = \left(\frac{6}{\pi^2} + O(m^{-\varepsilon/2+o(1)})\right)\frac{UV}{m}\prod_{p|m}\left(1+\frac{1}{p}\right)^{-1}.$$

4. Remarks. There is little doubt that our approach can also be used to obtain asymptotic formulas for the sums

$$\sum_{(u,v)\in\mathcal{H}_m(U,V)} |\mu(uv)| \quad \text{and} \quad \sum_{(u,v)\in\mathcal{H}_m(U,V)} |\mu(u)\mu(v)|$$

and several other sums. However, we do not see any approaches to bound the sums

$$\sum_{(u,v)\in\mathcal{H}_m(U,V)} \mu(uv) \quad \text{and} \quad \sum_{(u,v)\in\mathcal{H}_m(U,V)} \left(\frac{u}{v}\right),$$

where (u/v) is the Jacobi symbol, which we also extend to even values of v by putting $(u/v) = 0$ if $\gcd(v,2) = 2$.

Various properties of points on multidimensional hyperbolas

$$u_1 \cdots u_k \equiv 1 \pmod m$$

have been studied as well [1, 21, 22].

Hyperbolas $uv \equiv a \pmod m$ for an arbitrary integer a with $\gcd(a,m) = 1$ are also of interest. Although for every given a their theory is similar to the case $a = 1$, these new settings lead to a new type of problem of getting more precise results on average over a (see [6–10, 16, 19, 23, 31] and references therein)

Finally, solutions of more general polynomial congruences have also been studied in the literature (see for example [3, 4, 11, 25, 32]).

References

[1] E. Alkan, F. Stan and A. Zaharescu, *Lehmer k-tuples*, Proc. Amer. Math. Soc. 134 (2006), 2807–2815.

[2] F. P. Boca, C. Cobeli and A. Zaharescu, *Distribution of lattice points visible from the origin*, Comm. Math. Phys. 213 (2000), 433–470.

[3] C. Cobeli and A. Zaharescu, *Generalization of a problem of Lehmer*, Manuscripta Math. 104 (2001), 301–307.

[4] —, —, *On the distribution of the $\mathbb{F}_p$-points on an affine curve in r dimensions*, Acta Arith. 99 (2001), 321–329.

[5] 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.

[6] M. Z. Garaev, *Character sums in short intervals and the multiplication table modulo a prime*, Monatsh. Math. 148 (2006), 127–138.

[7] —, *On the logarithmic factor in error term estimates in certain additive congruence problems*, Acta Arith. 124 (2006), 27–39.

[8] M. Z. Garaev and A. A. Karatsuba, *On character sums and the exceptional set of a congruence problem*, J. Number Theory 114 (2005), 182–192.

[9] —, —, *The representation of residue classes by products of small integers*, preprint, 2006.

[10] M. Z. Garaev and K.-L. Kueh, *Distribution of special sequences modulo a large prime*, Int. J. Math. Math. Sci. 50 (2003), 3189–3194.

[11] A. Granville, I. E. Shparlinski and A. Zaharescu, *On the distribution of rational functions along a curve over* $\mathbb{F}_p$ *and residue races*, J. Number Theory 112 (2005), 216–237.

[12] M. N. Huxley and W. G. Nowak, *Primitive lattice points in convex planar domains*, Acta Arith. 76 (1996), 271–283.

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

[14] 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.

[15] M. R. Khan, I. E. Shparlinski and C. L. Yankov, *On the convex closure of the graph of modular inversions*, preprint, 2006.

[16] H. N. Liu and W. Zhang, *On a problem of D. H. Lehmer*, Acta Math. Sin. (Engl. Ser.) 22 (2006), 61–68.

[17] H. L. Montgomery, *Ten Lectures on the Interface between Analytic Number Theory and Harmonic Analysis*, Amer. Math. Soc., Providence, RI, 1994.

[18] W. G. Nowak, *Primitive lattice points inside an ellipse*, Czechoslovak Math. J. 55 (2005), 519–530.

[19] I. A. Semaev, *On the number of small solutions of a linear homogeneous congruence*, Mat. Zametki 50 (1991), no. 4, 102–107 (in Russian).

[20] I. E. Shparlinski, *On exponential sums with sparse polynomials and rational functions*, J. Number Theory 60 (1996), 233–244.

[21] —, *On the distribution of points on multidimensional modular hyperbolas*, Proc. Japan Acad. Sci. Ser. A, to appear.

[22] —, *On a generalisation of a Lehmer problem*, preprint, 2006.

[23] —, *Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average*, preprint, 2006.

[24] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, 1995.

[25] M. Vajaitu and A. Zaharescu, *Distribution of values of rational maps on the* $\mathbb{F}_p$*-points on an affine curve*, Monatsh. Math. 136 (2002), 81–86.

[26] W. G. Zhai, *On primitive lattice points in planar domains*, Acta Arith. 109 (2003), 1–26.

[27] W. P. Zhang, *On a problem of D. H. Lehmer and its generalization*, Compos. Math. 86 (1993), 307–316.

[28] —, *On a problem of D. H. Lehmer and its generalization, II*, ibid. 91 (1994), 47–56.

[29] W. P. Zhang, *On the difference between a D. H. Lehmer number and its inverse modulo q*, Acta Arith. 68 (1994), 255–263.
[30] —, *On the distribution of inverses modulo n*, J. Number Theory 61 (1996), 301–310.
[31] —, *On a problem of D. H. Lehmer and Kloosterman sums*, Monatsh. Math. 139 (2003), 247–257.
[32] Z. Y. Zheng, *The distribution of zeros of an irreducible curve over a finite field*, J. Number Theory 59 (1996), 106–118.

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

Received September 19, 2006;
received in final form November 21, 2006 (7552)