On the Convex Hull of the Points on Modular Hyperbolas

Sergei V. Konyagin
Steklov Mathematical Institute
8, Gubkin Street, Moscow, 119991, Russia
konyagin@mi.ras.ru

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

December 14, 2010

Abstract

Given integers a and $m \geq 2$, let $\mathcal{H}_a(m)$ be the following set of integral points

$$\mathcal{H}_a(m) = \{(x, y) \ : \ xy \equiv a \pmod m, \ 1 \leq x, y \leq m-1\}$$

We improve several previously known upper bounds on $v_a(m)$, the number of vertices of the convex closure of $\mathcal{H}_a(m)$, and show that uniformly over all a with $\gcd(a, m) = 1$ we have $v_a(m) \leq m^{1/2+o(1)}$ and furthermore, we have $v_a(m) \leq m^{5/12+o(1)}$ for m which are almost squarefree.

2010 Mathematics Subject Classification: 11A07, 11C08, 11D79

Keywords: congruence, modular hyperbola, integral polygon, convex hull

1 Introduction

For integers a and $m \geq 2$, we define the modular hyperbola, $\mathcal{H}_a(m)$, to be the set of integral points

$$\mathcal{H}_a(m) = \{(x, y) \ : \ xy \equiv a \pmod{m}, \ 1 \leq x, y \leq m-1\}.$$

A systematic study of geometric properties of the set $\mathcal{H}_a(m)$ has been initiated in [7] and continued in a number of works, see [4, 5, 6, 11, 14, 16, 17] and references therein, where also several surprising links to various number theoretic questions have been discovered.

In particular, following [6, 11], we consider the convex closure $\mathcal{C}_s(a, m)$ of the set $\mathcal{H}_a(m)$ and let $v_a(n)$ denote the number of vertices of $\mathcal{C}_s(a, m)$.

For $a = 1$, it is shown in [11] that

$$v_1(m) \leq m^{3/4+o(1)}, \tag{1}$$

which has been improved in [6] as

$$v_1(m) \leq m^{7/12+o(1)}, \tag{2}$$

by using the bound $O(S^{1/3})$ of G. Andrews [2] on the number of vertices of a convex polygon of area S vertices on the integral lattice $\mathbb{Z}^2$. In [11] a number of other lower and upper bounds on $v_1(m)$ have been established, which however apply only to special classes of integers m. For example, it shown in [11, Theorem 3.2] that for all $m > 1$,

$$v_1(m) \geq 2(\tau(m-1) - 1)$$

where $\tau(k)$ is the number of positive integer divisors of k, and this estimate is tight as

$$\#\{m \leq x \ : \ v_1(m) = 2(\tau(m-1) - 1)\} \gg \frac{x}{\log x},$$

where, as usual, the notations $U \ll V$ and $V \gg U$ are equivalent to $U = O(V)$ (throughout the paper, except Lemma 4, the implied constants are absolute). Besides, one can find in [11] an extensive numerical study of $v_1(m)$ which shows a somewhat mysterious behaviour which exhibits both some chaotic and regular aspects.

It has also been noticed in [6] that [16, Theorem 1] implies that

$$v_a(m) \le m^{1/2+o(1)}, \tag{3}$$

for all but $o(\varphi(m))$ integers a with $1 \le a \le m-1$ and $\gcd(a, m) = 1$, where, as usual, $\varphi(m)$ denotes the Euler function.

Here we use rather elementary arguments to improve and generalise the bounds (1), (2) and (3) and show that in fact (3) holds for all a with $\gcd(a, m) = 1$ and also prove a stronger bound for integers m which are almost squarefree. More precisely, we obtain the following results.

Theorem 1. *For an arbitrary integer $m \ge 2$, uniformly over integers a with $\gcd(a, m) = 1$, we have*

$$v_a(m) \le m^{1/2+o(1)},$$

as $m \to \infty$.

For an integer m we denote by m^* its kernel, that is, the product of all prime divisors of m.

Theorem 2. *For an arbitrary integer $m \ge 2$, uniformly over integers a with $\gcd(a, m) = 1$, we have*

$$v_a(m) \le t m^{5/12+o(1)},$$

where $t = m/m^*$.

In particular, for a squarefree m we have $m^* = m$, thus we have:

Corollary 1. *For an arbitrary squarefree integer $m \ge 2$, uniformly over integers a with $\gcd(a, m) = 1$, we have*

$$v_a(m) \le m^{5/12+o(1)}.$$

Finally, a simple counting argument shows that $m^* = m^{1+o(1)}$ for almost all m and thus leads to the following estimate:

Corollary 2. *For $M \to \infty$ and all but $o(M)$ positive integers $m \le M$, uniformly over integers a with $\gcd(a, m) = 1$, we have*

$$v_a(m) \le m^{5/12+o(1)}.$$

2 Distribution of Points on Curves

We denote

$$N(a, m; U, V) = \{(x, y) \ : \ xy \equiv a \pmod m, \ 1 \le x \le U, \ 1 \le y \le V\}.$$

We need the following asymptotic formula on $N(a, m; U, V)$ that is immediate from the Weil bound of Kloosterman sums; see, for example, [8] (we note that in [8] it is given only for $a = 1$ but the proof extends to arbitrary a with $\gcd(a, m) = 1$ at the cost of only obvious typographical adjustments).

Lemma 3. *Uniformly over integers a, U, V,*

$$N(a, m; U, V) = UV\frac{\varphi(m)}{m^2} + O\left(m^{1/2+o(1)}\right).$$

We prove the following statement in a much more general form that we need for our purpose as we believe this can be of independent interest.

Lemma 4. *Let $\mu_i(X, Y) = X^{h_i}Y^{k_i}$, $i = 1, \ldots, s$, be s arbitrary distinct monomials. Assume that for a set of $K \ge s$ distinct points $(x_\nu, y_\nu) \in \mathbb{Z}^2$ with $\max\{|x_\nu|, |y_\nu|\} \le H$, $\nu = 1, \ldots, K$, over an arbitrary field $\mathbb{F}$ we have*

$$\det\left(\mu_i(x_{\nu_j}, y_{\nu_j})\right)_{i,j=1}^{s} = 0$$

for any $1 \le \nu_1 < \ldots < \nu_s \le K$. Then there is a polynomial F of the form

$$F(X, Y) = \sum_{i=1}^{s} A_i\mu_i(X, Y)$$

with integer coefficients satisfying $|A_i| \le H^{O(1)}$, $i = 1, \ldots, s$, where the implied constant depends only on s, and such that $F(x_\nu, y_\nu) = 0$, $\nu = 1, \ldots, K$.

Proof. Let r be the largest rank of all matrices $\left(\mu_i(x_{\nu_j}, y_{\nu_j})\right)_{i,j=1}^{s}$ with $1 \le \nu_1 < \ldots < \nu_s \le K$. We have $1 \le r \le s - 1$. Without loss of generality we can assume that the matrix

$$M = \det\left(\mu_i(x_j, y_j)\right)_{i,j=1}^{r+1,r}$$

is of rank r. Thus, there is a unique nontrivial vanishing linear combination of columns with relatively prime coefficients $a_1, \ldots, a_{r+1}$ such that the first nonzero coefficient is 1. Furthermore, it is obvious (from the explicit expression for solutions of system of linear equations via determinants and trivial upper bounds on these determinants), that $|a_i| \le H^{O(1)}$, $i = 1, \ldots, r+1$

Thus for any $\nu = 1, \ldots, K$ the matrix obtained from M by adding the bottom row $(\mu_1(x_\nu, y_\nu), \ldots, \mu_r(x_\nu, y_\nu))$ is also of rank k, so

$$a_1\mu_1(x_\nu, y_\nu) + \ldots + a_{r+1}\mu_{r+1}(x_\nu, y_\nu) = 0,$$

which concludes the proof. □

Lemma 5. *Let*

$$G(X,Y) = AX^2 + BXY + CY^2 + DX + EY + F \in \mathbb{Z}[X,Y]$$

be an irreducible quadratic polynomial with coefficients of size at most H. Assume that $G(X,Y)$ is not affine equivalent to a parabola $Y = X^2$ and has a nonzero determinant

$$\Delta = B^2 - 4AC \ne 0.$$

Then the equation $G(x,y) = 0$ has at most $H^{o(1)}$ integral solutions $(x,y) \in [0,H] \times [0,H]$.

Proof. The proof is based on the reduction of the equation $G(x,y) = 0$ to a Pell equation $X^2 - UY^2 = V$ with some integers U and V of size $H^{O(1)}$ together with the estimate of R. C. Vaughan and T. D. Wooley [18, Lemma 3.5] on the number of solutions of this equation of a given size.

In the case when the discriminant Δ is not a perfect square the above reduction is given by J. Cilleruelo and M. Z. Garaev [5, Proposition 1]. If Δ is a perfect square it is obtained by V. Shelestunova [13, Theorem 1]. □

3 Integral Polygons

We say that a polygon $\mathcal{P} \subseteq \mathbb{R}^2$ is integral if all its vertices belong to the integral lattice $\mathbb{Z}^2$.

Also, following V. I. Arnold [1] we say two polygons $\mathcal{P}, \mathcal{Q} \subseteq \mathbb{R}^2$ are equivalent is there is an affine transformation

$$T : \mathbf{x} \mapsto A\mathbf{x} + \mathbf{b}, \qquad \mathbf{x} \in \mathbb{R}^2$$

for $A = \mathrm{GL}_2(\mathbb{Z})$ and $\mathbf{b} \in \mathbb{Z}^2$ preserving the integral lattice $\mathbb{Z}^2$ (that is, $\det A = \pm 1$) that maps $\mathcal{P}$ to $\mathcal{Q}$.

We need the following result of I. Bárány and J. Pach [3, Lemma 3]:

Lemma 6. *An integral polygon of area S is equivalent to a polygon contained in some box $[0,u] \times [0,v]$ of area $uv \le 4S$.*

We note that it can also be derived (with a slightly weaker constant) from a result of V. I. Arnold [1, Lemma 1 of Section 2] that asserts that any integral convex polygon of area S can be covered by an integral parallelogram of area at most $6S$.

We also recall the following general result of F. V. Petrov [12, Lemma 2.2] which we use only in $\mathbb{R}^2$. We use $\mathrm{vol}\,\mathfrak{A}$ to denote the volume of a compact set $\mathfrak{A} \subseteq \mathbb{R}^d$

Lemma 7. *Let $\mathfrak{U} \subseteq \mathbb{R}^d$ be a convex compact. We consider a finite sequence of compacts $\mathfrak{V}_i \subseteq K$, $i = 1, \ldots, n$, such that none of them meets the convex hull of others. Then*

$$\sum_{i=1}^{n} (\mathrm{vol}\,\mathfrak{V}_i)^{(d-1)/(d+1)} \ll (\mathrm{vol}\,\mathfrak{U})^{(d-1)/(d+1)},$$

where the implied constant depends only on d.

4 Proof of Theorem 1

We estimate the number of vertices (x,y) of $\mathcal{C}_s(a,m)$ that are inside of the square $[0,m/2] \times [0,m/2]$. The other three squares

$$[0,m/2] \times [m/2,m], \quad [m/2,m] \times [0,m/2], \quad [m/2,m] \times [m/2,m] \tag{4}$$

can be dealt with fully analogously.

We fix some $\varepsilon > 0$ and also recall the well-known estimates on the divisors and Euler functions

$$\tau(s) = s^{o(1)} \qquad \text{and} \qquad \varphi(s) = s^{1+o(1)}, \tag{5}$$

as $s \to \infty$, see [10, Theorems 317 and 328], we obtain our main technical result.

We claim that, for a sufficiently large m we have

$$xy \le m^{3/2+\varepsilon}. \tag{6}$$

for each such vertex. Indeed, assume that condition (6) fails.

Then applying Lemma 3 to $\mathcal{H}_a(m)$ with $U = xm^{-\varepsilon/4}$ and $V = ym^{-\varepsilon/4}$, we see that there are points $\mathbf{w}_j$, $j = 1, 2, 3, 4$, in each of the translates of the box $[0, U] \times [0, V]$ to the corners of the $[0, m] \times [0, m]$ square.

Therefore the point (x, y) is inside of the convex hull of the points $\mathbf{w}_j$, $j = 1, 2, 3, 4$, but is different from all of them, and thus cannot be a point on $\mathcal{C}_s(a, m)$.

We now see that there is some integer A with $1 \le A < m$ such that for $(x, y) \in \mathcal{C}_s(a, m)$ we have

$$xy = A + m\ell$$

with some nonnegative integer $\ell \le m^{3/2-1+\varepsilon}$. When such an integer k is fixed, by (5) there are $m^{o(1)}$ possibilities for the point (x, y) and the result now follows.

5 Proof of Theorem 2

Fix some $\varepsilon > 0$.

As in the proof of Theorem 1 we see from Lemma 3 that all vertices (u, v) on $\mathcal{C}_s(a, m)$ that are also inside of the square $[0, m/2] \times [0, m/2]$ satisfy

$$uv \le m^{3/2+o(1)}.$$

We estimate the number of such points.

The number of vertices of $\mathcal{C}_s(a, m)$ inside of the squares (4) can be estimated fully analogously.

Hence, it is enough to estimate the number of vertices of $\mathcal{C}_s(a, m)$ inside of each of the boxes $[1, U] \times [1, V]$ with $U = 2^j$, $V = m^{3/2+\varepsilon}2^{-j}$, $j = 1, 2, \ldots$. Since only $O(\log m)$ such boxes are of our interest.

Let $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathcal{C}_s(a, m)$ be located in $[1, U] \times [1, V]$. Assume that $r \ge tm^{\varepsilon}$ as otherwise there is nothing to prove. Select

$$k = \lfloor tm^{\varepsilon} \rfloor .$$

By Lemma 7, there are k consecutive vertices $\mathbf{v}_{j+1}, \ldots, \mathbf{v}_{j+k}$ such that the area of the polygon formed by these vertices is bounded by

$$Q = O(UV(r/k)^{-3}) = O(m^{3/2+4\varepsilon}t^3r^{-3}). \tag{7}$$

In particular, we have $k \ge 5$ for a sufficiently large m.

By Lemma 6, we have an affine transformation of $\mathbb{R}^2$ preserving $\mathbb{Z}^2$ such that the images of all points $\mathbf{v}_{j+\nu}$ are points $(X_\nu, Y_\nu) \in [0, u] \times [0, v]$, $\nu = 1, \ldots, k$ for some real positive u and v with $uv \ll Q$.

Note that all these points satisfy the congruence

$$f(X_\nu, Y_\nu) \equiv 0 \pmod m, \qquad \nu = 1, \ldots, k, \tag{8}$$

where f is a nonzero modulo m quadratic polynomial (which is the image of $XY - a$ under the above transformation).

Without loss of generality, we can assume that $X_k = Y_k = 0$. So, the constant term of f is 0. Take arbitrary $\nu_1 < \ldots < \nu_5$. The matrix

$$W = (X_{\nu_i}^2, X_{\nu_i} Y_{\nu_i}, Y_{\nu_i}^2, X_{\nu_i}, Y_{\nu_i})_{i=1,\ldots,5}$$

is singular modulo m since $f(X_{\nu_i}, Y_{\nu_i}) \equiv 0 \pmod m$, $i = 1, \ldots, 5$. This implies that the determinant $\det W$ is divisible by m. Examining the structure of the terms of $\det W$ one also sees that $\det W = O(Q^4)$.

Therefore, if $Q \le c m^{1/4}$ with an appropriate constant c then $\det W = 0$ (over $\mathbb{Z}$). We now see from Lemma 4 that there is a nonzero quadratic polynomial $F(X, Y)$ such that

$$F(X_\nu, Y_\nu) = 0, \qquad \nu = 1, \ldots, k, \tag{9}$$

with the integer coefficients of size $m^{O(1)}$. Moreover, we may assume that the coefficients of F are relatively prime.

Let $\mathbf{v}_{j+\nu} = (x_\nu, y_\nu)$, $\nu = 1, \ldots, k$. The equation (9) is equivalent to the equation

$$G(x_\nu, y_\nu) = 0, \qquad \nu = 1, \ldots, k, \tag{10}$$

for some quadratic polynomial $G(X, Y) \in \mathbb{Z}[X, Y]$ with relatively prime coefficients. Next, we consider the polynomial $H(X) = X^2 G(X, a/X)$ over the ring of residues modulo m. For any $\nu = 1, \ldots, k$ we have $H(x_\nu) \equiv 0 \pmod m$.

We take an arbitrary prime divisor $p > 5$ of m^*. Assume that all coefficients of H are divisible by p. Then any solution of the congruence $xy \equiv a \bmod p$ also satisfies the congruence $G(x, y) \equiv 0 \bmod p$. Therefore, there are at least $p - 1 > 4$ common zeros of polynomials $xy - a$ and G modulo p. By the Bézout Theorem, see, for example, [9, Section 5.3], the polynomial G is a multiple of $xy - a$ modulo p. Then G is irreducible and is not affine equivalent to a parabola modulo p. Consequently, G is irreducible and is not affine equivalent to a parabola over $\mathbb{Z}$ and also has a nonzero determinant. Thus, we can apply Lemma 5 and conclude that the equation $G(x, y) = 0$ has at most $m^{o(1)}$ integral solutions $(x, y) \in [0, m] \times [0, m]$. Now assume that for any prime divisor $p > 5$ of m^* there is a coefficient of H not divisible by p. Using the Chinese Remainder Theorem, we see that the congruence $H(x) \equiv 0 \pmod m$, $1 \le x \le m$, has at most $t4^{\omega(m^*)} = t\tau(m^*)^2$ solutions, where $\omega(s)$ is the number of prime divisors of an integer s. Recalling (5) we see that in both cases $k = tm^{o(1)}$ which contradicts to our choice of $k = \lfloor tm^{\varepsilon} \rfloor$. Therefore $Q > cm^{1/4}$ which together with (7) implies $r = O\left(tm^{5/12+4\varepsilon/3}\right)$. Since $\varepsilon > 0$ is arbitrary, the result now follows.

6 Comments

It is shown in [16] that for almost all residue classes a modulo m, the asymptotic formula of Lemma 3 can be improved. Perhaps this can be used to improve the bound of Theorems 1 and 2 on average over a.

Convex hull of the points on multidimensional hyperbolas can be studied as well. In fact in the multidimensional case a different technique can be used to obtain versions of Lemma 3 which have no analogues in the two dimensional case, see [15]. Furthermore, the method of proof of Theorem 1 easily extends to the multidimensional case as well. However extending the method of proof of Theorem 2 seems to be more difficult and we pose this as an open question.

Acknowledgement

The authors would like to thank Imre Bárány for the information about the existence of a proof of Lemma 6 in [3] and Oleg German for an alternative proof of this result. The authors are also grateful to Pär Kurlberg for supplying then with an alternative proof of Lemma 5 and to David McKinnon and Alfred Menezes for useful discussion and for the information about the thesis of V. Shelestunova [13].

The research of S. K. was supported in part Russian Fund of Basic Researches Grant N. 11-01-00329 from the Russian Fund of Basic Researches and that of I. S. by ARC grant DP1092835.

References

[1] V. I. Arnold, 'Statistics of integral polygons', *Funct. Anal Appl.*, **14**(2) (1980), 1–3 (in Russian).

[2] G. Andrews, 'A lower bound for the volume of strictly convex bodies with many boundary lattice points', *Trans. Amer. Math. Soc.*, **106** (1963), 270–279.

[3] I. Bárány and J. Pach, 'On the number of convex lattice polygons', *Combinatorics, Probability, and Computing*, **1** (1992), 193–302.

[4] T. H. Chan and I. E. Shparlinski, 'On the concentration of points on modular hyperbolas and exponential curves', *Acta Arith.*, **142** (2010), 59–66

[5] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Preprint*, 2010 (available from `http://arxiv.org/abs/1007.1526`).

[6] K. Ford, M. R. Khan and , I. E. Shparlinski, 'Geometric properties of points on modular hyperbolas', *Proc. Amer. Math. Soc.*, **133** (2010), 4177–4185.

[7] 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.

[8] A. Fujii and Y. Kitaoka, 'On plain lattice points whose coordinates are reciprocals modulo a prime', *Nagoya Math. J.*, **147** (1997), 137–146.

[9] M. Fulton, *Algebraic curves: An Introduction to algebraic geometry*, 3rd edition, Addison Wesley, 2008.

[10] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[11] M. R. Khan, I. E. Shparlinski and C. L. Yankov, 'On the convex closure of the graph of modular inversions', *Experimental Math.*, **17** (2008), 91–104.

[12] F. V. Petrov, ‘An estimate for the number of rational points on convex curves and surfaces’, *Zapiski Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, **344** (2007), 174–189 (in Russian).

[13] V. Shelestunova, ‘Upper bounds for the number of integral points on quadratic curves and surfaces’, *PhD Thesis*, University of Waterloo, Ontario, Canada, 2010.

[14] I. E. Shparlinski, ‘Primitive points on a modular hyperbola’, *Bull. Polish Acad. Sci. Math.*, **54** (2006), 193–200.

[15] I. E. Shparlinski, ‘On the distribution of points on multidimensional modular hyperbolas’, *Proc. Japan Acad. Sci., Ser.A*, **83** (2007), 5–9.

[16] I. E. Shparlinski, ‘Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average;, *Michigan Math. J.*, **56** (2008), 99–111.

[17] I. E. Shparlinski and A. Winterhof, ‘On the number of distances between the coordinates of points points on modular hyperbolas’, *J. Number Theory*, **128** (2008), 1224–1230.

[18] R. C. Vaughan and T. D. Wooley, ‘Further improvements in Waring’s problem’, *Acta Math.*, **174** (1995), 147–240.