GEOMETRIC PROPERTIES OF POINTS ON MODULAR HYPERBOLAS

KEVIN FORD, MIZAN R. KHAN, AND IGOR E. SHPARLINSKI

(Communicated by Matthew A. Papanikolas)

ABSTRACT. Given an integer $n \geq 2$, let $\mathcal{H}_n$ be the set

$$\mathcal{H}_n = \{(a, b) : ab \equiv 1 \pmod{n}, 1 \leq a, b \leq n-1\}$$

and let $M(n)$ be the maximal difference of $b-a$ for $(a, b) \in \mathcal{H}_n$. We prove that for almost all n , $n - M(n) = O(n^{1/2+o(1)})$. We also improve some previously known upper and lower bounds on the number of vertices of the convex closure of $\mathcal{H}_n$.

1. INTRODUCTION

This paper pursues two goals. We prove a weak version of a conjecture in the paper [4] and improve some results in [9]. To put our results in context, we begin by discussing the contents of [4] and [9].

For an integer $n \geq 2$, we define the modular hyperbola, $\mathcal{H}_n$, to be the set

$$\mathcal{H}_n = \{(a, b) : ab \equiv 1 \pmod{n}, 1 \leq a, b \leq n-1\}.$$

There are many interesting and productive questions one can pose about this set. One is the study of $M(n)$, the maximal difference between the components of points of $\mathcal{H}_n$, that is,

$$M(n) = \max\{b-a : (a, b) \in \mathcal{H}_n\}.$$

This function has been studied in two papers [8, 4]. In [8, Theorem 4] it is proved via Kloosterman sums that $n - M(n) \leq n^{3/4+o(1)}$, and in [4] it is shown that for almost all n ,

$$n - M(n) \geq n^{1/2}(\log n)^{\delta/2}(\log \log n)^{3/4}f(n),$$

where

$$\delta = 1 - \frac{1 + \log \log 2}{\log 2} = 0.08607\dots,$$

and $f(n)$ is an arbitrary function with $\lim_{n \rightarrow \infty} f(n) = 0$. Furthermore, in [4], the authors have conjectured that if $g(n) \rightarrow \infty$ as $n \rightarrow \infty$, then

$$n - M(n) \leq n^{1/2}(\log n)^{\delta/2}(\log \log n)^{3/4}g(n)$$

Received by the editors February 11, 2010.

2010 *Mathematics Subject Classification*. Primary 11A07; Secondary 11H06, 11N69.

The research of the first author was supported in part by NSF grants DMS-0555367 and DMS-0901339.

The research of the third author was supported by ARC grants DP0556431 and DP1092835.

FIGURE 1. The curve $\mathcal{H}_{47}$ with the lines of symmetry $y = x$, $y + x = 47$

for almost all n , and have given a heuristic for this statement. We prove a weaker form of this conjecture.

Theorem 1. *For every $\varepsilon > 0$ and $A > 0$, we have $n - M(n) = O(n^{1/2+\varepsilon})$ for all integers $n \leq x$ with at most $O(x/(\log x)^A)$ exceptions.*

In particular, we see that $n - M(n) = n^{1/2+o(1)}$ for almost all n . After proving Theorem 1, we turn our attention to improving certain results that have appeared in [9]. Following [9], let $\mathcal{C}_n$ denote the convex closure of the set $\mathcal{H}_n$ and let $v(n)$ denote the number of vertices of $\mathcal{C}_n$. The paper [9] is an attempt to determine asymptotic bounds for $v(n)$, and in this the authors have only been partly successful. Let us describe some elementary properties of $\mathcal{H}_n$ and $\mathcal{C}_n$.

The first is that the lines $y = x$ and $y = n - x$ are lines of symmetry of $\mathcal{H}_n$. These symmetries reduce the amount of work needed to determine the vertices of $\mathcal{C}_n$, as one can restrict the search to the vertices of $\mathcal{C}_n$ that lie in the triangle $\mathcal{T}_n$ with vertices $(0, 0)$, $(0, n)$ and $(n/2, n/2)$. Following [9], let $(a_0, b_0) = (1, 1), (a_1, b_1), \dots, (a_s, b_s)$, with $a_0 < a_1 < \dots < a_s$, be the vertices of $\mathcal{C}_n$ in $\mathcal{T}_n$. Then $M(n) = b_s - a_s$; that is, the maximum difference is achieved by the highest vertex of $\mathcal{C}_n$ in $\mathcal{T}_n$.

We illustrate this in Figure 1 with the graph of $\mathcal{H}_{47}$ with the lines of symmetry $y = x$ and $y = 47 - x$. We note that $(a_1, b_1) = (2, 24)$ and $(a_s, b_s) = (a_2, b_2) = (10, 33)$.

One of the first results in [9] is that for all $n > 1$,

$$v(n) \geq 2(\tau(n-1) - 1),$$

where $\tau(k)$ is the number of positive integer divisors of k . The proof follows from observing that the lattice points on the curves

$$x(n-y) = n-1 \text{ and } (n-x)y = n-1, \text{ with } 1 \leq x, y \leq n-1,$$

belong to $\mathcal{C}_n$ with the points $(1, 1)$ and $(n-1, n-1)$ being common to both curves. We illustrate this in Figure 2. This estimate is tight as $v(n) = 2(\tau(n-1) - 1)$ for

 FIGURE 2. The curves $x(47 - y) = 46, (47 - x)y = 46$ enclosing $\mathcal{H}_{47}$

infinitely many integers n . Specifically in [9, Theorem 3.2] it is shown that

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

where, as usual, the notation $U \ll V$ and $V \gg U$ is equivalent to $U = O(V)$ (throughout the paper, the implied constants may depend on the positive parameter ε and are absolute otherwise).

The authors [9, Theorem 3.4 (b)] then give a conditional proof of $v(n) > 2(\tau(n-1) - 1)$ for almost all n under the hypothesis that for almost all n , $n - M(n) \leq n^{1/2+o(1)}$. The proof is by combining a result of [3] with the inequality $n - M(n) \leq n^{1/2+o(1)}$ to obtain that for almost all n , the vertex (a_s, b_s) does not lie on the curve $x(n-y) = n-1$. Hence, by proving Theorem 1 we obtain the following unconditional result.

Corollary 1. *The set of integers n for which $v(n) > 2(\tau(n-1) - 1)$ has asymptotic density 1.*

Another result of [9] is that $v(n)/\tau(n-1) \neq O(1)$. Specifically it is shown in [9] that for infinitely many primes p ,

$$(1) \quad v(p+1) \geq \exp\left(\left(\frac{2 \log 2}{11} + o(1)\right) \frac{\log p}{\log \log p}\right).$$

The basic idea of the proof is to find primes, p , such that $2p+1$ has “many” factors. This is achieved by combining the prime number theorem with the Heath-Brown estimate [7] on the smallest prime in an arithmetic progression (see [9, Theorem 3.5]). In this paper we improve (1) by applying a result of Alford, Granville and Pomerance [1, Theorem 2.1] on the distribution of primes in almost all arithmetic progressions.

Theorem 2. *There are infinitely many primes p with*

$$v(p+1) \geq \exp\left(\left(\frac{5 \log 2}{12} + o(1)\right) \frac{\log p}{\log \log p}\right).$$

The set of vertices of $\mathcal{C}_n$ seems to be a “hybrid” set in the sense that Tao uses it in [12, page 156]. The structured part of this set comprises the vertices that arise from the divisors of $n-1$. The remaining vertices seem to arise from a combination of pseudorandomness and the structure of divisors of $nj-1$ for some “small” values of $j \geq 2$. A recurrent theme in our attempts to handle the difficulties arising from the “pseudorandomness” of $v(n)$ is to apply the properties of the special vertex (a_s, b_s) . So for example the bound

$$n - (b_s - a_s) = n - M(n) \leq n^{3/4+o(1)}$$

immediately gives us that

$$(2) \quad v(n) \leq n^{3/4+o(1)}.$$

Unfortunately this is a pretty crude bound, as the numerics in [9] indicate that $v(n) \leq n^{o(1)}$. (We should mention that in [9, Section 5.2] there are a couple of “reasonable” numerical approximations to the difference $v(n) - 2(\tau(n-1) - 1)$, but these are just guesses.) In this paper we make a small improvement to (2) by using a result of Andrews [2] on the number of integral vertices of convex flat (that is, 2-dimensional) polygons. We prove the following result.

Theorem 3. *We have*

$$v(n) \leq n^{7/12+o(1)}.$$

2. PRELIMINARIES

We need the following special case of [5, Proposition 1].

Lemma 2.1. *Let L, N and Q be arbitrary real numbers, which for a fixed $\varepsilon > 0$ satisfy the inequalities*

$$2 \leq L^\varepsilon \leq N \leq L^{1/2-\varepsilon} \quad \text{and} \quad 2 \leq Q \leq L^{3/4-\varepsilon},$$

and let $(\alpha_m)_{m \in [L, 2L]}$ be an arbitrary sequence of complex numbers with $|\alpha_m| \leq 1$. Then, for every fixed $A > 0$ we have

$$\sum_{1 \leq q \leq Q} \left(\sum_{\substack{L < m \leq 2L \\ N < n \leq 2N \\ mn \equiv 1 \pmod{q}}} \alpha_m - \frac{1}{\varphi(q)} \sum_{\substack{L < m \leq 2L \\ N < n \leq 2N \\ \gcd(mn, q) = 1}} \alpha_m \right) \ll LN(\log L)^{-A}.$$

Let $\varphi(x; n) = \#\{a : 1 \leq a \leq x, \gcd(a, n) = 1\}$ be the standard extension of the Euler function. Then, by the inclusion-exclusion principle, we have

$$\varphi(x; n) = \sum_{d|n} \left\lfloor \frac{x}{d} \right\rfloor \mu(d),$$

where $\mu(d)$ is the Möbius function. We need the following two consequences of this identity.

Lemma 2.2. *Let $I, L \in \mathbb{Z}^+$, let $x \geq 0$, and let $\tau^*(L)$ denote the number of square-free divisors of L . Then,*

$$\sum_{\substack{I < j \leq I+J \\ \gcd(j, L) = 1}} 1 = \frac{\varphi(L)}{L} J + O(\tau^*(L))$$

and

$$\sum_{\substack{I < j \leq I+J \\ \gcd(j, L)=1}} \frac{1}{j} = \frac{\varphi(L)}{L} \log(1 + J/I) + O(\tau^*(L)/I).$$

We remark that when we apply Lemma 2.2 we replace $\tau^*(L)$ in the error term with $L^{o(1)}$. Finally, we recall the following special case of a general result of Andrews [2].

Lemma 2.3. *A convex 2-dimensional polygon of area S , with all vertices on the lattice $\mathbb{Z}^2$, has at most $O(S^{1/3})$ vertices.*

3. PROOF OF THEOREM 1

Let m be a positive integer, and let Q and R be two positive real numbers. We define $\mathcal{V}(m; Q, R)$ to be the set

$$\mathcal{V}(m; Q, R) = \left\{ (q, r) \in \mathbb{Z}^2 : \frac{Q}{2} < q \leq Q, \frac{mR+1}{q} < r \leq \frac{2mR+1}{q}, \gcd(qr, m) = 1 \right\}.$$

This set plays a central role in our proof, and we require the following asymptotic for $\#\mathcal{V}(m; Q, R)$:

Lemma 3.1. *We have*

$$\#\mathcal{V}(m; Q, R) = \frac{\varphi(m)^2}{m} R \log 2 + O(Qm^{o(1)}).$$

Proof.

$$\begin{aligned} \#\mathcal{V}(m; Q, R) &= \sum_{\substack{Q/2 < q \leq Q \\ \gcd(q, m)=1}} \sum_{\substack{(mR+1)/q < r \leq (2mR+1)/q \\ \gcd(r, m)=1}} 1 \\ &= \sum_{\substack{Q/2 < q \leq Q \\ \gcd(q, m)=1}} \left(\frac{\varphi(m)R}{q} + O(m^{o(1)}) \right) \\ &= R\varphi(m) \sum_{\substack{Q/2 < q \leq Q \\ \gcd(q, m)=1}} \frac{1}{q} + O(m^{o(1)}Q). \end{aligned}$$

Applying Lemma 2.2 we conclude the proof. $\square$

We are now ready to prove Theorem 1. Let m be a positive integer, let Q and R be two positive real numbers, and let $N(m; Q, R)$ denote the number of solutions to the congruence:

$$qr \equiv -1 \pmod{m}, \quad (q, r) \in \mathcal{V}(m; Q, R).$$

If this congruence has a solution, then $M(m) \geq m - r - q$, that is, $r + q \geq m - M(m)$. So the plan to prove the result is to find appropriate bounds for Q and R and then apply Lemma 2.1 to obtain $r + q \leq L^{1/2+o(1)}$ for $L \leq m$.

For $L > Q \geq 2$, with $L < m \leq 2L$, we consider the sum

$$\begin{aligned}
 W(L; Q, R) &= \sum_{L < m \leq 2L} \left| N(m; Q, R) - \frac{1}{\varphi(m)} \# \mathcal{V}(m; Q, R) \right| \\
 &= \sum_{L < m \leq 2L} \alpha_m \left(N(m; Q, R) - \frac{1}{\varphi(m)} \# \mathcal{V}(m; Q, R) \right) \\
 &= \sum_{L < m \leq 2L} \alpha_m \left(N(m; Q, R) - \frac{1}{\varphi(m)} \sum_{(q,r) \in \mathcal{V}(m; Q, R)} 1 \right) \\
 &= U_1 - U_2,
 \end{aligned} \tag{3}$$

where $\alpha_m = \pm 1$,

$$\begin{aligned}
 U_1 &= \sum_{Q/2 < q \leq Q} \sum_{\substack{L < m \leq 2L \\ \gcd(m, q) = 1}} \alpha_m \sum_{\substack{(mR+1)/q < r \leq (2mR+1)/q \\ rq \equiv -1 \pmod{m}}} 1, \\
 U_2 &= \sum_{Q/2 < q \leq Q} \sum_{\substack{L < m \leq 2L \\ \gcd(m, q) = 1}} \frac{\alpha_m}{\varphi(m)} \sum_{\substack{(mR+1)/q < r \leq (2mR+1)/q \\ \gcd(r, m) = 1}} 1.
 \end{aligned}$$

We now replace the condition $rq \equiv -1 \pmod{m}$ with the equation $rq = mn - 1$, where for $(r, q) \in \mathcal{V}(m; Q, R)$ we have $R < n \leq 2R$.

Therefore,

$$U_1 = \sum_{Q/2 < q \leq Q} \sum_{\substack{L < m \leq 2L \\ \gcd(m, q) = 1}} \alpha_m \sum_{\substack{R < n \leq 2R \\ mn \equiv 1 \pmod{q}}} 1.$$

We now fix some $\varepsilon > 0$ and take

$$Q = L^{1/2+\varepsilon} \quad \text{and} \quad R = L^\varepsilon. \tag{4}$$

Then Lemma 2.1 can be applied (with q varying from $Q/2$ to Q), followed by an application of Lemma 2.2. We obtain

$$\begin{aligned}
 U_1 &= \sum_{Q/2 < q \leq Q} \frac{1}{\varphi(q)} \sum_{\substack{L < m \leq 2L \\ R < n \leq 2R \\ \gcd(mn, q) = 1}} \alpha_m + O\left(LR(\log L)^{-(A+\varepsilon/2)}\right) \\
 &= R \sum_{Q/2 < q \leq Q} \frac{1}{q} \sum_{\substack{L < m \leq 2L \\ \gcd(m, q) = 1}} \alpha_m + O\left(LR(\log L)^{-(A+\varepsilon/2)}\right).
 \end{aligned}$$

Again by Lemma 2.2, we have

$$\begin{aligned}
 U_2 &= \sum_{Q/2 < q \leq Q} \sum_{\substack{L < m \leq 2L \\ \gcd(m, q) = 1}} \frac{\alpha_m}{\varphi(m)} \left(\frac{\varphi(m)R}{q} + O\left(L^{\varepsilon/4}\right) \right) \\
 &= R \sum_{Q/2 < q \leq Q} \frac{1}{q} \sum_{\substack{L < m \leq 2L \\ \gcd(m, q) = 1}} \alpha_m + O\left(L^{1+\varepsilon/4}\right).
 \end{aligned} \tag{5}$$

Inserting the bounds for U_1 and U_2 into (3), we obtain

$$W(L; Q, R) \ll LR(\log L)^{-(A+\varepsilon/2)}. \tag{6}$$

Combining Lemma 3.1 with (6) we get

$$\sum_{L < m \leq 2L} \left| N(m; Q, R) - \frac{\varphi(m)}{m} R \log 2 \right| \ll LR(\log L)^{-(A+\epsilon/2)}.$$

Since $\varphi(m) \gg m/\log \log m$, this shows that $N(m; Q, R) \geq 1$ for all $m \in (L, 2L]$ with at most

$$O\left(\frac{L \log \log L}{(\log L)^{A+\epsilon/2}}\right) \ll \frac{L}{(\log L)^A}$$

exceptions.

If $N(m; Q, R) \geq 1$, then we have a lattice point $(q, r) \in \mathcal{V}(m; Q, R)$ satisfying the congruence $qr \equiv -1 \pmod{m}$. We now get that

$$m - M(m) \leq r + q \ll L^{1/2+\epsilon} \ll m^{1/2+\epsilon}.$$

4. PROOF OF THEOREM 2

Let p be a prime. A simple geometric calculation shows that every divisor d of $2p+1$, with $3 < d < (2p+1)/3$, gives rise to a lattice point on the curve $x(n-y) = 2p+1$ that is a vertex of $\mathcal{C}_{p+1}$. This immediately leads to the inequality

$$(7) \quad v(p+1) \geq 2(\tau(2p+1) - 3).$$

(See the beginning of the proof of [9, Theorem 3.5] for the details.) So the main difficulty is to show the existence of primes such that $\tau(2p+1)$ is large. This we do by applying the result of Alford, Granville and Pomerance [1, Theorem 2.1]. The next couple of paragraphs are devoted to setting up the hypotheses so that we can invoke this result.

We start by fixing an arbitrary $A > 12/5$ and a sufficiently small $\delta > 0$. We now consider the set $\mathcal{D}_{1/2,\delta}(x)$ as defined in [1, Theorem 2.1] (that is, we apply it with $\varepsilon = 1/2$, but we can choose any ε such that $0 < \varepsilon < 1$). Two parameters associated with $\mathcal{D}_{1/2,\delta}$ are the positive integer $D_{1/2,\delta}$ and the positive real number $x_{\varepsilon,\delta}$. We assume that $x \geq x_{1/2,\delta}$ is sufficiently large. We now need to determine a modulus q that satisfies three conditions:

- $q \leq x^{1/A-\delta}$;
- q has many prime factors;
- q is relatively prime to every element in $\mathcal{D}_{1/2,\delta}(x)$.

Let

$$\theta(x) = \sum_{\substack{\ell \leq x, \\ \ell \text{ prime}}} \log \ell$$

denote the Chebyshev function and let L be the largest integer that satisfies the inequality

$$\theta(L) - \log 2 \leq (1/A - \delta) \log x.$$

By the prime number theorem

$$(8) \quad L = \left(\frac{1}{A} - \delta + o(1) \right) \log x.$$

Let

$$D(x) = \prod_{d \in \mathcal{D}_{1/2,\delta}(x)} d, \quad Q = \exp(\theta(L) - \log 2).$$

We now set q to be the integer

$$q = \frac{Q}{\gcd(Q, D(x))}.$$

Since $\#\mathcal{D}_{1/2,\delta}(x) \leq D_{1/2,\delta}$, we have

$$(9) \quad \tau(q) \geq 2^{\pi(L)-D_{1/2,\delta}} = 2^{\pi(L)+O(1)} = 2^{(1+o(1))L/\log L},$$

and so we see that q indeed satisfies all three conditions that we listed.

On applying the bound of [1, Theorem 2.1] with $d = q$ and $y = x$, we see that for a sufficiently large x (depending only on A and δ) there is a prime $p \leq x$ in the arithmetic progression $2p \equiv -1 \pmod{q}$. Combining (8), (9) and the inequality $\tau(2p+1) \geq \tau(q)$ we obtain that

$$\tau(2p+1) \geq \exp\left(\left(\left(\frac{1}{A} - \delta\right) \log 2 + o(1)\right) \frac{\log x}{\log \log x}\right).$$

Using (7) and recalling that $A \geq 12/5$ and $\delta > 0$ are arbitrary, we conclude the proof of Theorem 2.

5. PROOF OF THEOREM 3

We recall that $(a_0, b_0), (a_1, b_1), \dots, (a_s, b_s)$ denote the vertices of $\mathcal{C}_n$ that lie in the triangle with vertices $(0, 0), (0, n)$ and $(n/2, n/2)$. Since the lines $y = x$ and $y = n - x$ are lines of symmetry of $\mathcal{H}_n$ (and consequently also of $\mathcal{C}_n$) we can conclude that

$$v(n) = \begin{cases} 4s + 2 & \text{if } (a_s, b_s) \text{ does not lie on } y = n - x, \\ 4s & \text{if } (a_s, b_s) \text{ lies on } y = n - x. \end{cases}$$

Let C be the convex closure of the points $(a_0, b_0), (a_1, b_1), \dots, (a_s, b_s)$. Clearly C lies inside the rectangle with vertices $(1, 1), (a_s, 1), (1, b_s)$ and (a_s, b_s) . We now apply the inequalities

$$a_s < (n - b_s) + a_s = n - M(n) \leq n^{3/4+o(1)} \text{ and } b_s < n$$

to deduce

$$\text{area}(C) \leq a_s \cdot b_s \leq n^{7/4+o(1)}$$

and then invoke Lemma 2.3 to conclude that $s \leq n^{7/12+o(1)}$.

6. COMMENTS

We note that one can also combine the arguments of the proofs of Theorems 1 and 3 to show that for almost all n we have

$$v(n) \leq n^{1/2+o(1)}.$$

Furthermore, it is easy to see that the proof of Theorem 3 generalizes to the number of vertices, $v_h(n)$, of the convex closure $\mathcal{C}_{h,n}$ of the hyperbola

$$\mathcal{H}_{h,n} = \{(a, b) : ab \equiv h \pmod{n}, 1 \leq x, y \leq n-1\}$$

for an arbitrary integer h satisfying $\gcd(h, n) = 1$. In particular, we have a full analogue of Theorem 3 for $v_h(n)$. Moreover, using [11, Theorem 1] one can easily derive that

$$v_h(n) = n^{1/2+o(1)}$$

for all but $o(\varphi(n))$ integers h with $1 \leq h \leq n-1$ and $\gcd(h, n) = 1$, where $\varphi(n)$ denotes the Euler function. Unfortunately, the result of Andrews [2] does not help in this case.

One can also use [10, Theorems 8 and 9] in conjunction with similar arguments to obtain results for the number of vertices of the convex closure of a multidimensional hyperbola. We recall that the result of Andrews [2] generalises to multidimensional polygons. Interestingly, Theorem 2 does not immediately generalise to $v_d(n)$ or the multidimensional case. Finally, we remark that the result of Harman [6] may possibly lead to a further improvement of Theorem 2.

REFERENCES

- [1] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math. (2) **139** (1994), 703–722. MR1283874 (95k:11114)
- [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. MR0143105 (26:670)
- [3] K. Ford, *The distribution of integers with a divisor in a given interval*, Annals. of Math. (2) **168** (2008), 367–433. MR2434882 (2009m:11152)
- [4] 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. MR2163580 (2006c:11108)
- [5] É. Fouvry, *Sur le problème des diviseurs de Titchmarsh*, J. Reine Angew. Math. **357** (1985), 51–76. MR783533 (87b:11090)
- [6] G. Harman, *On the number of Carmichael numbers up to x* , Bull. London Math. Soc. **37** (2005), 641–650. MR2164825 (2006d:11106)
- [7] D. R. Heath-Brown, *Zero-free regions for Dirichlet L -functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. **64** (1992) 265–338. MR1143227 (93a:11075)
- [8] M. R. Khan and I. E. Shparlinski, *On the maximal difference between an element and its inverse modulo n* , Periodica Math. Hungarica **47** (2003), 111–117. MR2024977 (2004k:11006)
- [9] M. R. Khan, I. E. Shparlinski and C. L. Yankov, *On the convex closure of the graph of modular inverses*, Experimental Math. **17** (2008), 91–104. MR2410119 (2009e:11003)
- [10] I. E. Shparlinski, *On the distribution of points on multidimensional modular hyperbolas*, Proc. Japan Acad. Sci., Ser. A **83** (2007), 5–9. MR2303621 (2008g:11161)
- [11] I. E. Shparlinski, *Distribution of modular inverses and multiples of small integers and the Sato–Tate conjecture on average*, Michigan Math. J. **56** (2008), 99–111. MR2433659 (2009e:11154)
- [12] T. Tao, *Structure and Randomness*, Amer. Math. Soc., Providence, RI, 2008. MR2459552

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 1409 WEST GREEN STREET, URBANA, ILLINOIS 61801
E-mail address: `ford@math.uiuc.edu`

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EASTERN CONNECTICUT STATE UNIVERSITY, WILLIMANTIC, CONNECTICUT 06226
E-mail address: `khanm@easternct.edu`

DEPARTMENT OF COMPUTING, MACQUARIE UNIVERSITY, SYDNEY, NSW 2109, AUSTRALIA
E-mail address: `igor@ics.mq.edu.au`