On the distribution of points on multidimensional modular hyperbolas

By Igor E. Shparlinski

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

(Communicated by Shigefumi Mori, m.j.a., Feb. 13, 2007)

Abstract: We study the distribution of points on the $(n+1)$-dimensional modular hyperbola $a_1 \cdots a_{n+1} \equiv c \pmod q$, where q and c are relatively prime integers. In particular, we show that an elementary argument leads to a straight-forward proof of a recent result of T. Zhang and W. Zhang, with a stronger error term. We also use character sums to obtain an asymptotic formula for the number of points in a given box that lie on such hyperbolas.

Key words: Multidimensional modular hyperbola; uniform distribution.

1. Introduction. As in [9], for arbitrary positive integers m, n, q, and c with $\gcd(c,q) = 1$ we consider the sum

$$M_{m,n}(q,c) = \sum_{\substack{a_1,\dots,a_{n+1}=1 \\ a_1\cdots a_{n+1}\equiv c \pmod q}}^{q} (a_1 \cdots a_n - a_{n+1})^m.$$

For $n = 1$ these sums are studied in [10, 11] using Kloosterman sums. Furthermore, for even $m = 2k$ and an arbitrary $n \geqslant 2$, similar tools are applied in [9] to derive the asymptotic formula

$$M_{2k,n}(q,c) = \frac{\varphi^n(q) q^{2kn}}{(2k+1)^n} + O\left(4^k q^{(2k+1)n-1/2} \tau^2(q) \log q\right),$$

where as usual $\varphi(q)$ is the Euler function and $\tau(q)$ is the number of integer divisors of q. Here we show that a direct and elementary argument leads us to a short proof of a stronger bound which also applies to odd m.

A more interesting problem than to estimate the sum $M_{m,n}(q,c)$ is to study the behaviour of the sums

$$S_{\mathbf{r},n}(q,c) = \sum_{\substack{a_1,\dots,a_{n+1}=1 \\ a_1\cdots a_{n+1}\equiv c \pmod q}}^{q} a_1^{r_1} \cdots a_{n+1}^{r_{n+1}}$$

with some real vector $\mathbf{r} = (r_1, \dots, r_{n+1})$, which are also considered in [9] (in some special cases). Here, using the approach of [7], we obtain precise and general results about the distribution of solutions to $a_1 \cdots a_{n+1} \equiv c \pmod q$. When $q = p$ is a prime, and $n \geqslant 4$, our estimate is more precise than that presented by Fouvry and Katz [2] as an example of their general bound for the number of points on algebraic varieties in a given box, which in turn is based on some deep methods from algebraic geometry. It should be noted that our improvement cannot be extended to other multivariate congruences and certainly does not affect the results of Fouvry and Katz [2] in their full generality.

Our result implies an estimate on the *discrepancy* $D_n(q,c)$ of the point set

$$\left\{\left(\frac{a_1}{q}, \dots, \frac{a_{n+1}}{q}\right) \mid 1 \leqslant a_1, \dots, a_{n+1} \leqslant q, \quad a_1 \cdots a_{n+1} \equiv c \pmod q\right\}, \tag{1}$$

which in turn immediately yields asymptotic formulas for average values of smooth functions on these points, see [5, Section 2.5]. In particular, one can easily derive asymptotic formulas for $S_{\mathbf{r},n}(q,c)$.

Throughout the paper, the implied constants in the symbols 'O' and '$\ll$' may depend on n but are uniform with respect to the other parameters such as c, m, and q. We recall that the notations $U = O(V)$ and $U \ll V$ are both equivalent to the assertion that the inequality $|U| \leqslant cV$ holds for some constant $c > 0$. We also use the symbol $o(1)$ to denote a function $f(q)$ such that $f(q) \to 0$ as $q \to \infty$.

2. Preparation.

2.1. Sums over reduced residue classes.

We recall the well-known bounds

$$\frac{d}{\varphi(d)} \ll \log\log d, \tag{2}$$

and

$$2^{\omega(d)} \leqslant \tau(d) = \exp\left(O(\log d/\log\log d)\right) \tag{3}$$

2000 Mathematics Subject Classiffcation. Primary 11A07, 11K38, 11L40.

where $\omega(d)$ is the number of distinct prime divisors of an integer $d \geqslant 1$, see [8, Sections I.5.2–I.5.4]

We need asymptotic formulas for the sums

$$\sigma_m(q) = \sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q} a^m \quad \text{and} \quad \varPhi_q(U) = \sum_{\substack{1\leqslant a\leqslant U\\ \gcd(a,q)=1}} 1,$$

which can be derived using the inclusion-exclusion principle.

Lemma 1. *For arbitrary positive integers m and q, we have*

$$\sigma_m(q) = \frac{\varphi(q)q^m}{m+1} + O\left(q^m\tau(q)\right).$$

Lemma 2. *For any positive integer $U \leqslant q$, we have*

$$\varPhi_q(U) = \frac{\varphi(q)}{q}U + O(2^{\omega(q)}).$$

2.2. Multiplicative character sums. Let $\mathcal{X}_q$ be the set of all multiplicative characters modulo q, thus $\#\mathcal{X}_q = \varphi(q)$. We recall that for $u \in \mathbf{Z}$,

$$(4) \quad \frac{1}{\varphi(q)} \sum_{\chi\in\mathcal{X}_q} \chi(u) = \begin{cases} 1 & \text{if } u \equiv 1 \pmod q, \\ 0 & \text{otherwise,} \end{cases}$$

see [6, Theorem 5.4]. We also use χ_0 to denote the principal character.

Using (4), one can immediately derive the following well known statement.

Lemma 3. *For any positive integer $U \leqslant q$, we have*

$$\sum_{\chi\in\mathcal{X}_q} \left|\sum_{a=1}^{U} \chi(a)\right|^2 \leqslant \varphi(q)U.$$

We then recall an estimate of the 4th moment of character sums which is given by Friedlander and Iwaniec [3].

Lemma 4. *For any positive integer $U \leqslant q$, we have*

$$\sum_{\substack{\chi\in\mathcal{X}_p\\ \chi\neq\chi_0}} \left|\sum_{a=1}^{U} \chi(a)\right|^4 \ll q^{1+o(1)}U^2.$$

We also need the following bound which is a combination of the Polya-Vinogradov (for $r = 1$) and Burgess (for $r \geqslant 2$) bounds, see [4, Theorems 12.5 and 12.6].

Lemma 5. *For any positive integer $U \leqslant q$ we have*

$$\max_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}} \left|\sum_{a=1}^{U} \chi(a)\right| \leqslant U^{1-1/r}q^{(r+1)/4r^2+o(1)}$$

with $r = 1, 2, 3$ for any q and with an arbitrary positive integer r if $q = p$ is a prime.

3. Main Results.

3.1. Bound for $M_{m,n}(q,c)$.

Theorem 6. *Let $n \geqslant 2$ be fixed. For arbitrary positive integers m, q, and c with* $\gcd(c,q) = 1$, *we have*

$$M_{m,n}(q,c) = \sigma_m(q)^n + O\left(mq^{(m+1)n-n+1}\right).$$

Proof. We note that

$$\begin{aligned} M_{m,n}(q,c) = &\sum_{\substack{a_1,\ldots,a_{n+1}=1\\ a_1\cdots a_{n+1}\equiv c \pmod q}}^{q} (a_1\cdots a_n)^m \\ &+ \sum_{\substack{a_1,\ldots,a_{n+1}=1\\ a_1\cdots a_{n+1}\equiv c \pmod q}}^{q} \sum_{\nu=1}^{m}(-1)^\nu\binom{m}{\nu}(a_1\cdots a_n)^{m-\nu}a_{n+1}^\nu \\ &= \sigma_m(q)^n \\ &+ O\left(\sum_{\substack{a_1,\ldots,a_{n+1}=1\\ a_1\cdots a_{n+1}\equiv c \pmod q}}^{q} \sum_{\nu=1}^{m}\binom{m}{\nu}q^{n(m-\nu)+\nu}\right) \\ &= \sigma_m(q)^n + O\left(q^{(m+1)n}\sum_{\nu=1}^{m}\binom{m}{\nu}q^{-\nu(n-1)}\right) \\ &= \sigma_m(q)^n + O\left(q^{(m+1)n}\left((1+q^{-n+1})^m - 1\right)\right). \end{aligned}$$

Clearly the result is trivial if $m > 2q^{n-1}$. Otherwise we have

$$(1+q^{-n+1})^m - 1 = O(mq^{-n+1})$$

which implies the desired bound. □

In particular we see that Theorem 6, combined with Lemma 1 and the bounds (2) and (3), yields the following statement:

Corollary 7. *For arbitrary positive integers m, q, and c such that*

$$\gcd(c,q) = 1 \qquad \text{and} \qquad m = O(1),$$

for every fixed integer $n \geqslant 2$, we have

$$M_{m,n}(q,c) = \frac{\varphi^n(q)q^{mn}}{(m+1)^n}\left(1 + O\left(q^{-1+o(1)}\right)\right).$$

3.2. Bound for $D_n(q,c)$. We recall that the discrepancy D of a set $\mathcal{T}$ of T points

$$\{(\eta_{1,t},\ldots,\eta_{s,t}) \in [0,1)^s \mid t = 1,\ldots,T\}$$

in the s-dimensional unit cube $[0,1)^s$ is defined as

$$D = \sup_{\Xi \subseteq [0,1)^s} \left| \frac{A(\Xi)}{T} - |\Xi| \right|,$$

where $A(\Xi)$ is the number of points of $\mathcal{T}$ in the box

$$\Xi = [0,\xi_1] \times \cdots \times [0,\xi_s] \subseteq [0,1)^s$$

of volume $|\Xi| = \xi_1 \cdots \xi_s$, and the supremum is taken over all such boxes. Thus to estimate the discrepancy $D_n(q,c)$ of points (1) it is enough to obtain an asymptotic formula for

$$N_n(\mathbf{U};q,c) = \#\{1 \leqslant a_i \leqslant U_i, i = 1,\ldots,n+1, \ | \ a_1 \cdots a_{n+1} \equiv c \pmod q\}$$

where $\mathbf{U} = (U_1,\ldots,U_{n+1}) \in \mathbf{Z}^{n+1}$ is an integer vector with $1 \leqslant U_i \leqslant q$, $i = 1,\ldots,n+1$.

We start with $n = 2$. The same argument works for any n but for $n \geqslant 3$ we can slightly modify the scheme and obtain a stronger bound.

Theorem 8. *For arbitrary positive integers q and c with $\gcd(c,q) = 1$, and a vector*

$$\mathbf{U} = (U_1,U_2,U_3) \in \mathbf{Z}^3$$

with $1 \leqslant U_1, U_2, U_3 \leqslant q$, the bound

$$N_2(\mathbf{U};q,c) = \frac{\Phi_q(U_1)\Phi_q(U_2)\Phi_q(U_3)}{\varphi(q)} + O\left((U_1U_2U_3)^{\alpha_r} q^{\beta_r + o(1)}\right)$$

holds with $r = 1,2,3$ for any q and with an arbitrary positive integer r if $q = p$ is a prime, where

$$\alpha_r = \frac{2r-1}{3r} \qquad \text{and} \qquad \beta_r = \frac{r+1}{4r^2}.$$

Proof. We see from (4) that

$$\begin{aligned} N_2(\mathbf{U};q,c) &= \sum_{a_1=1}^{U_1}\sum_{a_2=1}^{U_2}\sum_{a_3=1}^{U_3} \frac{1}{\varphi(q)} \sum_{\chi\in\mathcal{X}_q} \chi\left(a_1a_2a_3c^{-1}\right) \\ &= \frac{1}{\varphi(q)} \sum_{\chi\in\mathcal{X}_q} \chi\left(c^{-1}\right) \sum_{a_1=1}^{U_1}\sum_{a_2=1}^{U_2}\sum_{a_3=1}^{U_3} \chi\left(a_1a_2a_3\right). \end{aligned}$$

Extracting the term $\Phi_q(U_1)\Phi_q(U_2)\Phi_q(U_3)/\varphi(q)$ corresponding to the principal character χ_0, we obtain

$$N_2(\mathbf{U};q,c) = \frac{\Phi_q(U_1)\Phi_q(U_2)\Phi_q(U_3)}{\varphi(q)} + O(\Delta),$$

where

$$\Delta = \frac{1}{\varphi(q)} \sum_{\substack{\chi\in\mathcal{X}_q \\ \chi\neq\chi_0}} \prod_{i=1}^{3} \left| \sum_{a_i=1}^{U_i} \chi\left(a_i\right) \right|.$$

Thus, using the Hölder inequality, we deduce

$$\Delta^3 \leqslant \frac{1}{\varphi(q)^3} \prod_{i=1}^{3} \sum_{\substack{\chi\in\mathcal{X}_q \\ \chi\neq\chi_0}} \left| \sum_{a_i=1}^{U_i} \chi\left(a_i\right) \right|^3. \tag{5}$$

Applying Lemma 5 and then extending the summation to all characters $\chi \in \mathcal{X}_q$, we obtain that, with $r = 1,2,3$ for any q and with an arbitrary positive integer r if $q = p$ is a prime,

$$\sum_{\substack{\chi\in\mathcal{X}_q \\ \chi\neq\chi_0}} \left| \sum_{a_i=1}^{U_i} \chi\left(a_i\right) \right|^3 \leqslant U_i^{1-1/r} q^{(r+1)/4r^2+o(1)} \sum_{\chi\in\mathcal{X}_q} \left| \sum_{a_i=1}^{U_i} \chi\left(a_i\right) \right|^2$$

for each $i = 1,2,3$. We now infer from Lemma 3 that

$$\sum_{\substack{\chi\in\mathcal{X}_q \\ \chi\neq\chi_0}} \left| \sum_{a_i=1}^{U_i} \chi\left(a_i\right) \right|^3 \leqslant U_i^{2-1/r} q^{1+(r+1)/4r^2+o(1)}$$

which, via (2), (3) and (5), yields the desired bound. □

For $n \geqslant 3$ one use Lemma 4 instead of Lemma 3 to get a stronger bound.

Theorem 9. *For arbitrary positive integers $n \geqslant 3$, q, and c with $\gcd(c,q) = 1$, and a vector*

$$\mathbf{U} = (U_1,\ldots,U_{n+1}) \in \mathbf{Z}^{n+1}$$

with $1 \leqslant U_1,\ldots,U_{n+1} \leqslant q$, the bound

$$N_n(\mathbf{U};q,c) = \frac{\Phi_q(U_1)\cdots\Phi_q(U_{n+1})}{\varphi(q)} + O\left((U_1\cdots U_{n+1})^{\alpha_{n,r}} q^{\beta_{n,r}+o(1)}\right)$$

holds with $r = 1,2,3$ for any q and with an arbitrary positive integer r if $q = p$ is a prime, where

$$\alpha_{n,r} = 1 - \frac{n+2r-3}{(n+1)r} \quad \text{and} \quad \beta_{n,r} = \frac{(n-3)(r+1)}{4r^2}.$$

Proof. Arguing as in the proof of Theorem 8, we derive from (4) that

$$N_n(\mathbf{U};q,c) = \frac{\Phi_q(U_1)\cdots\Phi_q(U_{n+1})}{\varphi(q)} + O(\Delta),$$

where

$$\Delta = \frac{1}{\varphi(q)} \sum_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}} \prod_{i=1}^{n+1} \left| \sum_{a_i=1}^{U_i} \chi(a_i) \right|$$

$$\leqslant \frac{1}{\varphi(q)} \left(\prod_{i=1}^{n+1} \sum_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}} \left| \sum_{a_i=1}^{U_i} \chi(a_i) \right|^{n+1} \right)^{1/(n+1)} .$$

Applying Lemma 5 to the $(n-3)$th power of the character sums and then extending the summation to all characters $\chi \in \mathcal{X}_q$, we obtain that, for $r = 1, 2, 3$ for any q and with an arbitrary positive integer r if $q = p$ is a prime,

$$\sum_{\substack{\chi\in\mathcal{X}_q\\ \chi\neq\chi_0}} \left| \sum_{a_i=1}^{U_i} \chi(a_i) \right|^{n+1}$$

$$\leqslant \left(U_i^{1-1/r} q^{(r+1)/4r^2+o(1)} \right)^{n-3} \sum_{\chi\in\mathcal{X}_q} \left| \sum_{a_i=1}^{U_i} \chi(a_i) \right|^4$$

for $i = 1, \dots, n+1$. Now after a simple computation we obtain the desired bound. □

Taking $r = 1$, we derive from Lemma 2 and Theorems 8 and 9 the following estimate:

Corollary 10. *For arbitrary positive integers $n \geqslant 2$, q, and c with $\gcd(c, q) = 1$, the bound*

$$\max_{\mathbf{U}} \left| N_n(\mathbf{U}; q, c) - \frac{U_1 \cdots U_{n+1}}{q^{n+1}} \varphi(q)^n \right|$$

$$\leqslant \begin{cases} q^{3/2+o(1)} & \text{if } n = 2, \\ q^{n-1+o(1)} & \text{if } n \geqslant 3, \end{cases}$$

holds, where the maximum is taken over all vectors

$$\mathbf{U} = (U_1, \dots, U_{n+1}) \in \mathbf{Z}^{n+1}$$

with $1 \leqslant U_1, \dots, U_{n+1} \leqslant q$.

It is obvious that, for $n \geqslant 3$, the error in estimating the product $\Phi_q(U_1) \cdots \Phi_q(U_{n+1})$, which comes from Lemma 2, dominates the total error in Corollary 10. However, if $q = p$ is a prime then $\Phi_p(U) = U$ and this error does not appear at all. Hence, taking $r = 1$, we obtain:

Corollary 11. *For an integer $n \geqslant 2$, a prime $q = p$, and an arbitrary integer c with $\gcd(c, p) = 1$, the bound*

$$\max_{\mathbf{U}} \left| N_n(\mathbf{U}; p, c) - \frac{U_1 \cdots U_{n+1}}{p-1} \right| \leqslant p^{(n+1)/2+o(1)}$$

holds, where the maximum is taken over all vectors

$$\mathbf{U} = (U_1, \dots, U_{n+1}) \in \mathbf{Z}^{n+1}$$

with $1 \leqslant U_1, \dots, U_{n+1} < p$.

We are now ready to prove the bound for the discrepancy $D_n(q, c)$.

Theorem 12. *For arbitrary positive integers $n \geqslant 2$, q, and c with $\gcd(c, q) = 1$, the bound*

$$D_n(q, c) \leqslant \begin{cases} q^{-1/2+o(1)} & \text{if } n = 2, \\ q^{-1+o(1)} & \text{if } n \geqslant 3, \end{cases}$$

holds.

Proof. We have

$$D_n(q, c) = \max_{\Xi} \left| \frac{N_n\left((\lfloor \xi_1 q \rfloor, \dots, \lfloor \xi_{n+1} q \rfloor); q, c \right)}{\varphi(q)^n} - \xi_1 \cdots \xi_{n+1} \right|$$

where the maximum is taken over all boxes

$$\Xi = [0, \xi_1] \times \cdots \times [0, \xi_s] \subseteq [0, 1)^s.$$

Now Corollary 10 and the trivial the estimate

$$\max_{0 \leqslant \xi_1, \dots, \xi_{n+1} < 1} \left| \frac{\lfloor \xi_1 q \rfloor \cdots \lfloor \xi_{n+1} q \rfloor}{q^{n+1}} - \xi_1 \cdots \xi_{n+1} \right| \ll q^{-1}$$

yield the result. □

4. Remarks. Certainly one can obtain a more precise version of Lemma 1 and derive an asymptotic expansion for $\sigma_m(q)$.

We note that if $q = p$ is a prime, a generalisation of Lemma 4 is given by Ayyad, Cochrane and Zheng [1, Theorem 2] which applies to sums over arbitrary intervals $V + 1 \leqslant a \leqslant V + U$, while the result of Friedlander and Iwaniec [3] applies only to initial intervals $1 \leqslant a \leqslant U$.

For a prime $q = p$, we have $\Phi(U_i) = U_i + O(1)$ for any $U_i \in [1, p]$, $i = 1, \dots, n+1$. In this case the bound of Theorem 9 can be written as

$$N_n(\mathbf{U}; p, c) = \frac{U_1 \cdots U_{n+1}}{p-1} \Big(1 + O\Big((U_1 \cdots U_{n+1})^{\alpha_{n,r}-1} p^{\beta_{n,r}+1+o(1)} \Big) \Big)$$

$$= \frac{U_1 \cdots U_{n+1}}{p-1} \left(1 + O\left(p^{-\delta} \right) \right)$$

$$= \frac{U_1 \cdots U_{n+1}}{p} \left(1 + O\left(p^{-\delta} \right) \right)$$

for any fixed positive ε and δ with

$$\delta < \min\{1, \varepsilon(n+1)(1-\alpha_{n,r})\} \\ = \min\{1, \varepsilon(n+2r-3)/r\}$$

provided that

$$U_1 \cdots U_{n+1} \geqslant p^{(\gamma_{n,r}+\varepsilon)(n+1)},$$

where

$$\gamma_{n,r} = \frac{\beta_{n,r}+1}{(1-\alpha_{n,r})(n+1)} = \frac{4r^2+(n-3)(r+1)}{4r(n+2r-3)}.$$

Setting $r = \lceil n^{1/2} \rceil$, say, we obtain

$$\lim_{n\to\infty} \gamma_{n,\lceil n^{1/2}\rceil} = \frac{1}{4}.$$

Hence for any ε and sufficiently large n we have a nontrivial asymptotic formula for $N_n(\mathbf{U}; p, c)$ provided that

$$U_1 \cdots U_{n+1} \geqslant p^{(1/4+\varepsilon)(n+1)}.$$

We recall that it has been noticed by Fouvry and Katz [2] that very deep results about the distribution of points on algebraic varieties even in the special case of modular hyperbolas, give a nontrivial bound on $N_n(\mathbf{U}; p, c)$ only for

$$U_1 \cdots U_{n+1} \geqslant p^{(1/2+\varepsilon)(n+1)}$$

(in fact only the case $U_1 = \cdots = U_{n+1}$ is discussed in [2] but it can be extended to the case of arbitrary $U_1, \ldots, U_{n+1}$ without any difficulty). One easily verifies that

$$\min_{r\geqslant 1} \gamma_{n,r} \leqslant \gamma_{n,2} = \frac{3n+7}{8n+8} \leqslant \frac{19}{40} < \frac{1}{2}$$

for $n \geqslant 4$. Thus, as we have mentioned, for $n \geqslant 4$, our result is stronger than the one following from [2] specialized to our situation.

Acknowledgement. The author would like to thank the referee for a patient and careful reading which revealed a number of minor inaccuracies in the original version of the paper. This work was supported in part by ARC grant DP0556431.

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$, and mean values of character sums, J. Number Theory **59** (1996), no. 2, 398–413.

[2] E. Fouvry and N. Katz, A general stratification theorem for exponential sums, and applications, J. Reine Angew. Math. **540** (2001), 115–166.

[3] J. B. Friedlander and H. Iwaniec, The divisor problem for arithmetic progressions, Acta Arith. **45** (1985), no. 3, 273–277.

[4] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[5] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Intersci., New York, 1974.

[6] R. Lidl and H. Niederreiter, *Finite fields*, Second edition, Cambridge Univ. Press, Cambridge, 1997.

[7] I. E. Shparlinski, On a generalisation of a Lehmer problem. (Preprint).

[8] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Translated from the second French edition (1995) by C. B. Thomas, Cambridge Univ. Press, Cambridge, 1995.

[9] T. Zhang and W. Zhang, A generalization on the difference between an integer and its inverse modulo q. II, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 1, 7–11.

[10] W. Zhang, On the difference between an integer and its inverse modulo n, J. Number Theory **52** (1995), no. 1, 1–6.

[11] W. Zhang, On the difference between an integer and its inverse modulo n. II, Sci. China Ser. A **46** (2003), no. 2, 229–238.