BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 58, No. 1, 2010

NUMBER THEORY

Visible Points on Modular Exponential Curves

by

Tsz Ho CHAN and Igor E. SHPARLINSKI

Presented by Jerzy KACZOROWSKI

Summary. We obtain an asymptotic formula for the number of visible points (x,y), that is, with $\gcd(x,y)=1$, which lie in the box $[1,U]\times[1,V]$ and also belong to the exponential modular curves $y\equiv ag^x \pmod p$. Among other tools, some recent results of additive combinatorics due to J. Bourgain and M. Z. Garaev play a crucial role in our argument.

1. Introduction. We consider points on the exponential modular curves

$$\mathcal{E}_{a,g,p}=\{(x,y): y\equiv ag^x \pmod p\}.$$

Furthermore, for real U and V we use $\mathcal{E}_{a,g,p}(U,V)$ to denote the set of points $(x,y)\in\mathcal{E}_{a,g,p}$ which lie in the box $[1,U]\times[1,V]$.

Here we obtain an asymptotic formula for the number $N_{a,g,p}(U,V)$ of *visible points* $(x,y)\in\mathcal{E}_{a,g,p}(U,V)$, that is, points satisfying $\gcd(x,y)=1$.

We note that visible points on some other curves have been studied in [10, 11, 12]. However, their methods do not extend to the points on $\mathcal{E}_{a,g,p}$. In fact, a result of [2] is a crucial ingredient of our argument.

Throughout the paper, the implied constants in the symbols "O" and "$\ll$" are absolute (we recall that $A=O(B)$ and $A\ll B$ are both equivalent to the inequality $|A|\le cB$ with some constant $c>0$).

Theorem 1. *For $(a,p)=1$ and any primitive root ϑ modulo p,*

$$N_{a,\vartheta,p}(U,V)=\frac{6}{\pi^2}\cdot\frac{UV}{p}+O\biggl(\biggl(\frac{U^{1/2}V^{1/2}}{p^{1/4}}+\frac{U}{V^{1/35}}+\frac{V}{U^{1/35}}\biggr)p^{o(1)}\biggr)$$

for $1\le U,V\le p-1$ with $UV\ge p^{3/2}$.

2010 *Mathematics Subject Classification*: 11A07, 11B30.
Key words and phrases: exponential congruences, visible points.

DOI: 10.4064/ba58-1-2

Note that the bound of Theorem 1 is nontrivial if $\min\{U,V\} \ge p^{35/36+\varepsilon}$ for some fixed $\varepsilon > 0$.

2. Preparations. The following estimate is very well known ([7, 9] and also [3, 4, 6, 8]).

Let $M_{a,g,p}(U,V)$ be the number of points $(x,y) \in \mathcal{E}_{a,g,p}(U,V)$.

Lemma 2. *For $(ag,p) = 1$ and $U,V \le t$ where t is the multiplicative order of g modulo p,*

$$M_{a,g,p}(U,V) = \frac{UV}{p} + O(p^{1/2}(\log p)^2).$$

We now present an upper bound on $M_{a,g,p}(U,V)$ which is better than that in Lemma 2 for small U and V.

Lemma 3. *For $(ag,p) = 1$ and $U,V \le t$ where t is the multiplicative order of g modulo p, we have*

$$M_{a,g,p}(U,V) \ll \frac{UV}{p} + \frac{V}{U^{1/11+o(1)}} + \frac{U}{V^{1/11+o(1)}}$$

as $U,V \to \infty$.

Proof. By [2, Corollary 5], we have

$$M_{a,g,p}(U,U) \ll \frac{U^2}{p} + \frac{U}{U^{1/11+o(1)}}.$$

For $V \ge U$, we just divide the rectangle into $O(V/U)$ squares with side length U. Then

$$M_{a,g,p}(U,V) \ll \frac{V}{U}\left(\frac{U^2}{p} + \frac{U}{U^{1/11+o(1)}}\right),$$

which gives the desired estimate. The proof for $U \ge V$ is similar. ∎

We denote by $R_{a,g,p}(K;D)$ the number of solutions to the congruence

$$ad \equiv g^d \pmod p, \qquad K+1 \le d \le K+D.$$

Lemma 4. *For $(ag,p) = 1$ and $D \le p$, we have*

$$R_{a,g,p}(K;D) \ll D^{1/2}.$$

Proof. Clearly $R_{a,g,p}(K;D)^2$ is equal to the number of solutions to the system of congruences

$$ad \equiv g^d \pmod p \quad \text{and} \quad af \equiv g^f \pmod p, \quad K+1 \le d,f \le K+D.$$

Thus writing $f = d+e$ we see that

$$R_{a,g,p}(K;D)^2 \le Q_{a,g,p}(K;D), \tag{1}$$

where $Q_{a,g,p}(K;D)$ is the number of solutions to the system of congruences

$$ad \equiv g^d \pmod p \quad \text{and} \quad a(d+e) \equiv g^{d+e} \pmod p,$$

where

$$-D < e < D \quad \text{and} \quad K+1 \le d \le K+D.$$

We see that the above congruences imply

$$e \equiv d(g^e - 1) \pmod p. \tag{2}$$

For every e with $g^e \not\equiv 1 \pmod p$ the congruence (2) defines d uniquely, so there are $O(D)$ such solutions (e,d). For $g^e \equiv 1 \pmod p$ we see from (2) that $e \equiv 0 \pmod p$, which in turn implies $e = 0$ (and d can take any values with $K+1 \le d \le K+D$); so again there are $O(D)$ such solutions (e,d). Therefore

$$Q_{a,g,p}(K;D) \ll D,$$

and recalling (1) we conclude the proof. ∎

3. Proof of Theorem 1. For $(a,p) = 1 = (\vartheta, p)$, we have $(a\vartheta^y, p) = 1$. By the inclusion-exclusion principle,

$$\begin{aligned} N_{a,\vartheta,p}(U,V) &= \sum_{\substack{d=1\\ \gcd(d,p)=1}}^{\infty} \mu(d) \sum_{\substack{(x,y)\in\mathcal{E}_{a,\vartheta,p}(U,V)\\ d\mid(x,y)}} 1 \\ &= \sum_{\substack{d=1\\ \gcd(d,p)=1}}^{\infty} \mu(d) \sum_{1\le u\le U/d} \sum_{\substack{1\le v\le V/d\\ dv\equiv a\vartheta^{du} \pmod p}} 1 \\ &= \sum_{\substack{d=1\\ \gcd(d,p)=1}}^{\infty} \mu(d) M_{a\bar{d},\vartheta^d,p}\left(\frac{U}{d}, \frac{V}{d}\right), \end{aligned}$$

where $\overline{d}$ is the multiplicative inverse of d modulo p and $\mu(d)$ is the Möbius function (see [5, Section 16.3]). We now choose two real parameters $p \ge \Delta > \delta \ge 1$ and write

$$N_{a,\vartheta,p}(U,V) = \Sigma_1 + \Sigma_2 + \Sigma_3, \tag{3}$$

where

$$\Sigma_1 = \sum_{\substack{\gcd(d,p)=1\\ 1\le d\le\delta}} \mu(d) M_{a\bar{d},\vartheta^d,p}\left(\frac{U}{d}, \frac{V}{d}\right),$$

$$\Sigma_2 = \sum_{\substack{\gcd(d,p)=1\\ \delta<d\le\Delta}} \mu(d) M_{a\bar{d},\vartheta^d,p}\left(\frac{U}{d}, \frac{V}{d}\right),$$

$$\Sigma_3 = \sum_{\substack{\gcd(d,p)=1\\ d>\Delta}} \mu(d) M_{a\bar{d},\vartheta^d,p}\left(\frac{U}{d},\frac{V}{d}\right).$$

We use Lemmas 2, 3 and 4 to estimate Σ_1, Σ_2 and Σ_3 respectively.

By Lemma 2,

$$\begin{aligned}\Sigma_1 &= \sum_{d\le\delta}\mu(d)\left(\frac{U}{d}\cdot\frac{V}{d}\cdot\frac{1}{p} + O(p^{1/2}(\log p)^2)\right)\\ &= \frac{UV}{p}\sum_{d\le\delta}\frac{\mu(d)}{d^2} + O(\delta p^{1/2}(\log p)^2)\\ &= \frac{6}{\pi^2}\cdot\frac{UV}{p} + O\left(\frac{UV}{p\delta} + \delta p^{1/2}(\log p)^2\right)\end{aligned}$$

since

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

(see [5, Equation (17.2.2)]).

Without loss of generality, we can assume that $V \ge U$. Then by Lemma 3,

$$\begin{aligned}\Sigma_2 &\ll \sum_{\delta<d\le\Delta}\left(\frac{UV}{d^2p} + VU^{-1/11}d^{-10/11}p^{o(1)}\right)\\ &\ll \frac{UV}{p\delta} + VU^{-1/11}\Delta^{1/11}p^{o(1)}.\end{aligned}$$

We now define an integer L by the inequalities

$$2^L\Delta < \min(U,V) \le 2^{L+1}\Delta$$

and write

$$\begin{aligned}\Sigma_3 &\le \sum_{i=0}^{L}\sum_{2^i\Delta<d\le 2^{i+1}\Delta} M_{a\bar{d},\vartheta^d,p}\left(\frac{U}{2^i\Delta},\frac{V}{2^i\Delta}\right)\\ &= \sum_{i=0}^{L}\sum_{u\le\frac{U}{2^i\Delta}}\sum_{v\le\frac{V}{2^i\Delta}}\sum_{\substack{2^i\Delta<d\le 2^{i+1}\Delta\\ d\equiv a\bar{v}\vartheta^{du} \pmod p}} 1.\end{aligned}$$

Thus by Lemma 4,

$$\Sigma_3 \ll \sum_{i=0}^{L}\sum_{u\le\frac{U}{2^i\Delta}}\sum_{v\le\frac{V}{2^i\Delta}} (2^i\Delta)^{1/2} \ll UV\Delta^{-3/2}.$$

Substituting the above estimates in (3), we obtain

$$
\begin{aligned}
(4)\qquad N_{a,\vartheta,p}(U,V) &- \frac{6}{\pi^2}\cdot\frac{UV}{p} \\
&\ll \frac{UV}{p\delta} + \delta p^{1/2+o(1)} + VU^{-1/11}\varDelta^{1/11}p^{o(1)} + UV\varDelta^{-3/2}.
\end{aligned}
$$

We now choose

$$\delta = U^{1/2}V^{1/2}p^{-3/4}$$

to balance the first and the second terms and

$$\varDelta = U^{24/35}$$

to balance the third and the fourth terms on the right hand side of (4) (and note that since $UV \ge p^{3/2}$ and $U \le V < p$, the condition $p \ge \varDelta > \delta \ge 1$ is satisfied), getting

$$N_{a,\vartheta,p}(U,V) - \frac{6}{\pi^2}\cdot\frac{UV}{p} \ll (U^{1/2}V^{1/2}p^{-1/4} + VU^{-1/35})p^{o(1)},$$

which gives the desired result.

4. Comments. We remark that Lemma 3, which in turn depends on some results of additive combinatorics due to J. Bourgain and M. Z. Garaev [1], is an essential ingredient of our proof. Just a combination of Lemmas 2 and 4 is not sufficient to derive an asymptotic formula for $N_{a,\vartheta,p}(U,V)$. On the other hand, the ingredients of this paper are quite sufficient to obtain an asymptotic formula for $N_{a,g,p}(U,V)$ also in the case when g is not necessarily a primitive root modulo p.

References

[1] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Philos. Soc. 146 (2008), 1–21.

[2] T. H. Chan and I. E. Shparlinski, *On the concentration of points on modular hyperbolas and exponential curves*, Acta Arith. 142 (2010), 59–66.

[3] C. Cobeli, S. Gonek and A. Zaharescu, *On the distribution of small powers of a primitive root*, J. Number Theory 88 (2001), 49–58.

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

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, The Clarendon Press, Oxford Univ. Press, New York, 1979.

[6] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and Their Applications*, Cambridge Univ. Press, Cambridge, 1999.

[7] N. M. Korobov, *On the distribution of digits in periodic fractions*, Mat. Sb. 89 (1972), 654–670 (in Russian).

[8] H. L. Montgomery, *Distribution of small powers of a primitive root*, in: Advances in Number Theory, Clarendon Press, Oxford, 1993, 137–149.

[9] H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. 84 (1978), 957–1041.
[10] I. E. Shparlinski, *Primitive points on a modular hyperbola*, Bull. Polish Acad. Sci. Math. 54 (2006), 193–200.
[11] I. E. Shparlinski and J. F. Voloch, *Visible points on curves over finite fields*, ibid. 55 (2007), 193–199.
[12] I. E. Shparlinski and A. Winterhof, *Visible points on multidimensional modular hyperbolas*, J. Number Theory 128 (2008), 2695–2703.

Tsz Ho Chan
Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152, U.S.A.
E-mail: tchan@memphis.edu

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

Received December 8, 2009;
received in final form February 26, 2010 (7739)