Bull. Aust. Math. Soc. **97** (2018), 353–359
doi:10.1017/S0004972717001186

VISIBLE POINTS ON EXPONENTIAL CURVES

SIMON MACOURT

(Received 25 October 2017; accepted 16 November 2017; first published online 7 March 2018)

Abstract

We provide two new bounds on the number of visible points on exponential curves modulo a prime for all choices of primes. We also provide one new bound on the number of visible points on exponential curves modulo a prime for almost all primes.

2010 *Mathematics subject classification*: primary 11A07; secondary 11B30.
Keywords and phrases: exponential curve, visible points.

1. Introduction

1.1. Set up. We define

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

to be the set of points on an exponential modular curve. Furthermore, for real U, V, we define $\mathcal{E}_{a,g,p}(U, V)$ to be the set of points

$$(x, y) \in \mathcal{E}_{a,g,p} \cap ([1, U] \times [1, V]).$$

We also define the number of visible points $N_{a,g,p}(U, V)$ to be the number of points for which $(x, y) \in \mathcal{E}_{a,g,p}(U, V)$ and $\gcd(x, y) = 1$. Finally, we define $M_{a,g,p}(U, V)$ to be the number of points for which $(x, y) \in \mathcal{E}_{a,g,p}(U, V)$.

The visible points on these curves are the points which are visible from the origin. Visible points over integer-valued polynomials have recently been studied in [5] and visible points on modular hyperbolas have been studied in [4, 6]. These problems are related to the classical problems of studying the distribution of values of various arithmetic functions. The techniques involved in finding bounds for the visible points on the curves just mentioned do not extend to the case of exponential curves. As one can see in our proof of Lemma 2.5, we are using the property that products of exponentials give information involving sums. Hence our bounds are dependent on results from additive combinatorics (see [1, Lemma 20], as well as the proof of [2, Theorem 31]).

1.2. Main results. We improve previous results (see (1.1) below) by giving two bounds based on recent results of Bourgain *et al.* [1, Theorems 23 and 24].

THEOREM 1.1. *For* $\gcd(a,p)=1$, *any* g *of multiplicative order* t *modulo* p *and* $U,V \le t$,

$$N_{a,g,p}(U,V) = \frac{6}{\pi^2}\cdot\frac{UV}{p} + \begin{cases} O\left(\left(\dfrac{U^{3/4}V^{1/4}}{p^{1/8}} + U^{1/4}V^{5/8}\right)p^{o(1)}\right) & \text{for } U^3V \ge p^{5/2},\\ O\left(\left(\dfrac{U^{6/7}V^{1/7}}{p^{1/28}} + U^{3/13}V^{7/13}\right)p^{o(1)}\right) & \text{for } U^6V \ge p^{15/4}. \end{cases}$$

We also give a new bound for almost all p, using [2, Theorem 31].

THEOREM 1.2. *For sufficiently large positive integers* T, U *and* V *and for all but* $o(p/\log p)$ *primes* $p \in [T, 2T]$, *and for any* a *with* $\gcd(a,p)=1$, *any* g *of multiplicative order* t *modulo* p *and* $U,V \le t$,

$$N_{a,g,p}(U,V) = \frac{6}{\pi^2}\cdot\frac{UV}{p} + O\left(\left(\frac{U^{2/13}V^{11/13}}{p^{1/26}} + U^{7/22}V^{13/22}\right)p^{o(1)}\right)$$

for $U^2V^{11} \ge p^7$.

1.3. Comparing bounds. We recall the result of Chan and Shparlinski [3], for $\gcd(a,p)=1$ and any primitive root g modulo p,

$$N_{a,g,p}(U,V) = \frac{6}{\pi^2}\cdot\frac{UV}{p} + O\left(\left(\frac{U^{1/2}V^{1/2}}{p^{1/4}} + \frac{U}{V^{1/35}} + \frac{V}{U^{1/35}}\right)p^{o(1)}\right) \tag{1.1}$$

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

Theorems 1.1 and 1.2 are stronger than (1.1) for all possible values of U and V. Our results rely on recent bounds in additive combinatorics as well as some different methods to improve the bound of Σ_2 in the proof of Theorems 1.1 and 1.2. We also mention that for $U = V$ our bounds are stronger than the trivial bound

$$N_{a,g,p}(U,V) \le \min(U,V)$$

over their valid regions. We also see that for $U = V$ the first bound of Theorem 1.1 is always stronger than the second and that of Theorem 1.2 over the regions for which our new bounds are valid.

We notice that Theorem 1.2 is strongest for U much larger than V. Here we give examples when each result is strongest. One can check that the first bound of Theorem 1.1 is strongest for $U = V = p^{3/4}$, the second bound of Theorem 1.1 is strongest for $U = p^{3/4}, V = p^{7/8}$, and Theorem 1.2 is strongest for $U = p^{5/6}, V = p^{2/3}$.

We also mention that one can get another bound for all p using a result of [7, Lemma 2.1]. However, when compared to the bound from Theorem 1.1, one can see that it is trivial. Similarly, one can get another bound for almost all p using Lemma 2.5 with $n = 2$. Again, comparing this bound with Theorem 1.1 one can see that it is trivial.

https://doi.org/10.1017/S0004972717001186 Published online by Cambridge University Press

2. Set-up

We recall the following result given in [1].

LEMMA 2.1. *Let* $\gcd(a, p) = 1$ *and* g *be of multiplicative order* t *modulo* p. *Let* $\mathcal{I}_1$ *and* $\mathcal{I}_2$ *be two intervals consisting of* h_1 *and* h_2 *consecutive numbers respectively where* $h_2 \le t$. *Then*

$$M_{a,g,p}(\mathcal{I}_1, \mathcal{I}_2) < \min\left(\left(\frac{h_1}{p^{1/3}h_2^{1/6}} + 1\right)h_2^{1/2+o(1)}, \left(\frac{h_1}{p^{1/8}h_2^{1/6}} + 1\right)h_2^{1/3+o(1)}\right).$$

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

$$ad \equiv g^d \pmod p \quad \text{with } K + 1 \le d \le K + D.$$

We also recall the following lemmas given in [3].

LEMMA 2.2. *For* $\gcd(ag, p) = 1$ *and* $U, V \le t$ *where* t *is the multiplicative order of* g *modulo* p,

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

LEMMA 2.3. *For* $\gcd(ag, p) = 1$ *and* $D \le p$,

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

We define $K_\nu(p, h, s)$ to be the number of solutions of

$$(x_1 + s)\dots(x_\nu + s) \equiv (y_1 + s)\dots(y_\nu + s) \not\equiv 0 \pmod p,$$

where $x_i, y_i \in [1, h]$ for $i = 1, \dots, \nu$ and $s \in \mathbb{F}_p$. We recall the following result from [2, Theorem 31].

LEMMA 2.4. *Let* $\nu \ge 1$ *be a fixed positive integer. For sufficiently large positive integers* $T > h \ge 3$,

$$K_\nu(p, h, s) \le (h^\nu + h^{2\nu-1/2}T^{-1/2}) \exp\left(O\left(\frac{\log h}{\log\log h}\right)\right),$$

for all $s \in \mathbb{F}_p$ *and all but* $o(T/\log^2 T)$ *primes* $p \le T$.

We now give the following result. Our proof follows that of [1, Theorem 23].

LEMMA 2.5. *Let* n *be a fixed integer with* $n \ge 2$. *Let* h_1, h_2 *and* T *be sufficiently large fixed positive integers and let* p *be a prime with* $p \in [T, 2T]$ *and* $3 \le h_2 \le T$. *Let* g *be of multiplicative order* t *modulo* p *and* $\mathcal{I}_1$ *and* $\mathcal{I}_2$ *be two intervals consisting of* h_1 *and* h_2 *consecutive integers respectively with* $h_1, h_2 \le t$. *Then*

$$M_{a,g,p}(\mathcal{I}_1, \mathcal{I}_2) \le n^{1/(2n)}h_1^{1/(2n)}(h_2^{1/2} + h_2^{1-1/(4n)}p^{-1/(4n)})h_2^{o(1)}$$

for all but $o(p/\log^2 p)$ *primes* p *with* $\gcd(a, p) = 1$.

https://doi.org/10.1017/S0004972717001186 Published online by Cambridge University Press

PROOF. We recall that $M_{a,g,p}(\mathcal{I}_1, \mathcal{I}_2)$ is the number of solutions to

$$y \equiv ag^x \pmod{p}. \tag{2.1}$$

Define $\mathcal{Y} \subseteq \mathcal{I}_2$ to be the values of y which satisfy the congruence (2.1). Let

$$T(\lambda) = \#\{(y_1, \dots, y_n) \in \mathcal{Y}^n : \lambda \equiv y_1 \dots y_n \pmod{p}\}.$$

Therefore,

$$\#\{\lambda : T(\lambda) > 0\} \le nh_1$$

since

$$\lambda \equiv y_1 \dots y_n \equiv a^n g^{x_1 + \dots + x_n}.$$

By the Cauchy inequality

$$\sum_{\lambda \in \mathbb{F}_p^*} T(\lambda)^2 \ge \frac{1}{nh_1} \Big(\sum_{\lambda \in \mathbb{F}_p^*} T(\lambda) \Big)^2 = \frac{|\mathcal{Y}|^{2n}}{nh_1}.$$

Clearly,

$$\begin{aligned} \sum_{\lambda \in \mathbb{F}_p^*} T(\lambda)^2 &= \#\{(y_1, \dots, y_n, z_1, \dots, z_n) \in \mathcal{Y}^{2n} : y_1 \dots y_n \equiv z_1 \dots z_n \pmod{p}\} \\ &\le \#\{(y_1, \dots, y_n, z_1, \dots, z_n) \in \mathcal{I}_2^{2n} : y_1 \dots y_n \equiv z_1 \dots z_n \pmod{p}\}. \end{aligned}$$

Hence, by Lemma 2.4

$$\sum_{\lambda \in \mathbb{F}_p^*} T(\lambda)^2 \le (h_2^n + h_2^{2n-1/2} p^{-1/2}) h^{o(1)}$$

for all but $o(T/\log^2 T)$ primes p. Therefore,

$$\frac{|\mathcal{Y}|^{2n}}{nh_1} \le (h_2^n + h_2^{2n-1/2} p^{-1/2}) h^{o(1)}.$$

Rearranging, we complete the proof. □

3. Proofs of main results

3.1. Proof of Theorem 1.1. Our proof follows that of [3, Theorem 1], however we use Lemma 2.1 in place of Lemma 3 from [3].

From [3, Equation (3)],

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

https://doi.org/10.1017/S0004972717001186 Published online by Cambridge University Press

where

$$\begin{aligned}\Sigma_1 &= \sum_{\substack{\gcd(d,p)=1\\ 1\le d\le\delta}} \mu(d) M_{a\bar{d},g^d,p}\Big(\frac{U}{d},\frac{V}{d}\Big),\\ \Sigma_2 &= \sum_{\substack{\gcd(d,p)=1\\ \delta\le d\le\Delta}} \mu(d) M_{a\bar{d},g^d,p}\Big(\frac{U}{d},\frac{V}{d}\Big),\\ \Sigma_3 &= \sum_{\substack{\gcd(d,p)=1\\ d\ge\Delta}} \mu(d) M_{a\bar{d},g^d,p}\Big(\frac{U}{d},\frac{V}{d}\Big),\end{aligned} \tag{3.1}$$

for two real parameters δ and Δ, which will be chosen later. From [3],

$$\Sigma_1 = \frac{6}{\pi^2}\cdot\frac{UV}{p} + O\Big(\frac{UV}{p\delta} + \delta p^{1/2}(\log p)^2\Big)$$

and

$$\Sigma_3 \ll UV\Delta^{-3/2},$$

using Lemmas 2.2 and 2.3 respectively. We now use the first result of Lemma 2.1, combined with the triangle inequality, to obtain

$$\begin{aligned}\Sigma_2 &< \sum_{\substack{\gcd(d,p)=1\\ \delta\le d\le\Delta}} \Big(\frac{U}{p^{1/3}d^{5/6}V^{1/6}}+1\Big)\Big(\frac{V}{d}\Big)^{1/2+o(1)}\\ &\ll \frac{UV^{1/3+o(1)}}{\delta^{1/3}p^{1/3}} + \Delta^{1/2}V^{1/2+o(1)}.\end{aligned}$$

Therefore,

$$\begin{aligned}&N_{a,g,p}(U,V) - \frac{6}{\pi^2}\cdot\frac{UV}{p}\\ &\quad\ll \frac{UV}{p\delta} + \delta p^{1/2+o(1)} + \frac{UV^{1/3+o(1)}}{\delta^{1/3}p^{1/3}} + \Delta^{1/2}V^{1/2+o(1)} + UV\Delta^{-3/2}.\end{aligned} \tag{3.2}$$

Now,

$$\frac{UV}{p\delta} \le \frac{UV^{1/3+o(1)}}{\delta^{1/3}p^{1/3}}$$

since $\delta \ge 1$ and $U, V \le p$. We balance the second and third terms in (3.2) by selecting

$$\delta = \frac{U^{3/4}V^{1/4}}{p^{5/8}}.$$

For $\delta \ge 1$ we need

$$U^3V \ge p^{5/2}.$$

https://doi.org/10.1017/S0004972717001186 Published online by Cambridge University Press

We also balance the fourth and fifth terms in (3.2) by selecting

$$\Delta = U^{1/2}V^{1/4+o(1)}.$$

It is clear that $\delta \le \Delta$, therefore

$$N_{a,g,p}(U,V) - \frac{6}{\pi^2}\cdot\frac{UV}{p} \ll \left(\frac{U^{3/4}V^{1/4}}{p^{1/8}} + U^{1/4}V^{5/8}\right)p^{o(1)}.$$

We repeat the above but use the second result of Lemma 2.1 for Σ_2. Hence,

$$\begin{aligned}\Sigma_2 &< \sum_{\substack{\gcd(d,p)=1\\ \delta\le d\le\Delta}} \left(\frac{U}{p^{1/8}d^{5/6}V^{1/6}} + 1\right)\left(\frac{V}{d}\right)^{1/3+o(1)}\\ &\ll \left(\frac{UV^{1/6}}{\delta^{1/6}p^{1/8}} + \Delta^{2/3}V^{1/3}\right)p^{o(1)}.\end{aligned}$$

Choosing

$$\delta = \frac{U^{6/7}V^{1/7}}{p^{15/28}},$$

with $U^6V \ge p^{15/4}$, and

$$\Delta = U^{6/13}V^{4/13},$$

it is clear that $\delta \le \Delta$, therefore

$$N_{a,g,p}(U,V) - \frac{6}{\pi^2}\cdot\frac{UV}{p} \ll \left(\frac{U^{6/7}V^{1/7}}{p^{1/28}} + U^{3/13}V^{7/13}\right)p^{o(1)}.$$

This completes the proof. □

3.2. Proof of Theorem 1.2. We follow the proof of Theorem 1.1 picking up after (3.1). We now use Lemma 2.5, taking $n = 3$, to obtain

$$\begin{aligned}\Sigma_2 &\le \sum_{\substack{\gcd(d,p)=1\\ \delta\le d\le\Delta}} 3^{1/6}\left(\frac{U}{d}\right)^{1/6}\left(\left(\frac{V}{d}\right)^{1/2} + \left(\frac{V}{d}\right)^{11/12}p^{-1/12}\right)p^{o(1)}\\ &\ll U^{1/6}(V^{11/12}p^{-1/12}\delta^{-1/12} + \Delta^{1/3}V^{1/2})p^{o(1)}\end{aligned}$$

for all but $o(p/\log^2 p)$ primes p. Therefore,

$$\begin{aligned}&N_{a,g,p}(U,V) - \frac{6}{\pi^2}\cdot\frac{UV}{p}\\ &\quad\ll \frac{UV}{p\delta} + \delta p^{1/2+o(1)} + U^{1/6}(V^{11/12}p^{-1/12}\delta^{-1/12} + \Delta^{1/3}V^{1/2})p^{o(1)} + UV\Delta^{-3/2}. \quad (3.3)\end{aligned}$$

We note the first term is dominated by the third. We balance the second and third terms in (3.3) by selecting

$$\delta = \frac{U^{2/13}V^{11/13}}{p^{7/13}}.$$

https://doi.org/10.1017/S0004972717001186 Published online by Cambridge University Press

For $\delta \geq 1$ we need

$$U^2V^{11} \geq p^7.$$

Similarly, we balance the third and fourth terms by selecting

$$\Delta = U^{5/11}V^{3/11}.$$

Clearly $\delta \leq \Delta$, therefore

$$N_{a,g,p}(U,V) - \frac{6}{\pi^2} \cdot \frac{UV}{p} \ll (U^{2/13}V^{11/13}p^{-1/26} + U^{7/22}V^{13/22})p^{o(1)}$$

for all but $o(T/\log^2 T)$ primes $p \leq T$. This concludes the proof. □

Acknowledgement

The author would like to thank the referee for his comments and suggestions regarding the presentation of this manuscript.

References

[1] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Tr. Mat. Inst. Steklova* **280** (2013), 67–96.
[2] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'Multiplicative congruences with variables from short intervals', *J. Anal. Math.* **124** (2014), 117–147.
[3] T. H. Chan and I. E. Shparlinski, 'Visible points on modular exponential curves', *Bull. Pol. Acad. Sci. Math.* **58**(1) (2010), 17–22.
[4] I. E. Shparlinski, 'Primitive points on modular hyperbola', *Bull. Pol. Acad. Sci. Math.* **54**(3–4) (2006), 193–200.
[5] I. E. Shparlinski and J. F. Voloch, 'Visible points on curves over finite fields', *Bull. Pol. Acad. Sci. Math.* **55**(3) (2007), 193–199.
[6] I. E. Shparlinski and A. Winterhof, 'Visible points on multidimensional modular hyperbolas', *J. Number Theory* **128**(9) (2008), 2695–2703.
[7] I. E. Shparlinski and K.-H. Yau, 'Bounds of double multiplicative character sums and gaps between residues of exponential functions', *J. Number Theory* **167** (2016), 304–316.

SIMON MACOURT, Department of Pure Mathematics,
University of New South Wales, Sydney,
NSW 2052, Australia
e-mail: s.macourt@student.unsw.edu.au

https://doi.org/10.1017/S0004972717001186 Published online by Cambridge University Press