On Curves over Finite Fields with Jacobians of Small Exponent

KEVIN FORD
Department of Mathematics, 1409 West Green Street
University of Illinois at Urbana-Champaign
Urbana, IL 61801, USA
ford@math.uiuc.edu

IGOR SHPARLINSKI
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

September 9, 2018

Abstract
We show that finite fields over which there is a curve of a given genus \( g \geq 1 \) with its Jacobian having a small exponent, are very rare. This extends a recent result of W. Duke in the case \( g = 1 \). We also show when \( g = 1 \) or \( g = 2 \), our lower bounds on the exponent, valid for almost all finite fields \( \mathbb{F}_q \) and all curves over \( \mathbb{F}_q \), are best possible.

Keywords: Jacobian, group structure, distribution of divisors

2000 Mathematics Subject Classification: 11G20, 11N25, 14H40

1 Introduction
Let \( \mathcal{J}_C(\mathbb{F}_q) \) denote the Jacobian of a curve \( C \) defined over a finite field \( \mathbb{F}_q \) of \( q \) elements. We denote by \( \ell_q(C) \) the exponent of \( \mathcal{J}_C(\mathbb{F}_q) \) (that is, \( \ell_q(C) \) is the
largest order of elements of the Abelian group $\mathcal{J}_C(\mathbb{F}_q)$ and by $g$ the genus of $C$. We start with recalling two well known facts.

- The Weil bound implies that
  \[
  (q^{1/2} - 1)^{2g} \leq \#\mathcal{J}_C(\mathbb{F}_q) \leq (q^{1/2} + 1)^{2g},
  \]
  see Corollary 5.70, Theorem 5.76 and Corollary 5.80 of [1]. In particular, for fixed $g$,
  \[
  \#\mathcal{J}_C(\mathbb{F}_q) = q^g + O(q^{g-1/2}).
  \]

- The Jacobian $\mathcal{J}_C(\mathbb{F}_q)$ is an Abelian group with at most $2g$ generators, that is, for some positive integers $m_1, \ldots, m_{2g}$ we have
  \[
  \mathcal{J}_C(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_{2g}\mathbb{Z}, \quad \text{where} \quad m_1 \mid \ldots \mid m_{2g},
  \]
  (in particular $m_1 = \ldots = m_j = 1$ if the rank of $\mathcal{J}_C(\mathbb{F}_q)$ is $2g - j$) and also
  \[
  m_i|(q-1) \quad (1 \leq i \leq g),
  \]
  see Proposition 5.78 of [1].

Thus we see $\ell_q(C) = m_{2g}$ where $m_{2g}$ is defined by the representation (2), which together with (1) implies the following trivial bound

\[
\ell_q(C) \geq (\#\mathcal{J}_C(\mathbb{F}_q))^{1/2g} \geq q^{1/2} - 1.
\]

For elliptic curves $C = E$ over finite fields the exponent $\ell_q(E)$ has been studied in a number of works, see [3, 8, 9, 13, 14], with a variety of results, each of them indicating that in a “typical case” $\ell_q(E)$ tends to be substantially larger than the bound (1) guarantees. However for general curves the behavior of $\ell_q(C)$ has not been studied. Let $\pi(x)$ denote the number of primes $p \leq x$. W. Duke [3, footnote on page 691], among other results, has proved that for a sufficiently large $x$ and all but $o(\pi(x))$ of prime powers $q \leq x$, the bound

\[
\ell_q(E) \geq q^{3/4}/\log q
\]
holds for all elliptic curves $E$ defined over $\mathbb{F}_q$ (the paper [3] considers only primes, but including all prime powers in the statement is trivial of course).

We provide a generalization and some improvement of (5) for curves of arbitrary genus.
Theorem 1. Fix \( g \geq 1 \) and let \( \varepsilon(x) \) be a positive, decreasing function of \( x \) with \( \varepsilon(x) \to 0 \) as \( x \to \infty \). For all but \( o(\pi(x)) \) of the prime powers \( q \leq x \), the bound

\[
\ell_q(C) \geq q^{3/4+\varepsilon(q)}
\]

holds for all curves \( C \) of genus \( g \) defined over \( \mathbb{F}_q \).

The method of proof of (5), used in [3], is somewhat specific to elliptic curves, so here we use a slightly different approach to counting fields \( \mathbb{F}_q \) that may contain a “bad” curve.

We show that Theorem 1 is best possible for \( g = 1 \) and \( g = 2 \). In particular, the bound (5) of W. Duke [3] is quite sharp.

Theorem 2. For any fixed \( \varepsilon > 0 \) there exists \( \alpha > 0 \) such that for sufficiently large \( x \), there are at least \( \alpha \pi(x) \) primes \( q \leq x \) such that for some nonsupersingular elliptic curve \( E \) and some nonsupersingular curve \( C \) of genus \( g = 2 \) defined over \( \mathbb{F}_q \), the bounds

\[
\ell_q(E) \leq q^{3/4+\varepsilon} \quad \text{and} \quad \ell_q(C) \leq q^{3/4+\varepsilon}
\]

hold.

The proof is based on a special case of a certain lower bound on the number of shifted primes \( p - 1 \) having a divisor in a given interval. In full generality this bound is given in Theorem 7 of [5]. Such results have been applied to study the order of a given integer \( a > 1 \) modulo almost all primes \( p \), see [4, 7, 10], and now they have turned out to be useful for studying exponents of Jacobians. This argument also immediately implies the following result which applies to all curves over \( \mathbb{F}_q \) of all possible genera.

Theorem 3. Let \( \varepsilon(x) \) be a positive, decreasing function of \( x \) with \( \varepsilon(x) \to 0 \) as \( x \to \infty \). For all but \( o(\pi(x)) \) of the prime powers \( q \leq x \), the bound

\[
\ell_q(C) \geq q^{1/2+\varepsilon(q)}
\]

holds for all curves \( C \) of arbitrary genus defined over \( \mathbb{F}_q \).

Throughout the paper, the implied constants in the symbols ‘\( O \)’, ‘\( \ll \)’ and ‘\( \gg \)’ do not depend on any parameter unless indicated by a subscript, that is, \( O_g, \ll_g \) or \( \gg_g \) (we recall that the notations \( U = O(V) \), \( U \ll V \), and \( V \gg U \) are all equivalent to the assertion that the inequality \( |U| \leq cV \) holds for some constant \( c > 0 \)).
Acknowledgments. The authors would like to thank Bjorn Poonen for
a number of very helpful discussions. During the preparation of this paper,
K. F. was supported by NSF grants DMS-0301083 and DMS-0555367 and
I. S. was supported in part by ARC grant DP0556431.

2 Preliminaries

We have already mentioned that our results are based on some estimates
from [5] on shifted primes having a divisor in a given interval. Here we give
a brief guide to these estimates.

As in [5] we use $H(x, y, z)$ to denote the number of positive integers $n \leq x$
having a divisor $d$ with $y < d \leq z$. Theorem 1 of [5] gives the right order
of magnitude of $H(x, y, z)$ in the full range of parameters. However for our
purposes we need only the estimate

$$H(x, y, z) \ll xu^\delta (\log(2/u))^{-3/2}$$

(6)

where

$$\delta = 1 - \frac{1 + \log \log 2}{\log 2} = 0.086071 \ldots$$

and $u$ is defined by the equation $y^{1+u} = z$, which holds uniformly in the
range $2y \leq z \leq y^2$, $3 \leq y \leq \sqrt{x}$.

Furthermore, we need the upper bound on $H(x, y, z)$ only as tool of esti-
mating $H(x, y, z, P_\lambda)$ which is the number of primes $p \leq x$ such that $p + \lambda$
has a divisor $d$ with $y < d \leq z$. Theorem 6 of [5] gives the upper bound

$$H(x, y, z, P_\lambda) \ll \frac{H(x, y, z)}{\log x}$$

(7)

which holds for every fixed non-zero integer $\lambda$ in the range $z \geq y + (\log y)^{2/3}$
and $3 \leq y \leq \sqrt{x}$, which is much wider than is necessary for the purposes of
this paper.

We also need Theorem 7 of [5] which gives a lower bound on $H(x, y, z, P_\lambda)$
in a certain range of $x, y, z$. However, since its proof is quite short, we give
an independent derivation in Section 4.
3 Proof of Theorem \[1\]

The number of prime powers \( q = p^a \leq x \) with \( a \geq 2 \) is \( O(x^{1/2}) \). Thus, it suffices to show that for all but \( o(x/\log x) \) of the primes \( q \) with \( x/2 < q \leq x \), the bound

\[
\ell_q(\mathcal{C}) \geq q^{3/4+\varepsilon(q)}
\]

holds for all curves \( \mathcal{C} \) of genus \( g \) defined over \( \mathbb{F}_q \).

For a \((2g-1)\)-tuple \( k = (k_1, \ldots , k_{2g-1}) \) of positive integers, we consider the set \( Q_k \) of primes \( x/2 \leq q \leq x \) for which there exists a curve \( \mathcal{C} \) of genus \( g \geq 1 \) over \( \mathbb{F}_q \) such that

\[
m_1 = k_1, \quad m_i = m_{i-1}k_i, \quad \text{where } m_i \text{ is as in (2) and (3), } i = 1, \ldots , 2g - 1.
\]

In particular, if such a curve \( \mathcal{C} \) exists, then

\[
q - 1 \equiv 0 \pmod{k_1 \ldots k_g}. \tag{8}
\]

Since

\[
k_1^{2g}k_2^{2g-1} \ldots k_{2g-1}^2 \# J_{\mathcal{C}}(\mathbb{F}_q),
\]

we see by (1) that there are at most

\[
U_k = \frac{(x^{1/2} + 1)^{2g}}{k_1^{2g}k_2^{2g-1} \ldots k_{2g-1}^2} \tag{9}
\]

possibilities for the cardinality \( N = \# J_{\mathcal{C}}(\mathbb{F}_q) \).

For each of such values \( N \), we see by (1) that

\[
N^{1/g} - 2N^{1/2g} + 1 \leq q \leq N^{1/g} + 2N^{1/2g} + 1.
\]

Recalling (8) we deduce that for each possible cardinality \( N \) the prime powers \( q \) may take at most

\[
V_k = \frac{5(x^{1/2} + 1)}{k_1k_2 \ldots k_g} + 1 \tag{10}
\]

values. Therefore, combining (9) and (10), we derive

\[
\# Q_k \leq U_kV_k \leq \frac{5(x^{1/2} + 1)^{2g+1}}{k_1^{2g+1}k_2^{2g} \ldots k_g^{g+2}k_{g+1}^{g} \ldots k_{2g-1}^2} + \frac{(x^{1/2} + 1)^{2g}}{k_1^{2g}k_2^{2g-1} \ldots k_{2g-1}^2}. \tag{11}
\]

When \( g = 1 \), we interpret the right side as \( 5(x^{1/2} + 1)^3k_1^{-3} + (x^{1/2} + 1)^2k_1^{-2} \).
For any curve $C$ of genus $g \geq 1$ over $\mathbb{F}_q$ and any positive integer $s \leq 2g-1$, we have

$$\ell_q(C) = m_{2g} \geq \left( \frac{\#J_c(\mathbb{F}_q)}{m_1 \cdots m_s} \right)^{1/(2g-s)} \geq \left( \frac{(q^{1/2} - 1)^{2g}}{k_1^{1/2} k_2^{1/2} \cdots k_s^{1/2}} \right)^{1/(2g-s)}.$$  \hfill (12)

In fact, we only need (12) for $s = g$ and $s = 2g - 1$.

Suppose without loss of generality that $\varepsilon(x) \geq (\log x)^{-1/2}$ and write $\eta = \varepsilon(x/2)$. Assume $x$ is large, in particular so large that

$$\eta < \frac{1}{100g}.$$  

Let $I$ be the interval $(x^{1/4-3\eta}, x^{1/4+3\eta}]$. Let $K$ denote the set of $k$ satisfying

$$k_1 \cdots k_g \notin I,$$  \hfill (13)

$$k_1 g_1 \cdots k_g \geq x^{g/4 - 2\eta},$$  \hfill (14)

$$k_1 2g - 1 \cdots k_{2g-1} \geq x^{g/2 - 3/4 - 2\eta}.$$  \hfill (15)

Partition the primes $q \in (x/2, x]$ into three sets: $T_1$ is the set of such primes for which $q - 1$ has a divisor in $I$, $T_2$ is the set of such primes lying in a set $Q_k$ with $k \in K$, and $T_3$ is the set of remaining primes. By Theorems 1 and 6 of [5], that is, by a combination of (6) and (7), we have

$$\#T_1 \ll \frac{x \log x}{\eta} (\log 1/\eta)^{-3/2}.$$  \hfill (16)

Now consider $q \in T_2$. By (14),

$$k_1 \cdots k_g \geq (k_1 g_1 \cdots k_g)^{1/2} \geq x^{1/4 - 2\eta},$$

hence $k_1 \cdots k_g > x^{1/4 + 3\eta}$ by (13). Combined with (11), (15), and the inequality $k_i \leq (x^{1/2} + 1)^{2g}$ for each $i$, we obtain

$$\#T_2 \leq \sum_{k \in K} \#Q_k$$

$$\leq \left( \frac{5(x^{1/2} + 1)^{2g+1}}{x^{g-1/2+\eta}} + \frac{(x^{1/2} + 1)^{2g}}{x^{g-3/4 - 2\eta}} \right) \sum_{k \in K} \frac{1}{k_1 \cdots k_{2g-1}}$$

$$\leq \left( \frac{5(x^{1/2} + 1)^{2g+1}}{x^{g-1/2+\eta}} + \frac{(x^{1/2} + 1)^{2g}}{x^{g-3/4 - 2\eta}} \right) \frac{2g \log(x^{1/2} + 1) + 1)^{2g}}{x^{1-\eta/2}}$$

$$\ll g (\log x)^{2g-1} (x^{1-\eta} + x^{3/4+2\eta})$$

$$\ll g x^{1-\eta/2}.$$
Together with (16), we see that all but $o(x/\log x)$ primes $q \in (x/2, x]$ lie in $\mathcal{T}_3$. For $q \in \mathcal{T}_3$, the condition (13) holds, thus either (14) is false or (15) is false. In either case, the bound (12) implies that $\ell_q(\mathcal{C}) \gg_q x^{3/4+2\eta}$, and hence for large $x$

$$\ell_q(\mathcal{C}) \geq q^{3/4+\varepsilon(q)}$$

for any curve $\mathcal{C}$ of genus $g$ defined over $\mathbb{F}_q$. \hfill \square

4 Proof of Theorem 2

We start with the case $g = 1$.

Without loss of generality we can assume that $\varepsilon < 1/20$. Put

$$y = x^{1/4-\varepsilon} \quad \text{and} \quad z = x^{1/4-\varepsilon/2}.$$ 

Since $y > x^{1/5}$, an integer $k \leq x$ can have at most 4 prime factors $p$ with $y < p \leq z$. Hence, the set $\mathcal{P}$ of primes $x/\log x \leq q \leq x$ such that $q - 1$ has a prime divisor $p$ with $y < p \leq z$, is of cardinality least

$$\# \mathcal{P} \geq \frac{1}{4} \sum_{y < p \leq z \atop p \text{ prime}} \pi(x; p, 1) + O\left(\frac{x}{(\log x)^2}\right),$$

where, as usual, $\pi(x; k, a)$ is the number of primes $q \leq x$ with $q \equiv a \pmod{k}$.

By the Bombieri-Vinogradov theorem (see, for example, Section 28 of [2]),

$$\sum_{y < p \leq z \atop p \text{ prime}} \left| \pi(x; p, 1) - \frac{1}{p-1} \pi(x) \right| \ll \frac{x}{(\log x)^2}.$$ 

Therefore

$$\# \mathcal{P} \geq \frac{1}{4} \pi(x) \sum_{y < p \leq z \atop p \text{ prime}} \frac{1}{p-1} + O\left(\frac{x}{(\log x)^2}\right) = \frac{1}{4} \pi(x) \sum_{y < p \leq z \atop p \text{ prime}} \frac{1}{p} + O\left(\frac{x}{(\log x)^2}\right).$$

By the Mertens theorem (see Theorem 4.1 of Chapter 1 in [11]),

$$\sum_{y < p \leq z \atop p \text{ prime}} \frac{1}{p} = \log \log z - \log \log y + o(1) = \log \frac{1 - 2\varepsilon}{1 - 4\varepsilon} + o(1),$$
thus for large $x$ we have $\#\mathcal{P} \geq \alpha \pi(x)$ for a positive $\alpha$ depending on $\varepsilon$. This result is a special case of Theorem 7 of [5], but we include the proof because it is short.

For a sufficiently large $x$ and for any $q \in \mathcal{P}$, there are at least $2q^{1/2}z^{-2} - 1 \geq q^\varepsilon$ integers $k \in [q + 1 - 2q^{1/2}, q]$ with $p^2|k$ for some prime $p|q - 1$ with $y < p \leq z$. For any such $k$, by [12, 16, 17] one can always find an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ with $\mathcal{E}(\mathbb{F}_q) = k$ of $\mathbb{F}_q$-rational points and the exponent $\ell_q(\mathcal{E}) = k/p \leq q/y \leq q^{3/4+\varepsilon}$. This concludes the proof in the case $g = 1$. For $g = 2$, Proposition 5.4 in Section 5 of Chapter X of [15] implies that the cardinalities of elliptic curves $\mathcal{E}$ over $\mathbb{F}_q$ with $j$-invariant $j(\mathcal{E}) = 0, 1728$ take $O(1)$ values. Therefore we can choose $k$ and an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ of exponent $\ell_q(\mathcal{E}) \leq q^{3/4+\varepsilon}$ as in the above with the additional condition $j(\mathcal{E}) \neq 0, 1728$. By Corollary 6 of [6] we see that there is a curve $\mathcal{C}$ of genus $g = 2$ such that the Jacobian $J_\mathcal{C}(\mathbb{F}_q)$ is isogenous to $\mathcal{E}(\mathbb{F}_q) \times \mathcal{E}(\mathbb{F}_q)$. Moreover, there exists an isogeny from $\mathcal{E}(\mathbb{F}_q) \times \mathcal{E}(\mathbb{F}_q)$ to $J_\mathcal{C}(\mathbb{F}_q)$, whose kernel (over an algebraic closure of $\mathbb{F}_q$) is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So $\ell_q(\mathcal{C}) \geq \ell_q(\mathcal{E})/2$, which concludes the proof for $g = 2$. \hfill \Box

5 Proof of Theorem 3

The desired bound follows immediately from Theorems 1 and 6 of [5], that is, from (6) and (7), and the congruence $q - 1 \equiv 0 \pmod{m_g}$, where $m_i$, $i = 1, \ldots, 2g$, are as in (2). Again without loss of generality assume that $\varepsilon(x) \geq (\log x)^{-1/2}$. For $\eta = 2\varepsilon(x/2)$, similarly to (16), we see that the set $\mathcal{R}$ of primes $q \leq x$ such that $q - 1$ has a divisor $m \in [x^{1/2-2\eta}, x^{1/2+2\eta}]$, is of cardinality $\#\mathcal{R} = o(x/\log x)$. Consider a prime $q \in (2x^{1-\eta}, x]$ which does not lie in $\mathcal{R}$, and any curve $\mathcal{C}$ of genus $g$ over $\mathbb{F}_q$. If $m_g > x^{1/2+\eta}$ then

$$\ell_q(\mathcal{C}) = m_{2g} \geq m_g > q^{1/2+\varepsilon(q)}.$$ 

Otherwise, by (3), $m_g \leq x^{1/2-2\eta}$ and by (11) we obtain

$$\ell_q(\mathcal{C}) \geq \left( \frac{\#J_\mathcal{C}(\mathbb{F}_q)}{m_1 \cdots m_g} \right)^{1/g} \geq \left( \frac{(q^{1/2} - 1)^{2g}}{m_1 \cdots m_g} \right)^{1/g} \geq \left( \frac{x^{g-2\eta}}{x^{g/2-2\eta}} \right)^{1/g} \geq x^{1/2+\eta} > q^{1/2+\varepsilon(q)}$$

for large $x$. \hfill \Box
6 Remarks

It is interesting to note that using (12) for other values of \( s \) (besides \( s = g \) and \( s = 2g - 1 \) as in the proof of Theorem 1) and thus corresponding sets \( K \), does not lead to any improvements.

**Open Question.** Is the exponent in Theorem 1 sharp for arbitrary \( g \geq 3 \), as it is for \( g = 1, 2 \)?

Unfortunately the lack of knowledge about the distribution of possible cardinalities of Jacobians of curves of genus \( g \geq 2 \) prevents are from deriving an analogue of Theorem 2 for \( g \geq 2 \).

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Elliptic and hyperelliptic curve cryptography: Theory and practice*, CRC Press, 2005.

[2] H. Davenport, *Multiplicative number theory*, 2nd ed., Springer-Verlag, New York 1980.

[3] W. Duke, ‘Almost all reductions modulo \( p \) of an elliptic curve have a large exponent’, *C. R. Math. Acad. Sci. Paris*, 337 (2003), 689–692.

[4] P. Erdős and R. Murty, ‘On the order of \( a \pmod{p} \)’, *Proc. 5th Canadian Number Theory Association Conf.* (R. Gupta and K. S. Williams, eds), Amer. Math. Soc., Providence, RI, 1999, 87–97.

[5] K. Ford, ‘The distribution of integers with a divisor in a given interval’, *Ann. Math.* 168 (2008), 367–433.

[6] E. W. Howe, F. Leprévost and B. Poonen, ‘Large torsion subgroups of split Jacobians of curves of genus two or three’, *Forum Math.*, 12 (2000), 315–364.

[7] K.-H. Indlekofer and N. M. Timofeev, ‘Divisors of shifted primes’, *Publ. Math. Debrecen*, 60 (2002), 307–345.

[8] F. Luca, J. McKee and I. E. Shparlinski, ‘Small exponent point groups on elliptic curves’, *J. Théorie des Nombres Bordeaux*, 18 (2006), 471–476.
[9] F. Luca and I. E. Shparlinski, ‘On the exponent of the group of points on elliptic curves in extension fields’, *Intern. Math. Research Notices*, **2005** (2005), 1391–1409.

[10] F. Pappalardi, ‘On the order of finitely generated subgroups of $\mathbb{Q}^*$ (mod $p$) and divisors of $p - 1$’, *J. Number Theory*, **57** (1996), 207–222.

[11] K. Prachar, *Primzahlverteilung*, Springer, Berlin, 1957.

[12] H.-G. Rück, ‘A note on elliptic curves over finite fields’, *Math. Comp.*, **49** (1987), 301–304.

[13] R. Schoof, ‘The exponents of the group of points on the reduction of an elliptic curve’, *Arithmetic Algebraic Geometry* (G. van der Geer, F. Oort and J. Steenbrink, eds), Progr. Math., vol. 89, Birkhäuser, Boston, MA, 1991, 325–335.

[14] I. E. Shparlinski, ‘Orders of points on elliptic curves’, *Affine Algebraic Geometry* (J. Gutierrez, V. Shpilrain and J.-T. Yu, eds), Amer. Math. Soc., 2005, 245–252.

[15] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

[16] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer Acad. Pres, Dordrecht, 1991.

[17] J. F. Voloch, ‘A note on elliptic curves over finite fields’, *Bull. Soc. Math. France*, **116** (1988), 455–458.