On Balanced Subgroups of the Multiplicative Group

Carl Pomerance and Douglas Ulmer

In memory of Alf van der Poorten

Abstract A subgroup H of $(\mathbb{Z}/d\mathbb{Z})^\times$ is called *balanced* if every coset of H is evenly distributed between the lower and upper halves of $(\mathbb{Z}/d\mathbb{Z})^\times$, i.e., has equal numbers of elements with representatives in $(0,d/2)$ and $(d/2,d)$. This notion has applications to ranks of elliptic curves. We give a simple criterion in terms of characters for a subgroup H to be balanced, and for a fixed integer p, we study the distribution of integers d such that the cyclic subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p is balanced.

Mathematics Subject Classification (2010): Primary 11N37; Secondary 11G05

1 Introduction

Let $d > 2$ be an integer and consider $(\mathbb{Z}/d\mathbb{Z})^\times$, the group of units modulo d. Let A_d be the first half of $(\mathbb{Z}/d\mathbb{Z})^\times$, that is, A_d consists of residues with a representative in $(0,d/2)$. Let $B_d = (\mathbb{Z}/d\mathbb{Z})^\times \setminus A_d$ be the second half of $(\mathbb{Z}/d\mathbb{Z})^\times$. We say a subgroup H of $(\mathbb{Z}/d\mathbb{Z})^\times$ is *balanced* if for each $g \in (\mathbb{Z}/d\mathbb{Z})^\times$ we have $|gH \cap A_d| = |gH \cap B_d|$, that is, each coset of H has equally many members in the first half of $(\mathbb{Z}/d\mathbb{Z})^\times$ as in the second half.

C. Pomerance (✉)
Department of Mathematics, Dartmouth College, Hanover, NH 03755, USA
e-mail: carl.pomerance@dartmouth.edu

D. Ulmer
School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, USA
e-mail: douglas.ulmer@math.gatech.edu

J.M. Borwein et al. (eds.), *Number Theory and Related Fields: In Memory of Alf van der Poorten*, Springer Proceedings in Mathematics & Statistics 43,
DOI 10.1007/978-1-4614-6642-0_14,

Let φ denote Euler's function, so that $\varphi(d)$ is the cardinality of $(\mathbb{Z}/d\mathbb{Z})^\times$. If n and m are coprime integers with $m > 0$, let $l_n(m)$ denote the order of the cyclic subgroup $\langle n \bmod m\rangle$ generated by n in $(\mathbb{Z}/m\mathbb{Z})^\times$ (i.e., $l_n(m)$ is the multiplicative order of n modulo m).

Our interest in balanced subgroups stems from the following result:

Theorem 1.1 ([2]). *Let p be an odd prime number, let $\mathbb{F}_q$ be the finite field of cardinality $q = p^f$, and let $\mathbb{F}_q(u)$ be the rational function field over $\mathbb{F}_q$. Let d be a positive integer not divisible by p, and let E_d be the elliptic curve over $\mathbb{F}_q(u)$ defined by*

$$y^2 = x(x+1)(x+u^d).$$

Then we have

$$\operatorname{Rank} E_d(\mathbb{F}_q(u)) = \sum_{\substack{e|d,\ e>2 \\ \langle p \bmod e\rangle \text{ balanced}}} \frac{\varphi(e)}{l_q(e)}.$$

A few simple observations are in order. It is easy to see that $\langle -1\rangle$ is a balanced subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$. It is also easy to see that if $4 \mid d$, then $\langle \frac{1}{2}d+1\rangle$ is a balanced subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$. In addition, if H is a balanced subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ and K is a subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ containing H, then K is balanced as well. Indeed, K is a union of $[K:H]$ cosets of H, so for each $g \in (\mathbb{Z}/d\mathbb{Z})^\times$, gK is a union of $[K:H]$ cosets of H, each equally distributed between the first half of $(\mathbb{Z}/d\mathbb{Z})^\times$ and the second half. Thus, gK is also equally distributed between the first half and the second half.

It follows that if some power of p is congruent to -1 modulo d and if $q \equiv 1 \pmod{d}$, then the theorem implies that $\operatorname{Rank} E_d(\mathbb{F}_q(u)) = d-2$ if d is even and $d-1$ if d is odd. The rank of E_d when some power of p is -1 modulo d was first discussed in [12], and with hindsight it could have been expected to be large from considerations of "supersingularity." The results of [2] show, perhaps surprisingly, that there are many other classes of d for which high ranks occur. Our aim here is to make this observation more quantitative.

More precisely, the aim of this paper is to investigate various questions about balanced pairs (p,d), i.e., pairs such that $\langle p \bmod d\rangle$ is a balanced subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$. In particular, we give a simple criterion in terms of characters for a subgroup to be balanced (Theorem 2.1), and we use it to determine all balanced subgroups of order 2 (Theorem 3.2). We also investigate the distribution for a fixed p of the set of d's such that (p,d) is balanced (Theorems 4.1–4.3). We find that when p is odd, the divisors d of numbers of the form p^n+1 are not the largest contributor to this set. Finally, we investigate the average rank and typical rank of the curves E_d in Theorem 1.1 for fixed q and varying d.

2 Balanced Subgroups and Characters

The goal of this section is to characterize balanced subgroups of $(\mathbb{Z}/d\mathbb{Z})^\times$ in terms of Dirichlet characters. If χ is a character modulo d, we define

$$c_\chi = \sum_{0<a<d/2} \chi(a).$$

As usual, we say that χ is odd if $\chi(-1) = -1$ and χ is even if $\chi(-1) = 1$.

Theorem 2.1. *A subgroup $H \subset (\mathbb{Z}/d\mathbb{Z})^\times$ is balanced if and only if $c_\chi = 0$ for every odd character χ of $(\mathbb{Z}/d\mathbb{Z})^\times$ whose restriction to H is trivial.*

As an example, note that if $H = \langle -1 \rangle$, then there are no odd characters trivial on H and so the theorem implies that H is balanced.

Proof. Throughout the proof, we write G for $(\mathbb{Z}/d\mathbb{Z})^\times$. We also write A for A_d as above and similarly for B, so that G is the disjoint union $A \cup B$.

We write $\mathbf{1}_A$ for the characteristic function of $A \subset G$ and similarly for $\mathbf{1}_B$. Let $f: G \to \mathbb{C}$ be the sum over H of translates of $\mathbf{1}_A - \mathbf{1}_B$:

$$\begin{aligned} f(g) &= \sum_{h \in H} (\mathbf{1}_A(gh) - \mathbf{1}_B(gh)) \\ &= \#(gH \cap A) - \#(gH \cap B). \end{aligned}$$

By definition, H is balanced if and only if f is identically zero.

We write $\hat{G}$ for the set of complex characters of G, and we expand f in terms of these characters:

$$f = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi$$

where

$$\hat{f}(\chi) = \frac{1}{\varphi(d)} \sum_{g \in G} f(g)\chi^{-1}(g).$$

Thus, H is balanced if and only if $\hat{f}(\chi) = 0$ for all $\chi \in \hat{G}$.

It is easy to see that $\hat{f}(\chi_{triv}) = 0$. Since $\mathbf{1}_A - \mathbf{1}_B = 2\mathbf{1}_A - \mathbf{1}_G$, for χ nontrivial, we find that

$$\hat{f}(\chi^{-1}) = \frac{2}{\varphi(d)} \left(\sum_{h \in H} \chi(h) \right) \left(\sum_{a \in A} \chi(a) \right).$$

Note that $\sum_{h \in H} \chi(h)$ is zero if and only if the restriction of χ to H is nontrivial.

Note also that

$$c_\chi = \sum_{0<a<d/2} \chi(a) = \sum_{a \in A} \chi(a)$$

since χ is a Dirichlet character. If χ is even and nontrivial, then

$$c_\chi = \frac{1}{2} \sum_{g \in G} \chi(g) = 0.$$

Thus, $\hat{f}(\chi) = 0$ for all $\chi \in \hat{G}$ if and only if $c_\chi = 0$ for all odd characters χ which are trivial on H. This completes the proof of the theorem. □

We now give a non-vanishing criterion for c_χ.

Lemma 2.2. *If χ is a primitive, odd character of $(\mathbb{Z}/d\mathbb{Z})^\times$, then $c_\chi \neq 0$.*

Proof. Under the hypotheses on χ, the classical evaluation of $L(1,\chi)$ leads to the formula

$$L(1,\chi^{-1}) = \frac{\pi i \tau(\chi^{-1})}{d(\chi^{-1}(2)-2)} c_\chi$$

where $\tau(\chi^{-1})$ is a Gauss sum. (See, e.g., [7, pp. 200–201] or [8, Theorem 9.21], though there is a small typo in the second reference.) By the theorem of Dirichlet, $L(1,\chi^{-1}) \neq 0$ and so $c_\chi \neq 0$. □

In light of the lemma, we should consider imprimitive characters.

Lemma 2.3. *Suppose that ℓ is a prime number dividing d and set $d' = d/\ell$. Suppose also that χ is a nontrivial character modulo d induced by a character χ' modulo d'. If $\ell = 2$, then $c_\chi = -\chi'(2)c_{\chi'}$. If ℓ is odd, then $c_\chi = (1-\chi'(\ell))c_{\chi'}$. Here, we employ the usual convention that $\chi'(\ell) = 0$ if $\ell \mid d'$.*

Proof. First suppose $\ell = 2$. We have

$$c_\chi = \sum_{\substack{a<d/2 \\ \gcd(a,d)=1}} \chi(a) = \sum_{\substack{a<d' \\ \gcd(a,2d')=1}} \chi'(a).$$

If $2 \mid d'$, this is a complete character sum and so vanishes. If $2 \nmid d'$, then

$$\begin{aligned}
\sum_{\substack{a<d' \\ \gcd(a,2d')=1}} \chi'(a) &= \sum_{\substack{a<d' \\ \gcd(a,d')=1}} \chi'(a) - \sum_{\substack{a<d'/2 \\ \gcd(a,d')=1}} \chi'(2a) \\
&= - \sum_{\substack{a<d'/2 \\ \gcd(a,d')=1}} \chi'(2a) \\
&= -\chi'(2)c_{\chi'}
\end{aligned}$$

as desired.

Now assume that ℓ is odd. We have

$$c_\chi = \sum_{\substack{a<d/2 \\ \gcd(a,d)=1}} \chi(a) = \sum_{\substack{a<\ell d'/2 \\ \gcd(a,\ell d')=1}} \chi'(a).$$

If $\ell \mid d'$, then

$$\sum_{\substack{a<\ell d'/2 \\ \gcd(a,\ell d')=1}} \chi'(a) = \sum_{\substack{a<d'/2 \\ \gcd(a,d')=1}} \chi'(a) = c_{\chi'}.$$

If $\ell \nmid d'$, then

$$\begin{aligned}\sum_{\substack{a<\ell d'/2 \\ \gcd(a,\ell d')=1}} \chi'(a) &= \sum_{\substack{a<\ell d'/2 \\ \gcd(a,d')=1}} \chi'(a) - \sum_{\substack{a<d'/2 \\ \gcd(a,d')=1}} \chi'(\ell a) \\ &= \sum_{\substack{a<d'/2 \\ \gcd(a,d')=1}} \chi'(a) - \chi'(\ell) \sum_{\substack{a<d'/2 \\ \gcd(a,d')=1}} \chi'(a) \\ &= (1-\chi'(\ell))c_{\chi'}\end{aligned}$$

as desired. □

Applying the lemma repeatedly, we arrive at the following non-vanishing criterion:

Proposition 2.4. *Suppose that χ is an odd character modulo d induced by a primitive character χ' modulo d'. Then $c_\chi \neq 0$ if and only if the following two conditions both hold: (i) $4 \nmid d$ or d/d' is odd, and (ii) for every odd prime ℓ which divides d and does not divide d', we have $\chi'(\ell) \neq 1$.*

As an example, suppose that $4 \mid d$ and $H = \langle \frac{1}{2}d+1 \rangle$. Note that

$$(\mathbb{Z}/d\mathbb{Z})^\times / \langle \tfrac{1}{2}d+1 \rangle \cong (\mathbb{Z}/\tfrac{1}{2}d\mathbb{Z})^\times.$$

Thus, if χ is an odd character modulo d and $\chi(\frac{1}{2}d+1) = 1$, then the conductor d' of χ divides $d/2$. This shows that d/d' is even and so condition (i) of the proposition fails and $c_\chi = 0$. Therefore, H is balanced.

3 Balanced Subgroups of Small Order

In this section, we discuss balanced subgroups of small order. We have already seen that a subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ which contains -1 or $\frac{1}{2}d+1$ is balanced. We will show that in a certain sense small balanced subgroups are controlled by these balanced subgroups of order 2.

Theorem 3.1. *For every positive integer n there is an integer $d(n)$ such that if $d > d(n)$ and H is a balanced subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ of order n, then either $-1 \in H$ or $4 \mid d$ and $\frac{1}{2}d + 1 \in H$.*

We can make this much more explicit for subgroups of order 2.

Theorem 3.2. *A subgroup $H = \langle h \rangle$ of $(\mathbb{Z}/d\mathbb{Z})^\times$ of order 2 is balanced if and only if d and h satisfy one of the following conditions:*

1. $h \equiv -1 \pmod{d}$,
2. $d \equiv 0 \pmod{4}$ *and* $h \equiv \frac{1}{2}d + 1 \pmod{d}$,
3. $d = 24$ *and* $h \equiv 17 \pmod{d}$ *or* $h \equiv 19 \pmod{d}$,
4. $d = 60$ *and* $h \equiv 41 \pmod{d}$ *or* $h \equiv 49 \pmod{d}$.

Proof of Theorem 3.1. Throughout this proof and the next, we write G for $(\mathbb{Z}/d\mathbb{Z})^\times$. Using Proposition 2.4, we will show that if d is sufficiently large with respect to n, then for any subgroup $H \subset G$ of order n which does not contain -1 or $\frac{1}{2}d + 1$, there is a character χ which is odd, trivial on H, and with $c_\chi \neq 0$. By Theorem 2.1, this implies that H is not balanced.

Note that a balanced subgroup obviously has even order, so there is no loss in assuming that n is even. We make this assumption for the rest of the proof.

Let H^+ be the subgroup of G generated by H, -1 and, if $4 \mid d$, by $\frac{1}{2}d + 1$. Fix a character χ_0 of G which is trivial on H, odd, and -1 on $\frac{1}{2}d + 1$ if $4 \mid d$. The set of all characters satisfying these restrictions is a homogeneous space for $\widehat{G/H^+} \subset \hat{G}$. We will argue that multiplying χ_0 by a suitable $\psi \in \widehat{G/H^+}$ yields a $\chi = \chi_0\psi$ for which Proposition 2.4 implies that $c_\chi \neq 0$.

Note first that any character χ which is odd and, if $4 \mid d$, has $\chi(\frac{1}{2}d + 1) = -1$ automatically satisfies condition (i) in Proposition 2.4. Indeed, if $4 \mid d$, then the condition $\chi(\frac{1}{2}d + 1) = -1$ implies that χ is 2-primitive, i.e., the conductor d' of χ has d/d' odd. The rest of the argument relates to condition (ii) in Proposition 2.4.

Write $d = \prod_\ell \ell^{e_\ell}$ and write G_ℓ for $(\mathbb{Z}/\ell^{e_\ell}\mathbb{Z})^\times$ so that $G \cong \prod_\ell G_\ell$. Let $\chi = \prod_\ell \chi_\ell$. Note that ℓ divides the conductor of χ if and only if χ_ℓ is non-trivial.

We will sloppily write G_ℓ/H^+ for G_ℓ modulo the image of H^+ in G_ℓ. For odd ℓ, G_ℓ is cyclic and therefore so is G_ℓ/H^+; for $\ell = 2$, since $-1 \in H^+$, G_2/H^+ is also cyclic.

Note also that H^+ is the product of H and a group of exponent 2, namely, the subgroup of G generated by -1 or by -1 and $\frac{1}{2}d + 1$. Also, we have assumed that $n = |H|$ is even. If ℓ is odd, then G_ℓ is cyclic of even order, so it has a unique element of order 2. It follows that the order of the image of H^+ in G_ℓ divides n.

We define three sets of odd primes:

$$S_1 = \left\{\text{odd } \ell : \ell \mid d,\ G_\ell/H^+ = \{1\}\right\},$$

$$S_2 = \{\text{odd } \ell : \ell \mid d,\ \varphi(\ell^{e_\ell}) \mid n\},$$

and

$$S_3 = \{\text{odd } \ell : \varphi(\ell) \mid n\}.$$

Note that $S_1 \subset S_2 \subset S_3$ and S_3 depends only on n, not on d.

If ℓ is odd, $\ell \mid d$, and $\ell \notin S_1$, then G_ℓ/H^+ is nontrivial. Thus, choosing a suitable ψ, we may arrange that the conductor of $\chi_1 = \chi_0\psi$ is divisible by every prime dividing d which is not in S_1.

For the odd primes ℓ which divide d and do not divide the conductor of χ_1 (a subset of S_1, thus also a subset of S_3), we must arrange that $\chi'(\ell) \neq 1$ (where χ' is the primitive character inducing χ).

Recall that G_ℓ/H^+ is cyclic. We now remark that if C is a cyclic group and $a \in C$, then, for each $z \in \mathbb{C}$, the set of characters $\psi : C \to \mathbb{C}$ such that $\chi(a) \neq z$ has cardinality at least $|C|(1 - 1/|\langle a\rangle|)$ (where $|\langle a\rangle|$ is the order of a). If we have several elements $a_1, \ldots, a_n$ and several values $z_1, \ldots, z_n$ to avoid, then the number of characters ψ such that $\psi(a_i) \neq z_i$ is at least

$$|C|\left(1 - \frac{1}{|\langle a_1\rangle|} - \cdots - \frac{1}{|\langle a_n\rangle|}\right).$$

Thus we can find such a character provided that each a_i has order $> n$.

Now we use that d is large to conclude that a large prime power ℓ^e divides d. (Note that ℓ might be 2 here.) Then G_ℓ/H^+ is a cyclic group in which the order of each prime in S_1 is large. (The primes in S_1 are also in S_3, so belong to a set fixed independently of d.) We want a character ψ of G_ℓ/H^+ which satisfies $\psi(r) \neq \chi_1^{-1}(r)$ for all $r \in S_1$. We also want $\psi\chi_1$ to have nontrivial ℓ component which, phrased in the language above, means that we want $\psi(a) \neq 1$ for some fixed generator of G_ℓ/H^+. Since the size of S_1 is bounded depending only on n, the discussion of the previous paragraph shows that these conditions can be met if ℓ^e is large enough.

Setting $\chi = \psi\chi_1$ with ψ as in the previous paragraph yields a character χ such that $c_\chi \neq 0$, and this completes the proof. □

Proof of Theorem 3.2. We retain the concepts and notation of the proof of Theorem 3.1. We also say that a subgroup of order 2 is "exceptional" if it does not contain -1 or $\frac{1}{2}d + 1$.

Since $n = 2$, the set $S_3 = \{3\}$ and the set S_2 is either empty (if $3 \nmid d$ or $9 \mid d$) or $S_2 = \{3\}$ (if 3 exactly divides d). If S_2 is empty and H is an exceptional subgroup of order 2, then the first part of the proof of Theorem 3.1 provides a primitive odd character trivial on H, and so H is not balanced.

Suppose we are in the case where 3 exactly divides d. Following the first part of the proof of Theorem 3.1, we have a character χ_1 of G with conductor divisible by $d' = d/3$ which is odd, trivial on H, and, if $4 \mid d$, satisfies $\chi_1(\frac{1}{2}d + 1) = -1$. If the conductor of χ_1 is d or if the primitive character χ' inducing χ_1 has $\chi'(3) \neq 1$, then setting $\chi = \chi_1$ we have $c_\chi \neq 0$ and we see that H is not balanced.

If not, we will modify χ_1. Note that if $\ell = 2$ and $16 \mid d$, or $\ell = 5$ and $25 \mid d$, or ℓ is a prime ≥ 7 and $\ell \mid d$, then the order of 3 in G_ℓ/H^+ is at least 3. Thus, in these cases, there is a character ψ of G_ℓ/H^+ so that the ℓ part of $\chi = \chi_1\psi$ is nontrivial and so that the primitive character χ' inducing χ satisfies $\chi'(3) \neq 1$. Then $c_\chi \neq 0$ and H is not balanced.

This leaves a small number of values of d to check for exceptional balanced subgroups of order 2. Namely, we just need to check divisors of $8 \cdot 3 \cdot 5 = 120$ which are divisible by 3. A quick computation which we leave to the reader finishes the proof. □

4 Distribution of Numbers d with $\langle p \bmod d\rangle$ Balanced

For the rest of the paper, we write $\mathbb{U}_d$ for $(\mathbb{Z}/d\mathbb{Z})^\times$. Fix an integer p with $|p| > 1$. In our application to elliptic curves, p is an odd prime number, but it seems interesting to state our results on balanced subgroups in a more general context. Let $\mathscr{B}_p$ denote the set of integers $d > 2$ coprime to p for which $\langle p \bmod d\rangle$ is a balanced subgroup of $\mathbb{U}_d$. Further, define subsets of $\mathscr{B}_p$ as follows:

$$\mathscr{B}_{p,0} = \{d > 2 : (d,p) = 1,\ 4 \mid d,\ \tfrac{1}{2}d + 1 \in \langle p \bmod d\rangle\},$$
$$\mathscr{B}_{p,1} = \{d > 2 : (d,p) = 1,\ -1 \in \langle p \bmod d\rangle\}$$
$$\mathscr{B}_{p,*} = \mathscr{B}_p \setminus (\mathscr{B}_{p,0} \cup \mathscr{B}_{p,1}).$$

Note that if p is even then $\mathscr{B}_{p,0}$ is empty. For any set $\mathscr{A}$ of positive integers and x a real number at least 1, we let $\mathscr{A}(x) = |\mathscr{A} \cap [1,x]|$.

We state the principal results of this section, which show that when p is odd, most members of $\mathscr{B}_p$ lie in $\mathscr{B}_{p,0}$.

Theorem 4.1. *For each odd integer p with $|p| > 1$, there are positive numbers b_p, b'_p with*

$$b_p \frac{x}{\log\log x} \leq \mathscr{B}_{p,0}(x) \leq b'_p \frac{x}{\log\log x}$$

for all sufficiently large numbers x depending on the choice of p.

We remark that $\mathscr{B}_{p,1}$ has been studied by Moree. In particular we have the following result:

Theorem 4.2 ([9, Thm. 5]). *For each integer p with $|p| > 1$, there are positive numbers c_p, δ_p such that*

$$\mathscr{B}_{p,1}(x) \sim c_p \frac{x}{(\log x)^{\delta_p}} \quad \text{as } x \to \infty.$$

In particular, for p prime we have $\delta_p = \frac{2}{3}$.

Theorem 4.3. *For each integer p with $|p| > 1$, there is a number $\varepsilon_p > 0$ such that for all $x \geq 3$,*

$$\mathscr{B}_{p,*}(x) = O_p\left(\frac{x}{(\log x)^{\varepsilon_p}}\right).$$

Corollary 4.4. *If p is an odd integer with $|p| > 1$, then $\mathscr{B}_p(x) \sim \mathscr{B}_{p,0}(x)$ as $x \to \infty$.*

It is easy to see that $\mathscr{B}_{p,1} \cap \mathscr{B}_{p,0}$ has at most one element. Indeed, the cyclic group $\langle p \bmod d\rangle$ has at most one element of order exactly 2, so if $d \in \mathscr{B}_{p,1} \cap \mathscr{B}_{p,0}$, then for some f, we have $p^f \equiv -1 \equiv \frac{1}{2}d + 1 \mod d$, and this can happen only when $d = 4$. This shows that for $x \geq 4$,

$$\mathscr{B}_p(x) \geq \mathscr{B}_{p,0}(x) + \mathscr{B}_{p,1}(x) - 1.$$

We believe that $\mathscr{B}_{p,0}$ and $\mathscr{B}_{p,1}$ comprise most of $\mathscr{B}_p$, and in fact we pose the following conjecture:

Conjecture 4.5. *For each integer p with $|p| > 1$ we have*

$$\mathscr{B}_p(x) = \mathscr{B}_{p,0}(x) + (1 + o(1))\mathscr{B}_{p,1}(x) \quad \text{as } x \to \infty,$$

that is, $\mathscr{B}_{p,*}(x) = o(\mathscr{B}_{p,1}(x))$ as $x \to \infty$.

We now begin a discussion leading to the proofs of Theorems 4.1 and 4.3. The following useful result comes from [4, Theorem 2.2]:

Proposition 4.6. *There is an absolute positive constant c such that for all numbers $x \geq 3$ and any set $\mathscr{R}$ of primes in $[1,x]$, the number of integers in $[1,x]$ not divisible by any member of $\mathscr{R}$ is at most*

$$cx \prod_{r \in \mathscr{R}} \left(1 - \frac{1}{r}\right) \leq cx \exp\left(-\sum_{r \in \mathscr{R}} \frac{1}{r}\right).$$

Note that the inequality in the display follows immediately from the inequality $1 - \theta < \mathrm{e}^{-\theta}$ for every $\theta \in (0,1)$.

For a positive integer m coprime to p, recall that $l_p(m)$ denotes the order of $\langle p \bmod m\rangle$. If r is a prime, we let $v_r(m)$ denote that integer v with $r^v \mid m$ and $r^{v+1} \nmid m$.

We would like to give a criterion for membership in $\mathscr{B}_{p,0}$, but before this, we establish an elementary lemma.

Lemma 4.7. *Let p be an odd integer with $|p| > 1$ and let k, i be positive integers. Then*

$$v_2\left(\frac{p^{2^i k} - 1}{p^{2k} - 1}\right) = i - 1.$$

Proof. The result is clear if $i = 1$. If $i > 1$, we see that

$$\frac{p^{2^i k}-1}{p^{2k}-1} = (p^{2k}+1)(p^{4k}+1)\dots(p^{2^{i-1}k}+1),$$

which is a product of $i-1$ factors that are each 2 (mod 4). □

The following result gives a criterion for membership in $\mathscr{B}_{p,0}$:

Proposition 4.8. *Let p be odd with $|p| > 1$ and let $m \geq 1$ be an odd integer coprime to p. If $l_p(m)$ is odd, then $2^j m \in \mathscr{B}_{p,0}$ if and only if $j = 1 + v_2(p-1)$ or $j > v_2(p^2-1)$. If $l_p(m)$ is even, then $2^j m \in \mathscr{B}_{p,0}$ if and only if $j > v_2(p^{l_p(m)}-1)$.*

Proof. We first prove the "only if" part. Assume that $d = 2^j m \in \mathscr{B}_{p,0}$ and let f be an integer with $p^f \equiv \frac{1}{2}d + 1 \pmod{d}$. Then $l_p(m) \mid f$ so that $j - 1 = v_2(p^f - 1) \geq v_2(p^{l_p(m)} - 1)$. This establishes the "only if" part if $l_p(m)$ is even, and it also shows that $j \geq 1 + v_2(p-1)$ always, so in particular if $l_p(m)$ is odd. Suppose $l_p(m)$ is odd and $1 + v_2(p-1) < j \leq v_2(p^2-1)$. Then, $j - 1 > v_2(p-1)$, so that $l_p(2^{j-1}m)$ is even. Using $l_p(m)$ odd, this implies that $2l_p(m) \mid f$, so that $2^j \mid (p^2-1) \mid (p^f-1)$, contradicting $p^f \equiv \frac{1}{2}d + 1 \pmod{d}$.

Towards showing the "if" part, let $v = v_2(p^{l_p(m)} - 1)$. We have $p^{l_p(m)} - 1 \equiv 2^v m \pmod{2^{v+1}m}$, so that $2^{v+1}m \in \mathscr{B}_{p,0}$. If $j > v + 1$ and $l_p(m)$ is even, then with $f = 2^{j-v-1}l_p(m)$, Lemma 4.7 implies that $p^f - 1 \equiv 2^{j-1}m \pmod{2^j m}$, so that $2^j m \in \mathscr{B}_{p,0}$. If $l_p(m)$ is odd, then $v = v_2(p-1)$, so that $2^{v+1} \in \mathscr{B}_{p,0}$. Finally assume that $j > v_2(p^2-1)$ and $l_p(m)$ is odd. Then Lemma 4.7 implies that $p^{2^{j-v_2(p^2-1)}l_p(m)} - 1 \equiv 2^{j-1}m \pmod{2^j m}$, so that $2^j m \in \mathscr{B}_{p,0}$. This concludes the proof. □

Proof of Theorem 4.1. For $m \geq 1$ coprime to $2p$, let

$$f_p(m) := v_2\left(p^{l_p(m)} - 1\right), \quad f'_p(m) := \max\left\{f_p(m), v_2\left(p^2-1\right)\right\}.$$

Proposition 4.8 implies that if $2^j m \in \mathscr{B}_{p,0}$ with m odd, then $j > f_p(m)$. Further, if $(m, 2p) = 1$ then $2^j m \in \mathscr{B}_{p,0}$ for all $j > f'_p(m)$.

Using this last property, we have $\mathscr{B}_{p,0}(x)$ at least as big as the number of choices for m coprime to $2p$ with $1 < m \leq x/2^{f'_p(m)+1}$. Thus, the lower bound in the theorem will follow if we show that there are at least $b_p x/\log\log x$ integers m coprime to $2p$ with $m \leq x/2^{f'_p(m)+1}$.

Let $\lambda(m)$ denote Carmichael's function at m, which is the order of the largest cyclic subgroup of $\mathbb{U}_m$. Then $l_p(m) \mid \lambda(m)$. Also, for $m > 2$, $\lambda(m)$ is even, so that

$$f'_p(m) \leq g_p(m) := v_2\left(p^{\lambda(m)} - 1\right).$$

Thus, the lower bound in the theorem will follow if we show that there are at least $b_p x/\log\log x$ integers m coprime to $2p$ with $m \leq x/2^{g_p(m)+1}$. Using Lemma 4.7, we have $g_p(m)+1 = v_2(\lambda(m)) + v_2(p^2-1)$. Further, it is easy to see that $2^{v_2(p^2-1)} \le 2(|p|+1)$, with equality when $|p|+1$ is a power of 2.

It follows from [10, Section 2, Remark 1] that uniformly for all $x \ge 3$ and all positive integers n,

$$\sum_{\substack{r \le x \\ r \text{ prime} \\ n \mid r-1}} \frac{1}{r} = \frac{\log\log x}{\varphi(n)} + O\left(\frac{\log(2n)}{\varphi(n)}\right). \tag{4.9}$$

We apply this with $n = 2^{g_0+1}$, where g_0 is the first integer with $2^{g_0} \ge 4\log\log x$. Thus, if $\mathscr{R}$ is the set of primes $r \le x$ with $v_2(r-1) > g_0$, we have for x sufficiently large,

$$\sum_{r \in \mathscr{R}} \frac{1}{r} < \frac{1}{3}.$$

Let $z = x/(25|p|\log\log x)$. In $[1,z]$ there are $(\varphi(|p|)/(2|p|))z + O_p(1)$ integers coprime to $2p$. And for a given value of $r \in \mathscr{R}$, there are at most $(\varphi(|p|)/(2|p|))z/r + O_p(1)$ numbers in $[1,z]$ coprime to $2p$ and divisible by r. It follows that for x sufficiently large depending on the choice of p, there are at least

$$\frac{\varphi(|p|)}{2|p|}z - \frac{\varphi(|p|)}{2|p|}z\sum_{r \in \mathscr{R}} \frac{1}{r} + O_p\left(\sum_{r \in \mathscr{R}} 1\right) > \frac{\varphi(|p|)}{4|p|}z$$

integers $m \le z$ coprime to $2p$ and not divisible by any prime $r \in \mathscr{R}$. (We used that $|\mathscr{R}| = O(x/\log x)$ to estimate the O-term above.)

It remains to note that if $m \le z$, m is coprime to $2p$, and m is not divisible by any prime in $\mathscr{R}$, then $v_2(\lambda(m)) \le g_0$, so that

$$\begin{aligned} 2^{g_p(m)+1} &\le 2^{v_2(\lambda(m))+v_2(p^2-1)} \le 2^{g_0}2^{v_2(p^2-1)} \\ &\le 2^{g_0}\cdot 2(|p|+1) \le 2^{g_0}\cdot 3|p| < 25|p|\log\log x. \end{aligned}$$

Thus, $2^{g_p(m)+1}m \in \mathscr{B}_{p,0}$ and $2^{g_p(m)+1}m \le x$, so that

$$\mathscr{B}_{p,0}(x) \ge \frac{\varphi(|p|)}{100p^2}\frac{x}{\log\log x},$$

for x sufficiently large depending on the choice of p. This completes our proof of the lower bound.

For the upper bound, it suffices to show that

$$N(x) := \mathscr{B}_{p,0}(x) - \mathscr{B}_{p,0}(x/2) = O_p\left(\frac{x}{\log\log x}\right).$$

(With this assumption, no two numbers d counted can have the same odd part.) We shall assume that p is not a square, the case when $p = p_0^{2^j}$ for some integer p_0 and $j \geq 1$ being only slightly more complicated. From Proposition 4.8, $N(x)$ is at most the number of odd numbers m coprime to p with $m \leq x/2^{f_p(m)+1}$. Let $N_k(x)$ be the number of odd numbers $m \leq x/2^{k+1}$ with m coprime to p and $f_p(m) = k$. Then

$$N(x) = \sum_k N_k(x) = \sum_{2^k \leq \log\log x} N_k(x) + O\left(\frac{x}{\log\log x}\right).$$

We now concentrate our attention on $N_k(x)$ with $2^k \leq \log\log x$. If $f_p(m) = k$, then m is not divisible by any prime r with $(p/r) = -1$ and $2^{k+1} \mid r-1$. Then, using (4.9) and quadratic reciprocity,

$$\sum_{\substack{r \leq x \\ (p/r)=-1 \\ 2^{k+1} \mid r-1 \\ r \text{ prime}}} \frac{1}{r} = \frac{\log\log x}{2^{k+1}} + O_p\left(\frac{k}{2^k}\right).$$

By Proposition 4.6, the number of integers $m \leq x/2^{k+1}$ not divisible by any such prime r is at most

$$O\left(\frac{x}{2^{k+1}} \exp\left(-\sum_r \frac{1}{r}\right)\right) = O_p\left(\frac{x}{2^{k+1}} \exp\left(-\frac{\log\log x}{2^{k+1}}\right)\right).$$

Summing this expression for $2^k \leq \log\log x$ gives $O_p(x/\log\log x)$, which completes the proof of Theorem 4.1.

Remark 4.10. One might wonder if there is a positive constant β_p such that if p is odd with $|p| > 1$, then $\mathscr{B}_{p,0}(x) \sim \beta_p x/\log\log x$ as $x \to \infty$. Here we sketch an argument that no such β_p exists, that is,

$$0 < \liminf_{x\to\infty} \frac{\mathscr{B}_{p,0}(x)}{x/\log\log x} < \limsup_{x\to\infty} \frac{\mathscr{B}_{p,0}(x)}{x/\log\log x} < \infty.$$

First note that but for $O_p(x/(\log x)^{1/2})$ values of $d \leq x$, there is a prime $r \mid d$ with $(p/r) = -1$. (We are assuming here that p is not a square.) For such values of $d = 2^j m$, with m odd, we have $2 \mid l_p(m)$, so that in the notation above we have $f_p(m) = f'_p(m) \geq 3$. Thus it suffices to count numbers $2^j m \leq x$ with m odd and $j > f_p(m) \geq 3$. Note that

$$f_p(m) = v_2(l_p(m)) + v_2(p^2 - 1) - 1 = v_2(l_p(m)) + h_p - 1,$$

say. Further,

$$v_2(l_p(m)) = \max_{r \mid m} v_2(l_p(r)),$$

where r runs over the prime divisors of m. We have $\{r \text{ prime} : v_2(l_p(r)) = k\}$ equal to

$$\bigcup_{i\geq 0}\big\{r \text{ prime} : v_2(r-1) = k+i,\\ p \text{ is a } 2^i \text{ power } \pmod r \text{ and not a } 2^{i+1} \text{ power } \pmod r\big\}.$$

For $k > (\log\log\log x)^2$, the density of primes $r \equiv 1 \pmod{2^k}$ is so small that we may assume that no d is divisible by such a prime r. For k below this bound, the density of primes r with $v_2(l_p(r)) = k$ is $1/(3\cdot 2^{k-1})$. Thus, there is a positive constant $c_{k,p}$ with $c_{k,p} \to 1$ as $k \to \infty$ such that the density of integers m coprime to $2p$ and with $f_p(m) < k + h_p$ is asymptotically equal to

$$c_p(\varphi(2|p|)/(2|p|))\exp(-(\log\log x)/(3\cdot 2^k)),$$

as $x \to \infty$. Thus, the number of $m \leq x/2^{k+h_p}$ coprime to $2p$ and with $f_p(m) = k + h_p - 1$ is asymptotically equal to

$$c_{k,p}\frac{\varphi(2|p|)}{2|p|}\frac{x}{2^{k+h_p}}\frac{\log\log x}{3\cdot 2^k}\exp\left(-\frac{\log\log x}{3\cdot 2^k}\right)$$

as $x \to \infty$. This expression then needs to be summed over k. For k small, the count is negligible because of the exp factor. For k larger, we can assume that the coefficients $c_{k,p}$ are all 1, and then the sum takes on the form

$$\frac{\varphi(2|p|)}{2|p|2^{h_p}}\frac{x}{\log\log x}\sum_k \frac{(\log\log x)^2}{3\cdot 2^{2k}}\exp\left(-\frac{\log\log x}{3\cdot 2^k}\right).$$

Letting this sum on k be denoted $g(x)$, it remains to note that $g(x)$ is bounded away from both 0 and ∞ yet does not tend to a limit, cf. [5, Theorem 3.25].

To prove Theorem 4.3, we first establish the following result.

Proposition 4.11. *Let p be an integer with $|p| > 1$. Let d be a positive integer coprime to p such that d is divisible by odd primes s, t with*

$$l_p(s) \equiv 2 \pmod 4,\quad l_p(t) \equiv 1 \pmod 2,\quad \langle p, -1 \bmod s\rangle \neq \mathbb{U}_s,\quad \langle p, -1 \bmod t\rangle \neq \mathbb{U}_t.$$

Assume that $4 \mid l_p(d)$. *Then either* $4 \mid d$ *and* $\frac{1}{2}d + 1 \in \langle p \bmod d\rangle$ *or* $\langle p \bmod d\rangle$ *is not balanced.*

Proof. Let $k = l_p(d)$. First assume that $4 \mid d$ and $\frac{1}{2}d + 1 \notin \langle p \bmod d\rangle$. Let 2^κ be the largest power of 2 in k. Write $d = 2^j m$ where m is odd, let 2^{κ_1} be the power of 2 in $l_p(m)$, and let $2^{\kappa_2} = l_p(2^j)$. Then $\kappa = \max\{\kappa_1, \kappa_2\}$. Suppose that $\kappa_2 > \kappa_1$. We have $p^{k/2} \equiv 1 \pmod m$ and $p^{k/2} \not\equiv 1 \pmod{2^j}$. Since $4 \mid k$, we have $p^{k/2} + 1 \equiv 2$

mod 4, and since $p^k - 1 = (p^{k/2}-1)(p^{k/2}+1)$, we have $p^{k/2} \equiv 1 \pmod{2^{e-1}}$. Thus, $p^{k/2} \equiv \frac{1}{2}d + 1 \pmod{d}$, contrary to our assumption. Hence, we may assume that $\kappa = \kappa_1 \geq \kappa_2$. Note that this inequality holds too in the case that $4 \nmid d$, since then $\kappa_2 = 0$.

We categorize the odd prime powers r^a coprime to p as follows:

- **Type 1**: $\langle p, -1 \bmod r^a \rangle = \mathbb{U}_{r^a}$.
- **Type 2**: $\langle p, -1 \bmod r^a \rangle \neq \mathbb{U}_{r^a}$.
- **Type 3**: It is Type 2 and also $l_p(r^a) \equiv 2 \pmod{4}$.
- **Type 4**: It is Type 2 and also $l_p(r^a)$ is odd.

By assumption d has at least one Type 3 prime power component and at least one Type 4 prime power component. We will show that $\langle p \bmod d \rangle$ is not balanced in $\mathbb{U}_d$. By Proposition 2.4, it is sufficient to exhibit an odd character $\chi \pmod{d}$ that is trivial at p with conductor d' divisible by the same odd primes as are in d, and with either $d \equiv 2 \pmod{4}$ or d/d' odd.

Let $r_1^{a_1} \| d$ where the power of 2 in $l_p(r_1^{a_1})$ is 2^{κ_1}. (Note that $r_1^{a_1}$ cannot be Type 3 nor Type 4, since we have $\kappa_1 = \kappa \geq 2$, so that $4 \mid l_p(r_1^{a_1})$.) Consider the Type 1 prime powers in d, other than possibly $r_1^{a_1}$ in case it is of Type 1. For each we take the quadratic character, and we multiply these together to get a character χ_1 whose conductor contains all of the primes involved in Type 1 prime powers, except possibly r_1.

If $j \leq 1$, we let ψ_{2^j} be the principal character mod 2^j. If $j \geq 2$, let ψ_{2^j} be a primitive character mod 2^j with $\psi_{2^j}(p) = \zeta$, a primitive 2^{κ_2}-th root of unity. Let $\chi_2 = \chi_1 \psi_{2^j}$.

We choose a character $\psi_{r_1^{a_1}}$ mod $r_1^{a_1}$ with $\psi_{r_1^{a_1}}(p) = \chi_2(p)^{-1}$ if $\chi_2(p) \neq 1$, and otherwise we choose it so that $\psi_{r_1^{a_1}}(p) = -1$. Thus, this character is non-principal. Let $\chi_3 = \psi_{r_1^{a_1}} \chi_2$. We now have $\chi_3(p) = \pm 1$.

If $\chi_3(p) = -1$ we use a Type 3 prime power $r_3^{a_3} \| d$ and choose a character $\psi_{r_3^{a_3}} \pmod{r_3^{a_3}}$ with $\psi_{r_3^{a_3}}(p) = -1$. Let $\chi_4 = \chi_3 \psi_{r_3^{a_3}}$. If $\chi_3(p) = 1$, we let $\chi_4 = \chi_3$. We now have $\chi_4(p) = 1$.

If $\chi_4(-1) = 1$, we use a Type 4 prime power $r_4^{a_4} \| d$ and choose a character $\psi_{r_4^{a_4}} \pmod{r_4^{a_4}}$ with $\psi_{r_4^{a_4}}(p) = 1$ and $\psi_{r_4^{a_4}}(-1) = -1$. Let $\chi_5 = \chi_4 \psi_{r^a}$. If $\chi_4(-1) = -1$, we let $\chi_5 = \chi_4$.

All remaining prime powers r^a in d are of Type 2. For these we take non-principal characters that are trivial on $\langle p, -1 \bmod r^a \rangle$ and multiply them in to χ_5 to form χ_6. This is the character we are looking for, and so $\langle p \bmod d \rangle$ is not balanced. This completes our proof. □

Proof of Theorem 4.3. In the proof we shall assume that p is neither a square nor twice a square, showing in these cases that we may take $\varepsilon_p = 1/16$. The remaining cases are done with small adjustments to the basic argument but may require a smaller value for ε_p.

Let $d \le x$ be coprime to p. The set of primes $r \nmid p$ with $r \equiv 1 \pmod 4$ and for which p is a quadratic nonresidue has density $1/4$, and in fact, the sum of reciprocals of such primes $r \le x$ is $\frac{1}{4}\log\log x + O_p(1)$. (This follows from either (4.9) and quadratic reciprocity or from the Chebotarev density theorem.) Thus by Proposition 4.6, the number of integers $d \le x$ not divisible by any of these primes r is $O_p(x/(\log x)^{1/4})$. Thus, we may assume that d is divisible by such a prime r and so that $4 \mid l_p(d)$.

Note that if $r \equiv 5 \pmod 8$ and that p is a quadratic residue modulo r, but not a fourth power, then any r^a is of Type 3. The density of these primes r is $1/16$, by the Chebotarev theorem; in fact, the sum of reciprocals of such primes $r \le x$ is $\frac{1}{16}\log\log x + O_p(1)$. So the number of values of $d \in [3,x]$ not divisible by at least one of them is $O_p(x/(\log x)^{1/16})$, using Proposition 4.6. Also note that if $r \equiv 5 \pmod 8$ and p is a nonzero fourth power modulo r, then any r^a is Type 4. The density of these primes r is also $1/16$, and again the number of $d \in [3,x]$ not divisible by at least one of them is $O_p(x/(\log x)^{1/16})$.

Thus, the number of values of $d \le x$ coprime to p and not satisfying the hypotheses of Proposition 4.11 is $O(x/(\log x)^{1/16})$. This completes the proof of Theorem 4.3.

5 The Average and Normal Order of the Rank

In this section we consider the average and normal order of the rank of the curve E_d given in Theorem 1.1 as d varies.

It is clear from Theorem 1.1 that for q odd,

$$\operatorname{Rank} E_d(\mathbb{F}_q(u)) \le \begin{cases} d-2 & \text{if } d \text{ is even} \\ d-1 & \text{if } d \text{ is odd} \end{cases}$$

with equality when $d \in \mathscr{B}_{p,1}$ and $q \equiv 1 \pmod d$.

For all q and $d > 1$, it is known [1, Prop. 6.9] that

$$\operatorname{Rank} E_d(\mathbb{F}_q(u)) \le \frac{d}{2\log_q d} + O\left(\frac{d}{(\log_q d)^2}\right).$$

(Here $\log_q d$ is the logarithm of d base q, i.e., $\log d/\log q$.) We do not include the details here, but this bound can be proved directly for the the curves in Theorem 1.1 using that theorem. In addition, for q odd, considering values of d of the form $q^f + 1$ for some positive integer f and using Theorem 1.1, we see that the main term in this inequality is sharp for this family of curves.

We show below that although the average rank of $E_d(\mathbb{F}_q(u))$ is large—its average for d up to x is at least $x^{1/2}$—for "most" values of d the rank is much smaller.

Theorem 5.1. *There is an absolute constant $\alpha > \frac{1}{2}$ with the following property: For each odd prime p and finite field $\mathbb{F}_q$ of characteristic p, with $\mathbb{F}_q(u)$ and E_d as in Theorem 1.1, we have*

$$x^{\alpha} \le \frac{1}{x} \sum_{d \le x} \operatorname{Rank} E_d(\mathbb{F}_q(u)) \le x^{1-\log\log\log x/(2\log\log x)}$$

for all sufficiently large x depending on the choice of p.

Proof. This result follows almost immediately from [11, Theorem 1]. A result is proved there for the average value of the rank of curves in a different family also parametrized by a positive integer d. Using the notation from this chapter, if $d \in \mathscr{B}_{p,1}$, the rank of the curve considered in [11] is within 4 of

$$\sum_{\substack{e \mid d \\ e > 2}} \frac{\varphi(e)}{l_q(e)}. \tag{5.2}$$

We have $d \in \mathscr{B}_{p,1}$ implies that $e \in \mathscr{B}_{p,1}$ for all $e \mid d$ with $e > 2$. By Theorem 1.1, formula (5.2) is exactly the rank of $E_d(\mathbb{F}_q(u))$ for $d \in \mathscr{B}_{p,1}$. Since the proof of the lower bound x^{α} in [11] uses only values of $d \in \mathscr{B}_{p,1}$, we have the lower bound x^{α} in the present theorem.

Since the rank of $E_d(\mathbb{F}_q(u))$ is bounded above by the formula (5.2) whether or not d is in $\mathscr{B}_{p,1}$, and in fact whether or not $\langle p \bmod d \rangle$ is balanced, the argument given in [11] for the upper bound gives our upper bound here. $\square$

Theorem 5.3. *For each odd prime p and finite field $\mathbb{F}_q$ of characteristic p, with $\mathbb{F}_q(u)$ and E_d as in Theorem 1.1, we have but for $o(x/\log\log x)$ values of $d \le x$ with $d \in \mathscr{B}_p$ that*

$$\operatorname{Rank} E_d(\mathbb{F}_q(u)) \ge (\log d)^{(1+o(1))\log\log\log d}$$

as $x \to \infty$. Further, assuming the GRH, we have but for $o(x/\log\log x)$ values of $d \le x$ with $d \in \mathscr{B}_p$ that

$$\operatorname{Rank} E_d(\mathbb{F}_q(u)) \le (\log d)^{(1+o(1))\log\log\log d}$$

as $x \to \infty$. Assuming the GRH, this upper bound holds but for $o(x)$ values of $d \le x$ coprime to p as $x \to \infty$, regardless of whether $d \in \mathscr{B}_p$.

Proof. For $d \in \mathscr{B}_p$, Theorem 1.1 implies that the rank of $E_d(\mathbb{F}_q(u))$ is at least $\varphi(d)/l_q(d) \ge \varphi(d)/\lambda(d)$, where λ was defined in the previous section as the order of the largest cyclic subgroup of $\mathbb{U}_d$. It is shown in the proof of Theorem 2 in [3] that on a set of asymptotic density 1, we have $\varphi(d)/\lambda(d) = (\log d)^{(1+o(1))\log\log\log d}$. We would like to show this holds for almost all $d \in \mathscr{B}_p$. Note that we have $\varphi(m)/\lambda(m) = (\log m)^{(1+o(1))\log\log\log m}$ for almost all odd numbers m. We have for all odd m and every integer $j \ge 0$ that

$$\frac{\varphi(m)}{\lambda(m)} \leq \frac{\varphi(2^j m)}{\lambda(2^j m)} \leq 2^j \frac{\varphi(m)}{\lambda(m)}. \tag{5.4}$$

Thus, for almost all odd numbers m, we have for all nonnegative integers j with $2^j \leq \log m$ that $\varphi(2^j m)/\lambda(2^j m)) = (\log(2^j m))^{(1+o(1))\log\log\log(2^j m)}$. Further, it follows from (4.9) that but for a set of odd numbers m of asymptotic density 0, we have $v_2(\lambda(m)) \leq 2\log\log\log m$. It thus follows from Proposition 4.8 that for almost all odd numbers m, there is some nonnegative j with $2^j m \in \mathscr{B}_p$ and $2^j \leq \log m$. By Theorems 4.1 and 4.3 almost all members of $\mathscr{B}_p$ are of this form, and so we have the lower bound in the theorem.

For the upper bound, we use an argument in [6]. There, Corollary 2 and the following remark imply that under the assumption of the GRH, for almost all numbers d coprime to p, we have $\varphi(d)/l_q(d) = (\log d)^{(1+o(1))\log\log\log d}$. We use that $\varphi(e)/l_q(e) \mid \varphi(d)/l_q(d)$ for $e \mid d$ and from the normal order of the number-of-divisors function $\tau(d)$, that most numbers d have $\tau(d) \leq \log d$. It thus follows from Theorem 1.1 and the GRH that for almost all numbers d coprime to p that

$$\operatorname{Rank} E_d(\mathbb{F}_q(u)) \leq \tau(d)\frac{\varphi(d)}{l_q(d)} \leq (\log d)\frac{\varphi(d)}{l_q(d)} = (\log d)^{(1+o(1))\log\log\log d}.$$

We would like to show as well that this inequality continues to hold for almost all d that are in $\mathscr{B}_p$. As above, the GRH implies that for almost all odd numbers m coprime to p, we have $\varphi(m)/l_q(m) = (\log m)^{(1+o(1))\log\log\log m}$. Since (5.4) continues to hold with l_q in place of λ, it follows that for almost all odd m and for all j with $1 \leq 2^j \leq \log m$, that $\varphi(2^j m)/l_q(2^j m) = (\log(2^j m))^{(1+o(1))\log\log\log(2^j m)}$. Again using the normal order of the number-of-divisors function τ, we have that for almost all odd m and all j with $1 \leq 2^j \leq \log m$, that $\tau(2^j m) \leq \log m$. Further, as we noted above, from Theorems 4.1 and 4.3, it follows that almost all members d of $\mathscr{B}_p$ are of the form $2^j m$ with m odd and $2^j \leq \log m$. The rank formula in Theorem 1.1 implies that the rank of $E_d(\mathbb{F}_q(u))$ is bounded above by $\tau(d)\varphi(d)/l_q(d)$. Thus, for almost all $d \in \mathscr{B}_p$, we have the rank at most $(\log d)^{(1+o(1))\log\log\log d}$. This completes the proof. □

Acknowledgements The authors gratefully thank the referee for some useful suggestions. In addition, CP acknowledges partial support from NSF grant DMS-1001180.

References

1. A. Brumer, The average rank of elliptic curves. I. Invent. Math. **109**, 445–472 (1992)
2. R. Conceição, C. Hall, D. Ulmer, Explicit points on the Legendre curve II (2013, in preparation)
3. P. Erdős, C. Pomerance, E. Schmutz, Carmichael's lambda function. Acta Arith. **58**, 363–385 (1991)
4. H. Halberstam, H.-E. Richert, *Sieve Methods* (Academic Press, London, 1974)

5. S. Li, On Artin's conjecture for composite moduli. Ph.D. Thesis, U. Georgia, 1998
6. S. Li, C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli. J. Reine Angew. Math. **556**, 205–224 (2003)
7. D. Marcus, *Number Fields* (Springer, New York, 1977)
8. H.L. Montgomery, R.C. Vaughan, *Multiplicative Number Theory. I. Classical Theory* (Cambridge U. Press, Cambridge, 2007)
9. P. Moree, On the divisors of $a^k + b^k$. Acta Arith. **80**, 197–212 (1997)
10. C. Pomerance, On the distribution of amicable numbers. J. Reine Angew. Math. **293/294**, 217–222 (1977)
11. C. Pomerance, I.E. Shparlinski, Rank statistics for a family of elliptic curves over a function field. Pure Appl. Math. Q. **6**, 21–40 (2010)
12. D. Ulmer, Explicit points on the Legendre curve. Preprint available at arXiv:1002.3313