Rank statistics for a family of elliptic curves over a function field

Carl Pomerance
Department of Mathematics, Dartmouth College
Hanover, NH 03755-355, USA
carl.pomerance@dartmouth.edu

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

November 19, 2006

dedicated to John Tate

Abstract

We show that the average and typical ranks in a certain parametric family of elliptic curves described by Ulmer are large.

2000 Mathematics Subject Classification: 11N25, 11R17, 11R37
The first author was supported in part by NSF grant DMS-0401422. The second author was supported in part by ARC grant DP0556431.

1 Introduction

1.1 Background

Let $\mathbb{F}_q$ be the finite field of q elements of prime characteristic p. We consider the parametric family of curves

$$\mathbf{E}_d : \quad y^2 + xy = x^3 - t^d$$

over the function field $\mathbb{F}_q(t)$.

Denote by $\mathcal{U}_p$ the set of positive integers which divide some member of the sequence $p^n + 1$, for $n = 1, 2, \ldots$. Let φ denote Euler's function, and for a, b coprime integers with $b > 0$, let $\ell_a(b)$ be the multiplicative order of the residue class a in the group $(\mathbb{Z}/b\mathbb{Z})^\times$. We always have $\ell_a(b) \mid \varphi(b)$. Ulmer [17] has shown that for every $d \in \mathcal{U}_p$, the rank $R_q(d)$ of $\mathbf{E}_d$ over $\mathbb{F}_q(t)$ is given by

$$R_q(d) \;=\; I_q(d) - C_q(d), \tag{1}$$

where

$$I_q(d) \;=\; \sum_{e \mid d} \frac{\varphi(e)}{\ell_q(e)}$$

and $C_q(d)$ is an explicit correction term that always satisfies $0 \le C_q(d) \le 4$. (Note that $d \in \mathcal{U}_p$ implies that $\gcd(e, q) = 1$ for each $e \mid d$, so that $I_q(d)$ is well defined.) In fact, he shows that the Birch–Swinnerton Dyer conjecture holds for the curves $\mathbf{E}_d$ so that the rank computation holds for both the algebraic and analytic ranks.

Ulmer [17] considers the specific case $d = p^n + 1$ and $q = p$. Then $\ell_p(d) = 2n$, and each $\ell_p(e) \mid 2n$, so that

$$I_p(p^n + 1) \;\ge\; \sum_{e \mid p^n + 1} \frac{\varphi(e)}{2n} \;=\; \frac{p^n + 1}{2n}.$$

Thus,

$$R_p(d) \;\ge\; \frac{d \log p}{2 \log d} - 4,$$

which compares very nicely with the upper bound

$$R_p(d) \;\le\; \frac{d \log p}{2 \log d} + O\left(\frac{d (\log p)^2}{(\log d)^2}\right)$$

(uniformly over d and p) due to Brumer [2].

It is interesting that the expression $I_q(d)$ occurs in other contexts. For example, Moree and Solé [12] show that $I_q(d)$ is the number of irreducible factors of t^d-1 in $\mathbb{F}_q[t]$ and go on to apply $I_q(d)$ to a combinatorial problem.

1.2 Our results

Using (1), we show that on average over all numbers d (without the restriction that $d \in \mathcal{U}_p$), the rank is quite large.

Theorem 1. *There exists an absolute constant $\alpha > 1/2$, such that for all finite fields $\mathbb{F}_q$ and all sufficiently large large values of x (depending only on the characteristic p of $\mathbb{F}_q$),*

$$\frac{1}{x}\sum_{d\le x} R_q(d) \;\ge\; \frac{1}{x}\sum_{d\in\mathcal{U}_p(x)} R_q(d) \;\ge\; x^{\alpha}.$$

The constant α in Theorem 1 can be explicitly evaluated. Moreover, assuming the Elliott–Halberstam conjecture about the distribution of primes in residue classes (described below), we can show that α in Theorem 1 may be taken as any number smaller than 1.

This average order is presumably skewed by a few numbers d where the rank is especially big, at least that is the way we prove Theorem 1. One might wonder about $R_q(d)$ for a "typical" number d. We show that for almost all d, in the sense of asymptotic density, the rank is still fairly large.

Theorem 2. *Let $\mathbb{F}_q$ be a finite field of characteristic p and let $\varepsilon > 0$ be arbitrary. As $x \to \infty$, except for $o_{p,\varepsilon}(x)$ values of $d \le x$, we have*

$$R_q(d) \;\ge\; (\log d)^{(1/3-\varepsilon)\log\log\log d}.$$

It is shown in [2] that the average analytic rank over all elliptic curves over a function field of positive characteristic is bounded above by 2.3 asymptotically. Since the algebraic rank is bounded by the analytic rank, the same bound holds as well for the algebraic rank. Thus, Theorems 1 and 2 show that the thin family consisting of the curves $\mathbf{E}_d$ is indeed very special.

We remark that it seems very plausible that using the methods of [5] and [11] one can show that under the assumption of the Generalized Riemann Hypothesis for Kummerian fields over $\mathbb{Q}$, we have $R_q(d) = (\log d)^{(1+o(1))\log\log\log d}$

for almost all numbers $d \in \mathcal{U}_p$ in the sense of asymptotic density. We hope to take this up in a future paper.

Perhaps more importantly, it should be interesting to investigate the situation for more families of elliptic curves than the one family of Ulmer that we consider here. For example, in Darmon [3] quite general families are considered each of a similar flavor to Ulmer's. One does not know the Birch–Swinnerton-Dyer conjecture in many of these cases, but at least some statistical information might be gleaned for the analytic ranks.

1.3 Notation

We always use the letters l, p, r, s, and t to denote prime numbers, while d, e, k, m, and n always denote positive integers. We let $P(n)$ denote the largest prime factor of n if $n > 1$, and $P(1) = 1$.

As usual, we use $\pi(x; k, a)$ to denote the number of primes $r \le x$ with $r \equiv a \pmod{k}$, and we let $\pi(x)$ denote the total number of all primes $r \le x$.

Given a set $\mathcal{A}$ of positive integers, we use $\mathcal{A}(x)$ to denote the subset of $a \in \mathcal{A}$ with $a \le x$.

For any real number $x > 0$ and any integer $\nu \ge 1$, we write $\log_\nu x$ for the function defined inductively by $\log_1 x = \max\{\log x, 1\}$ (where $\log x$ is the natural logarithm of x) and $\log_\nu x = \log_1(\log_{\nu-1} x)$ for $\nu > 1$.

We use the order symbols O, o, $\ll$, $\gg$ with their usual meanings in analytic number theory, where all implied constants are *absolute*, unless specifically remarked otherwise (and indicated by subscripts). (We recall that the notations $A \ll B$, $B \gg A$ and $A = O(B)$ are equivalent.

We use $v_l(n)$ to denote the (exponential) l-adic valuation of n; that is, $v_l(n)$ is the exponent on the prime l in the prime factorization of n.

2 Preparations

2.1 Structure of $\mathcal{U}_p$

Recall that $\mathcal{U}_p$ is the set of natural numbers that divide $p^n + 1$ for some positive integer n.

Lemma 3. *Suppose $d \in \mathcal{U}_p$.*

(i) There is a positive integer k such that $v_2(\ell_p(r)) = k$ for each odd prime factor r of d.

(ii) If $p > 2$ and $k = 1$, then $v_2(d) \le v_2(p+1)$, while if $p > 2$ and $k > 1$, then $v_2(d) \le 1$.

Proof. Suppose $d \in \mathcal{U}_p$ and r is an odd prime factor of d. Since $d \mid p^n + 1$ for some positive integer n, we have $r \mid p^n + 1$ and $r \nmid p^n - 1$. Thus, $\ell_p(r) \mid 2n$ and $\ell_p(r) \nmid n$, so $v_2(\ell_p(r)) = v_2(2n) = v_2(n) + 1$. Thus, (i) follows with $k = v_2(n) + 1$. For (ii) note that from our proof of (i), $k = 1$ if and only if n is odd. But for odd n we have $v_2(p^n + 1) = v_2(p + 1)$, so $v_2(d) \le v_2(p + 1)$. And if $k > 1$, we have n even, so $p^n + 1 \equiv 2 \pmod 4$ and $v_2(d) \le 1$. □

For p prime and k a positive integer let $\mathcal{U}_{p,k}$ denote the set of integers d coprime to p such that for each odd prime $r \mid d$ we have $v_2(\ell_p(r)) = k$; further, if $p > 2, k = 1$, then $v_2(d) \le v_2(p + 1)$, and if $p > 2, k > 1$, then $v_2(d) \le 1$. Thus, Lemma 3 implies that $\mathcal{U}_p \subset \bigcup_{k \ge 1} \mathcal{U}_{p,k}$. In fact, they are equal.

Lemma 4. *For each prime p, we have $\mathcal{U}_p = \bigcup_{k \ge 1} \mathcal{U}_{p,k}$.*

Proof. Suppose $d \in \mathcal{U}_{p,k}$. We may assume $d > 2$. If d is a power of 2, then $k = 1$, $p > 2$, and $d | p + 1$, so that $d \in \mathcal{U}_p$. If d is not a power of 2, let d_o be the odd part of d and let $m = \ell_p(d_o)$. Then m is the least common multiple of the numbers $\ell_p(r^a)$ where r^a runs over the odd prime power divisors of d. We have $\ell_p(r^a)/\ell_p(r) \mid r^{a-1}$, so that if r is odd, we have $v_2(\ell_p(r^a)) = v_2(\ell_p(r)) = k$. Thus, $v_2(m) = k$ and we have $r \nmid p^{m/2} - 1$. But $r^a \mid p^m - 1$, so we have $r^a \mid p^{m/2} + 1$. Thus, the odd part of d divides $p^{m/2} + 1$. If $k > 1$ and $p > 2$, then $v_2(d) \le 1$, so that the even part of d also divides $p^{m/2} + 1$. Further, if $k = 1$ and $p > 2$, then $v_2(d) \le v_2(p + 1)$. In this case, $m/2$ is odd, so that $p + 1 \mid p^{m/2} + 1$, and so the even part of d again divides $p^{m/2} + 1$. We thus have that $d \mid p^{m/2} + 1$, and this concludes the proof. □

Let $\mathcal{R}_{p,k}$ denote the set of odd prime members of $\mathcal{U}_{p,k}$. That is,

$$\mathcal{R}_{p,k} \ = \ \{r \text{ an odd prime } : r \ne p, \ v_2(\ell_p(r)) = k\}.$$

Then, $\mathcal{U}_{p,k}$ is the set of integers d all of whose odd prime factors come from $\mathcal{R}_{p,k}$, with $v_2(d)$ bounded as discussed above. After a classical result of Wirsing [18], the distribution of the sets $\mathcal{U}_{p,k}$ within the natural numbers follows from the distribution of the sets $\mathcal{R}_{p,k}$ within the prime numbers in a way that is made more precise below.

The following result follows essentially from [14, Theorem 1.3], but we have slightly stronger error estimates and an explicit dependence on p. We discuss the proof in the next subsection.

Proposition 1. *Let x be large and let $p \le (\log x)^{1/3}$ be a prime number. Let $E(x) = x/(\log x)^{4/3}$. For $p > 2$, we have*

$$\#\mathcal{R}_{p,1}(x) \;=\; \frac{1}{3}\pi(x) + O(E(x)), \qquad \#\mathcal{R}_{p,2}(x) \;=\; \frac{1}{6}\pi(x) + O(E(x)),$$
$$\sum_{k\ge 3} \#\mathcal{R}_{p,k}(x) \;=\; \frac{1}{6}\pi(x) + O(E(x)).$$

Further,

$$\#\mathcal{R}_{2,1}(x) \;=\; \frac{7}{24}\pi(x) + O(E(x)), \qquad \#\mathcal{R}_{2,2}(x) \;=\; \frac{1}{3}\pi(x) + O(E(x)),$$
$$\sum_{k\ge 3} \#\mathcal{R}_{2,k}(x) \;=\; \frac{1}{12}\pi(x) + O(E(x)).$$

For p a prime, let

$$\mathcal{R}_p = \begin{cases} \mathcal{R}_{p,1}\,, & p > 2 \\ \mathcal{R}_{2,2}\,, & p = 2. \end{cases}$$

From Proposition 1 we have

$$\#\mathcal{R}_p(x) \;=\; \frac{1}{3}\pi(x) + O\left(\frac{x}{(\log x)^{4/3}}\right). \tag{2}$$

Though it will not be needed, we note that using Wirsing's theorem [18] (see too [16, Chapter II.7, Exercise 9]), we have the following result about the distribution of the sets $\mathcal{U}_p$.

Proposition 2. *For each prime p, there is a positive constant c_p such that*

$$\#\mathcal{U}_p(x) \;\sim\; c_p x/(\log x)^{2/3}$$

as $x \to \infty$.

Proof. It follows directly from Proposition 1 and the cited result of Wirsing that there are positive constants c_p such that

$$\#\mathcal{U}_{p,1}(x) \;\sim\; c_p x/(\log x)^{2/3} \;\text{ for }\; p \ge 3 \;\text{ and }\; \#\mathcal{U}_{2,2}(x) \;\sim\; c_2 x/(\log x)^{2/3}$$

as $x \to \infty$. From the same tools, we have

$$\#\mathcal{U}_{2,1}(x) \;\ll\; x/(\log x)^{17/24}, \qquad \#\mathcal{U}_{p,2}(x) \;\ll\; x/(\log x)^{5/6} \;\text{ for }\; p \ge 3,$$
$$\#\left(\bigcup_{k\ge 3} \mathcal{U}_{p,k}\right)(x) \;\ll\; x/(\log x)^{5/6} \;\text{ for all }\; p.$$

The result thus follows from Lemma 4. □

2.2 Chebotarev density theorem and its applications

We let L be a finite Galois extension of $\mathbb{Q}$ with the Galois group G of degree $k = [L : \mathbb{Q}]$ and discriminant Δ. Let $\mathcal{C}$ be a union of conjugacy classes of G. We define

$$\pi_{\mathcal{C}}(x, L/\mathbb{Q}) = \#\{p \leq x \ : \ p \text{ unramified in } L/\mathbb{Q}, \ \sigma_p \in \mathcal{C}\},$$

where σ_p is the Artin symbol of p in the extension $L/\mathbb{Q}$, see [7].

Combining a version of the Chebotarev density theorem due to Lagarias and Odlyzko [9] together with a bound for a possible Siegel zero due to Stark [15], we obtain the following result.

Lemma 5. *There are absolute constants $A_1, A_2 > 0$ such that if*

$$x \geq 10k(\log|\Delta|)^2$$

then

$$\left|\pi_{\mathcal{C}}(x, L/\mathbb{Q}) - \frac{\#\mathcal{C}}{\#G}\mathrm{li}\,(x)\right| \ll \frac{\#\mathcal{C}}{\#G}\mathrm{li}\,\left(x^{\beta}\right) + \|\mathcal{C}\| x \exp\left(-A_1\sqrt{\frac{\log x}{k}}\right)$$

with some β satisfying the inequality

$$\beta < 1 - \frac{A_2}{\max\{|\Delta|^{1/k}, \log|\Delta|\}},$$

where $\|\mathcal{C}\|$ is the number of conjugacy classes in $\mathcal{C}$.

Key to the proof of Proposition 1 is an estimate for the discriminants of certain number fields, which we now present. For algebraic number fields $K \subset L$, let $\Delta(L/K)$ denote the relative discriminant of L over K and let $\Delta(L) = \Delta(L/\mathbb{Q})$.

Lemma 6. *Let n, d be positive integers with $d \mid n$ and let a be a nonzero integer. Let h denote the largest integer for which a is an h-th power in $\mathbb{Z}$ and assume* $\gcd(d, h) = 1$. *For the field $L = \mathbb{Q}(e^{2\pi i/n}, a^{1/d})$, we have*

$$[L : \mathbb{Q}] \ = \ d\varphi(n) \ \ or \ \ d\varphi(n)/2, \quad |\Delta(L)| \ \leq \ (d\varphi(n)|a|)^{[L:\mathbb{Q}]}.$$

Proof. Let K be the cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$. It follows from (2) and (3) in [14] that $[L:\mathbb{Q}] = d\varphi(n)/\theta$ where $\theta = 1$ or 2. When $\theta = 2$ we have d even and $a^{1/2} \in K$. Thus, the minimum polynomial for $a^{1/d}$ over K is $x^{d/\theta} - a^{1/\theta} = f(x)$, say. From elementary algebraic number theory we have

$$\Delta(L) \;=\; \Delta(K)^{[L:K]} N_{K/\mathbb{Q}}(\Delta(L/K)).$$

Now $\Delta(L/K)$ divides $N_{L/K}(f'(a^{1/d}))$ (see [13, Proposition 2.9]) so that

$$N_{K/\mathbb{Q}}(\Delta(L/K)) \mid N_{K/\mathbb{Q}}(N_{L/K}(f'(a^{1/d}))) \;=\; N_{L/\mathbb{Q}}((d/\theta)a^{1/\theta-1/d}).$$

Since each conjugate of $(d/\theta)a^{1/\theta-1/d}$ has absolute value $(d/\theta)|a|^{1/\theta-1/d}$, we have

$$|N_{K/\mathbb{Q}}(\Delta(L/K))| \;\le\; ((d/\theta)|a|^{1/\theta-1/d})^{[L:\mathbb{Q}]} \;\le\; (d|a|)^{[L:\mathbb{Q}]}.$$

It is well-known and easy to see from Hadamard's inequality for determinants that $|\Delta(K)| \le \varphi(n)^{\varphi(n)}$. Thus $|\Delta(K)|^{[L:K]} \le \varphi(n)^{[L:K]\varphi(n)} = \varphi(n)^{[L:\mathbb{Q}]}$. Assembling our estimates gives the lemma. □

Remark. It is interesting to know when $[L:\mathbb{Q}] = d\varphi(n)$. Let $a = a_1 a_2^2$ where a_1 is squarefree. According to [14], $[L:\mathbb{Q}] = d\varphi(n)/2$ exactly when d is even, $a_1 \mid n$, and $a_1 \equiv 1 \pmod 4$ or when d is even, $4a_1 \mid n$, and $a_1 \not\equiv 1 \pmod 4$.

For a prime p and natural numbers d, n with $d \mid n$, let

$$L_{p,n,d} \;=\; \mathbb{Q}(e^{2\pi i/n}, p^{1/d})$$

and let $\varpi_p(x; n, d)$ denote the number of primes $r \le x$ with $r \equiv 1 \pmod n$ and $d \mid (r-1)/\ell_p(r)$. Thus, $\varpi_p(x; n, d)$ is the number of primes $r \le x$ which split completely in $L_{p,n,d}$. We may thus use Lemmas 5 and 6 to estimate $\varpi_p(x; n, d)$.

Lemma 7. *For $p, n \le (\log x)^{1/3}$ we have*

$$\varpi_p(x; n, d) \;=\; \frac{1}{[L_{p,n,d}:\mathbb{Q}]}\mathrm{li}\,(x) + O\left(\frac{x}{(\log x)^{3/2}}\right).$$

Proof. Using Lemma 6 and the assumptions $p, n \le (\log x)^{1/3}$, we have with $\Delta = \Delta(L_{p,n,d})$,

$$\begin{aligned} \max\{|\Delta|^{1/[L_{p,n,d}:\mathbb{Q}]}, \log|\Delta|\} &\le \max\{d\varphi(n)p, d\varphi(n)\log(dnp)\} \\ &\le d\varphi(n)(\log x)^{1/3} \end{aligned}$$

for x large. We apply Lemma 5 to the primes that split completely in $L_{p,n,d}$. Thus, $\#\mathcal{C} = 1$ and $\#G = d\varphi(n)$ or $d\varphi(n)/2$, the latter coming from Lemma 6. For $d\varphi(n) \le A_2(\log x)^{2/3}/\log\log x$, we have $\beta < 1 - \log\log x/\log x$ and

$$\frac{\#\mathcal{C}}{\#G}\mathrm{li}\,(x^\beta) \;\le\; \mathrm{li}\,(x^\beta) \;\ll\; \frac{x}{(\log x)^2}.$$

And if $d\varphi(n) > A_2(\log x)^{2/3}/\log\log x$, then $\#\mathcal{C}/\#G \ll \log\log x/(\log x)^{2/3}$, so that in either case,

$$\frac{\#\mathcal{C}}{\#G}\mathrm{li}\,(x^\beta) \;\ll\; \frac{x\log\log x}{(\log x)^{5/3}} \;\ll\; \frac{x}{(\log x)^{3/2}}.$$

The second error term in Lemma 5 is smaller than this estimate when $n \le (\log x)^{1/3}$, so we have the lemma. □

We are now in a position to prove Proposition 1. For example, take the case of $\mathcal{R}_{p,1}$ for $p > 2$. Let

$$\begin{aligned} N_{p,k} \;&=\; \varpi_p(x; 2^k, 2^{k-1}) - \varpi_p(x; 2^k, 2^k) \\ &\quad - \left(\varpi_p(x; 2^{k+1}, 2^{k-1}) - \varpi_p(x; 2^{k+1}, 2^k)\right). \end{aligned}$$

Then $N_{p,k}$ is precisely the number of primes $r \le x$ with $v_2(\ell_p(r)) = 1$, and $v_2(r-1) = k$. Indeed, the first two terms count those primes r satisfying these conditions plus some additional primes r for which $v_2(r-1) > k$, and the last two terms remove from the count these extra primes r. Thus,

$$\#\mathcal{R}_{p,1}(x) \;=\; \sum_{k\ge 1} N_{p,k}. \tag{3}$$

By the remark following Lemma 6 and by Lemma 7, if $2^{k+1} \le (\log x)^{1/3}$, we have

$$N_{p,k} \;=\; \left(\frac{1}{2^{2k-2}} - \frac{1}{2^{2k-1}} - \frac{1}{2^{2k-1}} + \frac{1}{2^{2k}}\right)\mathrm{li}\,(x) + O\left(\frac{x}{(\log x)^{3/2}}\right). \tag{4}$$

Note that the coefficient of $\mathrm{li}\,(x)$ simplifies to $1/2^{2k}$. We apply (4) in (3) for those values of k with $2^{k+1} \le (\log x)^{1/3}$, and for larger values of k we use that by the Brun–Titchmarsh theorem, see [16, Chapter I.4, Theorem 9],

$$N_{p,k} \;\le\; 2\pi(x; 2^k, 1) \;\ll\; \frac{\pi(x)}{2^k} \quad \text{for} \quad 2^k \le x^{1/2},$$

and also the elementary estimate

$$N_{p,k} \ \leq \ 2\pi(x; 2^k, 1) \ \leq \ \frac{2x}{2^k} \ \text{ for } \ 2^k > x^{1/2},$$

so obtaining $\#\mathcal{R}_{p,1} = \frac{1}{3}\pi(x) + O(x/(\log x)^{4/3})$.

The remaining cases of Proposition 1 follow in a similar manner, noting that when $p = 2$ we can be in the situation when $[L_{p,n,d} : \mathbb{Q}] = d\varphi(n)/2$. In fact the same method can be used to prove a somewhat more specialized result which we will use in the sequel. Suppose m is an odd integer not divisible by p. Let

$$\mathcal{R}_p^m \ = \ \{r \in \mathcal{R}_p : r \equiv 1 \pmod{m}\}. \tag{5}$$

For $p, m \leq (\log x)^{1/3}$ we have

$$\#\mathcal{R}_p^m(x) \ = \ \frac{1}{3\varphi(m)}\pi(x) + O\left(\frac{x}{(\log x)^{4/3}}\right). \tag{6}$$

We suppress the details.

2.3 Ranks of curves $\mathbf{E}_d$

We need the following inequality which allows us study the rank of $\mathbf{E}_d$ for an arbitrary $d \geq 1$.

Lemma 8. *For positive integers f, d with $f \mid d$, we have $R_q(d) \geq R_q(f)$.*

Proof. It is clear that $\mathbf{E}_d$ contains the subgroup of points $(x(t^g), y(t^g))$, where $g = d/f$. This subgroup is isomorphic to $\mathbf{E}_f$. □

For d a positive integer and p a prime, let d_p be the largest divisor of d whose every prime factor comes from $\mathcal{R}_p$. We are now able to combine Lemma 8 with (1) to get the following result.

Proposition 3. *Let $\mathbb{F}_q$ be a finite field of characteristic p. For every positive integer d we have*

$$R_q(d) \ \geq \ \sum_{e \mid d_p} \frac{\varphi(e)}{\ell_q(e)} - 4.$$

Let λ denote the Carmichael function; it is defined for each integer $d \geq 1$ as the largest order of an element in the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^\times$. More explicitly, for any prime power l^ν, one has

$$\lambda(l^\nu) = \begin{cases} l^{\nu-1}(p-1), & \text{if } l \geq 3 \text{ or } \nu \leq 2, \\ 2^{\nu-2}, & \text{if } l = 2 \text{ and } \nu \geq 3, \end{cases}$$

and for an arbitrary integer $d \geq 2$,

$$\lambda(d) = \operatorname{lcm}\left[\lambda(l^\nu) \ : \ l^\nu \mid d\right].$$

Note that $\lambda(1) = 1$.

If d is coprime to q, then as is immediate from the definitions,

$$\ell_q(d) \ \leq \ \lambda(d).$$

We conclude from Proposition 3 that for any finite field $\mathbb{F}_q$ of characteristic p and any positive integer d, we have

$$R_q(d) \ \geq \ \frac{\varphi(d_p)}{\lambda(d_p)} - 4. \tag{7}$$

3 Proof of Theorem 1

We follow the construction from Erdős [4] to construct integers v with many solutions to the equation $\varphi(n) = v$. When p, the characteristic of $\mathbb{F}_q$, is odd, let u be an integer such that $u \equiv 3 \pmod 4$ and the Legendre symbol (u/p) is -1; and if $p = 2$, let $u = 5$. Let $1/12 > \delta > 0$ be a small absolute constant to be chosen shortly, let z be large, and let

$$\mathcal{I} \ = \ [z^{1/2-2\delta}, z^{1/2-\delta}], \quad \mathcal{R} \ = \ \{r \text{ prime } : \ r \equiv u \pmod{4p},\ P(r-1) \in \mathcal{I}\}.$$

Note that any prime $r \equiv u \pmod{4p}$ is in $\mathcal{R}_p$, so in particular, we have $\mathcal{R} \subset \mathcal{R}_p$. Let r, s, t denote prime variables. We have

$$\#\mathcal{R}(z) \ = \ \sum_{s \in \mathcal{I}} \sum_{\substack{r \leq z \\ r \equiv u \pmod{4p} \\ r \equiv 1 \pmod{s}}} 1 \ - \ \sum_{s \in \mathcal{I}} \sum_{s < t < z/s} \sum_{\substack{r \leq z \\ r \equiv u \pmod{4p} \\ r \equiv 1 \pmod{st}}} 1 \ = \ S_1 - S_2,$$

say. Indeed, any integer $n \leq z$ is divisible by either 0, 1, or 2 distinct primes that are greater than $z^{1/2-2\delta}$, so S_1 counts 0, 1, or 2 correspondingly if $r - 1$

has 0, 1, or 2 primes in $\mathcal{I}$; and S_2 makes the necessary correction in the case of 2 primes, or in the case that $r-1$ is also divisible by a larger prime.

We now recall the Bombieri–Vinogradov theorem which states that for each A there is some number B such that

$$\sum_{m\le z^{1/2}/\log^B z} \max_{\gcd(a,m)=1} \left|\pi(z;m,a) - \frac{1}{\varphi(m)}\mathrm{li}\,(z)\right| \ll \frac{z}{\log^A z}, \tag{8}$$

see [16, Chapter II.8, Theorem 11].

Using (8) and p fixed, we have

$$S_1 \sim \frac{\log((1-2\delta)/(1-4\delta))}{\varphi(4p)}\pi(z) \text{ as } z\to\infty.$$

We reorganize S_2 by letting $(r-1)/st = a$, so that

$$S_2 = \sum_{a<z^{4\delta}} \sum_{s\in\mathcal{I}} \sum_{\substack{s<t<z/as \\ ast+1\equiv u \pmod{4p} \\ ast+1 \text{ prime}}} 1.$$

Note that since $z/as \le z^{1/2+3\delta}$, we have by Brun's method (see [8, Theorem 2.3]) that the double sum on s and t is

$$\sum_s \sum_t 1 \ll \frac{\log((1-2\delta)/(1-4\delta))}{\varphi(4pa)}\frac{z}{\log^2 z}.$$

Thus,

$$S_2 \ll \sum_{a<z^{4\delta}} \frac{\log((1-2\delta)/(1-4\delta))}{\varphi(4pa)}\frac{z}{\log^2 z} \ll \delta\frac{\log((1-2\delta)/(1-4\delta))}{\varphi(4p)}\pi(z)$$

using the Landau [10] estimate

$$\sum_{a<Z}\frac{1}{\varphi(a)} \ll \log Z$$

(which can be proved using the identity $1/\varphi(a) = (1/a)\sum_{d|a}\mu^2(d)/\varphi(d)$ and interchanging the order of summation).

Thus, there is an absolute value of $\delta > 0$ such that for all large z depending on the choice of p, we have $S_2 \le S_1/4$. We now fix such a value of δ. Note

that the identity $\#\mathcal{R}(z) = S_1 - S_2$ applied to $z/2$ shows that $\#\mathcal{R}(z/2) \le (1/2 + o(1))S_1$. We conclude that for z sufficiently large, depending on the choice of p, that

$$\#(\mathcal{R} \cap [z/2, z]) \ \ge \ \frac{\log((1-2\delta)/(1-4\delta))}{5\varphi(4p)}\pi(z). \tag{9}$$

Let x be large, and let

$$y \ = \ \frac{\log x}{\log_2 x} \qquad \text{and} \qquad z \ = \ y^{1/(1/2-\delta)}.$$

Let M_y denote the least common multiple of the integers in $[1, y]$ and let

$$\mathcal{Q} = \{r \in \mathcal{R} \cap [z/2, z] \ : \ r - 1 \mid M_y\}.$$

The number of primes $r \le z$ such that $\ell^k | r - 1$ for some prime power $\ell^k > y$ with $k \ge 2$ is bounded by

$$\sum_{2 \le k \le \log z/\log 2} \ \sum_{\ell \,:\, \ell^k \ge y} \frac{z}{\ell^k} \ \ll \ z \sum_{2 \le k \le \log z/\log 2} \frac{1}{k y^{1-1/k}} \ \ll \ \frac{z \log z}{y^{1/2}}.$$

Combining this with (9) we have

$$\#\mathcal{Q} \ \ge \ \kappa \frac{z}{\log z} \tag{10}$$

for z sufficiently large depending on the choice of p, where

$$\kappa \ = \ \frac{\log((1-2\delta)/(1-4\delta))}{6\varphi(4p)}.$$

We now put

$$m \ = \ \left\lfloor \frac{\log x}{\log z} \right\rfloor$$

and consider the set $\mathcal{S}$ of all products of m distinct primes from $\mathcal{Q}$. Clearly

$$x \ \ge \ d \ \ge \ (z/2)^m \ = \ x^{1+o(1)} \tag{11}$$

for every $d \in \mathcal{S}$. Recalling (10), we also have

$$\begin{aligned} \#\mathcal{S} \ &= \ \binom{\#\mathcal{Q}}{m} \ \ge \ \left(\frac{\#\mathcal{Q}}{m}\right)^m \ \ge \ \left(\frac{\kappa z}{\log x}\right)^m \ \ge \ \frac{1}{z}\left(\frac{\kappa z}{\log x}\right)^{\log x/\log z} \\ &= \ x \exp\left(-\frac{\log x}{\log z}(\log_2 x + O(1))\right) \\ &= \ x \exp\big(-(1/2-\delta)\log x + O(\log x \log_3 x/\log_2 x)\big) \ = \ x^{1/2+\delta+o(1)}. \end{aligned}$$

Note that for every $d \in \mathcal{S}$ we have

$$\ell_q(d) \mid \lambda(d) \mid M_y.$$

Thus, from the prime number theorem, we obtain that

$$\ell_q(d) \ \leq \ \exp((1+o(1))y) = x^{o(1)}.$$

By the construction of $\mathcal{S}$ and Lemma 4 we have $d \in \mathcal{U}_p$ so that (1) can be applied to compute $R_q(d)$. Therefore, (11) and a standard estimate for $\varphi(d)$ imply that

$$R_q(d) \ \geq \ I_q(d) - 4 \ \geq \ \frac{\varphi(d)}{\ell_q(d)} - 4 \ = \ \frac{d^{1+o(1)}}{x^{o(1)}} \ = \ x^{1+o(1)}.$$

Thus, using our estimate for $\#\mathcal{S}$, we have

$$\sum_{d \leq x} R_q(d) \ \geq \ x^{1+o(1)} \#\mathcal{S} \ \geq \ x^{3/2+\delta+o(1)}$$

which concludes the proof.

Remark. A key step in the proof is the use of the Bombieri–Vinogradov theorem (8). We have applied this result in the proof to moduli $4ps$ with $s \in \mathcal{I}$. The Elliott–Halberstam conjecture looks superficially the same, but the range for m is allowed to be much larger: For every $\varepsilon > 0, A > 0$,

$$\sum_{m \leq z^{1-\varepsilon}} \max_{\gcd(a,m)=1} \left| \pi(z;m,a) - \frac{1}{\varphi(m)} \mathrm{li}\,(z) \right| \ll \frac{z}{\log^A z}.$$

Assuming this conjecture, the above proof gives Theorem 1 for every value of $\alpha < 1$. The idea is similar to the proof of Theorem 3 in [1] and is also mentioned in [6]. Let k be an arbitrarily large integer, let $\mathcal{I}_k = [z^{1/k-1/k^2}, z^{1/k}]$, and let $\mathcal{R}$ be the set of primes $r \equiv u \pmod{4p}$ with $r-1$ divisible by $k-1$ primes from $\mathcal{I}_k$. The primes $r \leq z$ constructed in this way have $P(r-1) \leq z^\eta$, where $\eta = 1 - (k-1)^2/k^2$. Further, by the Elliott–Halberstam conjecture, there are at least $c_{k,p}\pi(z)$ such primes r, where $c_{k,p} > 0$ depends only on k and p. Let $y = \log x / \log_2 x$ as before and let $z = y^{1/\eta}$. We do not have to worry about taking only those values of r that are $\geq z/2$, since each r is already guaranteed to be at least $z^{1-\eta}$, so that the values of d formed at the end of the proof are $\geq x^{1-\eta+o(1)}$. Each of these values of d has $l_q(d) \leq x^{o(1)}$ as before, so that $R_q(d) \geq x^{1-\eta+o(1)}$. Moreover, as before, there are $x^{1+o(1)}/\exp(\log x \log_2 x / \log z) = x^{1-\eta+o(1)}$ values of d, so that the average in Theorem 1 is at least $x^{1-2\eta+o(1)}$. Since k is arbitrary, this then proves that the average is $x^{1+o(1)}$.

4 Proof of Theorem 2

Our proof closely follows the proof of Theorem 2 in [5]. This result gives the normal order of $\lambda(n)$, showing that for almost all n (that is, on a set of asymptotic density 1), we have $\lambda(n) = n/(\log n)^{(1+o(1))\log_3 n}$. Since for all n we have $n \geq \varphi(n) \gg n/\log_2 n$, it follows that for almost all n we have

$$\frac{\varphi(n)}{\lambda(n)} \;=\; (\log n)^{(1+o(1))\log_3 n}$$

as $n \to \infty$.

We first note the elementary fact that

$$m \mid n \;\;\Longrightarrow\;\; \frac{\varphi(m)}{\lambda(m)} \;\Big|\; \frac{\varphi(n)}{\lambda(n)}. \tag{12}$$

Indeed, by the Chinese remainder theorem, there is an integer a such that for each prime power $l^\nu \mid n$ we have $\ell_a(l^\nu) = \lambda(l^\nu)$. Then $\ell_a(n) = \lambda(n)$ and $\ell_a(m) = \lambda(m)$. The canonical epimorphism from $(\mathbb{Z}/n\mathbb{Z})^\times$ to $(\mathbb{Z}/m\mathbb{Z})^\times$ induces an epimorphism from $(\mathbb{Z}/n\mathbb{Z})^\times/\langle a\rangle$ to $(\mathbb{Z}/m\mathbb{Z})^\times/\langle a\rangle$, so that (12) follows.

Let x be large and let $y = y(x) = \log_2 x$. In view of (7), it suffices to show that

$$\log\varphi(d_p) - \log\lambda(d_p) \;=\; \frac{1}{3}y\log y + O_p(y\log_2 y) \tag{13}$$

for all $d \leq x$ with at most $o_p(x)$ exceptions. (In fact (13) is somewhat stronger than required in that we really only need a lower bound for the left side. Nevertheless it is interesting to know the true order of $\varphi(d_p)/\lambda(d_p)$ for almost all integers d.) For all d we have

$$\log\varphi(d_p) \;=\; \sum_l v_l(\varphi(d_p))\log l, \quad \log\lambda(d_p) \;=\; \sum_l v_l(\lambda(d_p))\log l,$$

where the sums are over all primes l. It follows from (6) and (19) in [5] that

$$\sum_{l\leq y\log y} v_l(\lambda(d_p))\log l \;\leq \sum_{l\leq y\log y} v_l(\lambda(d))\log l \;=\; y\log_2 y + O(y)$$

for all but $o(x)$ values of $d \leq x$. Using (12), we have for each prime l,

$$v_l(\varphi(d_p)) - v_l(\lambda(d_p)) \;\leq\; v_l(\varphi(d)) - v_l(\lambda(d)).$$

Also, from (20), (21), and (22) in [5] we have

$$\sum_{l>y\log y} (v_l(\varphi(d)) - v_l(\lambda(d)))\log l \ \le \ \frac{y\log_2 y}{\log y} + (\log y)^2$$

for all but $o(x)$ values of $d \le x$. It thus follows that

$$\sum_{l>y\log y} (v_l(\varphi(d_p)) - v_l(\lambda(d_p)))\log l \ \le \ \frac{y\log_2 y}{\log y} + (\log y)^2$$

for all but $o(x)$ values of $d \le x$. Thus, to prove that (13) holds for all but $o_p(x)$ values of $d \le x$, it suffices to show that

$$\sum_{l\le y\log y} v_l(\varphi(d_p))\log l \ = \ \frac{1}{3}y\log y + O_p(y\log_2 y) \tag{14}$$

holds for all but $o_p(x)$ values of $d \le x$.

As in [5], we prove (14) using the Turán–Kubilius inequality. For real-valued additive functions $g(n)$ this theorem asserts that if

$$E(g,x) \ = \ \sum_{r^\nu\le x} \frac{g(r^\nu)}{r^\nu}\left(1-\frac{1}{r}\right), \quad V(g,x) \ = \ \sum_{r^\nu\le x} \frac{g(r^\nu)^2}{r^\nu},$$

then

$$\sum_{n\le x} (g(n) - E(g,x))^2 \ \le \ 10xV(g,x), \tag{15}$$

see [16, Chapter III.3, Theorem 1]. Let

$$h(n) \ = \ \sum_{l\le y\log y} v_l(\varphi(n))\log l, \quad h_p(n) \ = \ \sum_{l\le y\log y} v_l(\varphi(n_p))\log l,$$

so that h and h_p are both additive functions. It is shown in [5, pp. 366–367] that

$$V(h,x) \ \ll \ y(\log y)^2.$$

Since $V(h_p,x) \le V(h,x)$, we have $V(h_p,x) \ll y(\log y)^2$.

For the determination of $E(h_p,x)$ we use (6). Since $h_p(r^\nu) \le \log(r^\nu)$, we have

$$E(h_p,x) \ = \ \sum_{r^\nu\le x} \frac{h_p(r^\nu)}{r^\nu}\left(1-\frac{1}{r}\right) \ = \ \sum_{r\le x} \frac{h_p(r)}{r} + O(1).$$

Now

$$\sum_{r\le x}\frac{h_p(r)}{r} \;=\; \sum_{l\le y\log y}\sum_{\substack{r\le x\\ r\in\mathcal{R}_p}}\frac{v_l(r-1)\log l}{r} \;=\; \sum_{l\le y\log y}\log l\sum_{i\ge 1}\sum_{\substack{r\le x\\ r\in\mathcal{R}_p\\ v_l(r-1)=i}}\frac{1}{r}.$$

The inner sum is $\ll y/l^i$, so the contribution for values of $i>1$ is $\ll y$. We conclude that

$$E(h_p,x) \;=\; \sum_{l\le y\log y}\log l\sum_{\substack{r\le x\\ r\in\mathcal{R}_p\\ r\equiv 1 \pmod l}}\frac{1}{r}+O(y). \tag{16}$$

Recall the notation $\mathcal{R}_p^m$ from (5). We use partial summation on the inner sum in (16) getting

$$\sum_{r\in\mathcal{R}_p^l(x)}\frac{1}{r} \;=\; \frac{\#\mathcal{R}_p^l(x)}{x}+\int_2^x\frac{\#\mathcal{R}_p^l(z)}{z^2}\,dz.$$

We use the estimate $\#\mathcal{R}_p^l(z)\le\pi(z;l,1)\ll\pi(z)/l$ for $z\le\exp(l^3)$, and we use (6) for larger values of z, getting that

$$\sum_{r\in\mathcal{R}_p^l(x)}\frac{1}{r} \;=\; \frac{y}{3(l-1)}+O\left(\frac{\log l}{l}\right).$$

Putting this into (16) we get that

$$E(h_p,x) \;=\; \sum_{l\le y\log y}\frac{y\log l}{3(l-1)}+O(y) \;=\; \frac{1}{3}y\log(y\log y)+O(y).$$

We now use this estimate for $E(h_p,x)$ and our earlier estimate for V in the Turán Kubilius inequality (15) applied to the function h_p. We get that the number of $d\le x$ with

$$\left|h_p(d)-\frac{1}{3}y\log y\right| \;>\; y\log_2 y$$

is $\ll xy(\log y)^2/(y\log_2 y)^2=o(x)$. This concludes the proof of (14) and so proves the theorem.

References

[1] W. Alford, A. Granville, and C. Pomerance, 'There are infinitely many Carmichael numbers', *Annals Math.*, **140** (1994), 703–722.

[2] A. Brumer, 'The average rank of elliptic curves I', *Invent. Math.*, **109** (1992), 445–472.

[3] H. Darmon, 'Heegner points and elliptic curves of large rank over function fields', in *Heegner points and Rankin L-series*, 317–322, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.

[4] P. Erdős, 'On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's φ-function', *Quart. J. Math. (Oxford Ser.)*, **6** (1935), 205–213.

[5] P. Erdős, E. Schmutz, and C. Pomerance, 'Carmichael's lambda function', *Acta Arith.*, **58** (1991), 363–385.

[6] A. Granville, 'Smooth numbers: Computational number theory and beyond', *Proc. MSRI Conf. Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, Berkeley 2000*, Cambridge Univ. Press, (to appear).

[7] G. Gras, *Class field theory*, Springer–Verlag, Belin, 2005.

[8] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[9] J. C. Lagarias and A. M. Odlyzko, 'A bound for the least prime ideal in the Chebotarev density theorem', in *Algebraic Number Fields*, 409–464, Academic Press, New York, 1977.

[10] E. Landau, 'Über die Zahlentheoretische Function $\varphi(n)$ und ihre Beziehung zum Goldbachschen Satz', *Nachr. Königlichen Ges. Wiss. Göttingen, Math.-Phys. Klasse*, 1900, 177–186.

[11] S. Li and C. Pomerance, 'On generalizing Artin's conjecture on primitive roots to composite moduli', *J. Reine Angew. Math.*, **556** (2003), 205–224.

[12] P. Moree and P. Solé, 'Around Pelikán's conjecture on very odd sequences', *Manuscripta Math.*, **117** (2005), 219–238.

[13] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers, third edition*, Springer-Verlag, Berlin, Heidelberg, 2004.

[14] F. Pappalardi, 'Squarefree values of the order function', *New York J. Math.*, **9** (2003), 331–344.

[15] H. M. Stark, 'Some effective cases of the Brauer-Siegel theorem', *Invent. Math.*, **3** (1974), 135-152.

[16] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.

[17] D. Ulmer, 'Elliptic curves with large rank over function fields', *Ann. Math*, **155** (2002), 295–315.

[18] E. Wirsing, 'Über die Zahlen, deren Primteiler einer gegeben Menge angehören', *Arch. der Math.*, **7** (1956), 263–272.