AVERAGES OF THE NUMBER OF POINTS ON ELLIPTIC CURVES

GREG MARTIN, PAUL POLLACK, AND ETHAN SMITH

ABSTRACT. If E is an elliptic curve defined over $\mathbb{Q}$ and p is a prime of good reduction for E, let $E(\mathbb{F}_p)$ denote the set of points on the reduced curve modulo p. Define an arithmetic function $M_E(N)$ by setting $M_E(N) := \#\{p\colon \#E(\mathbb{F}_p) = N\}$. Recently, David and the third author studied the average of $M_E(N)$ over certain "boxes" of elliptic curves E. Assuming a plausible conjecture about primes in short intervals, they showed the following: for each N, the average of $M_E(N)$ over a box with sufficiently large sides is $\sim \frac{K^*(N)}{\log N}$ for an explicitly-given function $K^*(N)$.

The function $K^*(N)$ is somewhat peculiar: defined as a product over the primes dividing N, it resembles a multiplicative function at first glance. But further inspection reveals that it is not, and so one cannot directly investigate its properties by the usual tools of multiplicative number theory. In this paper, we overcome these difficulties and prove a number of statistical results about $K^*(N)$. For example, we determine the mean value of $K^*(N)$ over all N, odd N and prime N, and we show that $K^*(N)$ has a distribution function. We also explain how our results relate to existing theorems and conjectures on the multiplicative properties of $\#E(\mathbb{F}_p)$, such as Koblitz's conjecture.

1. INTRODUCTION

Let E be an elliptic curve defined over the field $\mathbb{Q}$ of rational numbers. For the sake of concreteness, we assume that the affine points of E are given by a Weierstrass equation of the form

$$E : Y^2 = X^3 + aX + b, \tag{1}$$

where a and b are integers satisfying the condition $-16(4a^3 + 27b^2) \neq 0$. For any prime p where E has good reduction, we let $E(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-points on the reduced curve. In [16], Kowalski introduced the arithmetic function $M_E(N)$, defined by

$$M_E(N) = \#\{p \text{ prime}\colon \#E(\mathbb{F}_p) = N\}.$$

The Hasse bound [13] implies that if p is counted by $M_E(N)$, then p lies between $(\sqrt{N}-1)^2$ and $(\sqrt{N}+1)^2$. Thus, $M_E(N)$ is a well-defined (finite) integer.

The problem of obtaining good estimates for $M_E(N)$ appears to be very difficult. The condition imposed by Hasse's bound together with an upper bound sieve gives the weak upper bound $M_E(N) \ll \sqrt{N}/\log(N+1)$ for any $N \geq 1$. Except in the case that E has complex multiplication, nothing stronger is known. As we will explain later, the average value of $M_E(N)$ as N varies over various sets of integers is related to some important theorems and conjectures in number theory. In [6], David and the third author established an "average value theorem" for $M_E(N)$ as E varies over a family of elliptic curves. That work was inspired by pioneering results of Fouvry and Murty [12], who proved an average value theorem for counts of supersingular primes. Unfortunately, because of the restriction that all primes counted by $M_E(N)$ lie between $(\sqrt{N}-1)^2$ and $(\sqrt{N}+1)^2$, the result of [6] is necessarily conditional upon a conjecture about the distribution of primes in short intervals (see Conjecture 1.5 below).

2010 *Mathematics Subject Classification.* Primary 11G05, Secondary 11N37, 11N60.

Key words and phrases. elliptic curves, Koblitz conjecture, mean values of arithmetic functions.

The main result of [6] introduced a strange arithmetic function, which was called $K(N)$ because it is “almost a constant”. In order to define $K(N)$, we recall the common notation $\nu_p(n)$ for the exact power of p that divides n, so that $n = \prod_p p^{\nu_p(n)}$. We also recall the Kronecker symbol $\left(\frac{a}{b}\right)$, an extension of the Jacobi symbol that is defined for all integers a and $b \neq 0$ (see, for instance, [5, Definition 1.4.8, page 28]).

Definition 1.1. For any positive integer N, we define

$$K(N) = \prod_{p\nmid N}\left(1 - \frac{\left(\frac{N-1}{p}\right)^2 p + 1}{(p-1)^2(p+1)}\right)\prod_{p\mid N}\left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right).$$

We also define $K^*(N) = K(N)N/\phi(N)$, where $\phi(N)$ is the usual Euler totient function.

As we will see later, it is actually the function $K^*(N)$ that has an interesting connection to the function $M_E(N)$. The purpose of the present work is a statistical study of the function $K^*(N)$. Our computations will illustrate a technique for dealing with arithmetic functions that have a form similar to, but are not exactly, multiplicative functions. Our first main result is the computation of the average value of K^*, first over all N and then over odd values of N.

Theorem 1.2. *For $x \geq 2$, we have*

$$\sum_{N\leq x} K^*(N) = x + O\left(\frac{x}{\log x}\right) \quad \textit{and} \quad \sum_{\substack{N\leq x\\ N \text{ odd}}} K^*(N) = \frac{x}{3} + O\left(\frac{x}{\log x}\right).$$

Thus K^* has average value 1 on all N, and average value $2/3$ on odd N.

Our second main result is the computation of the average value of K^* on primes. We employ the usual notation $\pi(x) = \#\{p \leq x \colon p \text{ is prime}\}$.

Theorem 1.3. *Fix $A > 1$. Then for $x \geq 2$,*

$$\sum_{p\leq x} K^*(p) = \tfrac{2}{3}C_2 J\,\pi(x) + O_A\left(\frac{x}{(\log x)^A}\right). \tag{2}$$

Here the constants C_2 and J are defined by

$$C_2 = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right), \tag{3}$$

and

$$J = \prod_{p>2}\left(1 + \frac{1}{(p-2)(p-1)(p+1)}\right). \tag{4}$$

Furthermore, the asymptotic formula (2) *also holds for $\sum_{p\leq x} K(p)$.*

Remark. We have written C_2 and J as two separate constants because C_2 arises naturally by itself in the analysis of the function $K(N)$ (see equation (5)).

The technique we use to establish Theorems 1.2 and 1.3, which is dictated by the unusual Definition 1.1 for $K(N)$, is of interest in its own right: the function K looks much like a multiplicative function but actually is not. One can rewrite Definition 1.1 in the following form:

$$K(N) = C_2 F(N-1)G(N) \tag{5}$$

where C_2 is the twin primes constant defined in equation (3),

$$F(n) = \prod_{\substack{p \mid n \\ p>2}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p \mid n} \left(1 - \frac{1}{(p-1)^2(p+1)}\right), \tag{6}$$

and

$$G(n) = \prod_{\substack{p \mid n \\ p>2}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p^\alpha \parallel n} \left(1 - \frac{1}{p^\alpha(p-1)}\right). \tag{7}$$

So to understand the average value of $K(N)$, we are forced to deal with the correlation between the multiplicative function F, evaluated at $N-1$, and the multiplicative function G evaluated at the neighboring integer N. It is perhaps somewhat surprising that the average values of $C_2F(N-1)G(N)$ described in Theorem 1.2 come out to simple rational numbers.

The fact that we can successfully compute average values of the function K^*, even though it is not truly multiplicative, makes it natural to wonder whether we can analyze K^* in other ways; this is indeed the case. Our next result is an analogue for $K^*(N)$ of a classical result of Schoenberg [19] for the function $n/\phi(n)$. Recall that a *distribution function* $D(u)$ is a nondecreasing, right-continuous function $D\colon \mathbb{R} \to [0,1]$ for which $\lim_{u\to-\infty} D(u) = 0$ and $\lim_{u\to\infty} D(u) = 1$.

Theorem 1.4. *The function K^* possesses a distribution function relative to the set of all natural numbers N. In other words, there exists a distribution function $D(u)$ with the property that at each of its points of continuity,*

$$D(u) = \lim_{x\to\infty} \frac{1}{x} \#\{N \le x \colon K^*(N) \le u\}.$$

As a consequence of Theorems 1.2 and 1.3, we are able to show that the main result of [6] is consistent with various unconditional results. As mentioned above, the restriction imposed by the Hasse bound creates a short-interval problem in any study of $M_E(N)$ when N is held fixed. Indeed, the interval is so short that not even the Riemann hypothesis is any help. This problem is circumvented in [6] by assuming a conjecture in the spirit of the classical Barban–Davenport–Halberstam theorem.

Conjecture 1.5. *Recall the notation $\theta(x;q,a) = \sum_{p\le x,\, p\equiv a \pmod q} \log p$. Let $0 < \eta \le 1$ and $\beta > 0$ be real numbers. Suppose that X, Y, and Q are positive real numbers satisfying $X^\eta \le Y \le X$ and $Y/(\log X)^\beta \le Q \le Y$. Then*

$$\sum_{q\le Q} \sum_{\substack{1\le a\le q \\ (a,q)=1}} \left| \theta(X+Y;q,a) - \theta(X;q,a) - \frac{Y}{\phi(q)} \right|^2 \ll_{\eta,\beta} YQ\log X.$$

Remark. We remark that Languasco, Perelli, and Zaccagnini [17] have established Conjecture 1.5 in the range $\eta > \frac{7}{12}$; they also showed, assuming the generalized Riemann hypothesis, that any $\eta > \frac{1}{2}$ is admissible.

Given integers a and b satisfying $-16(4a^3+27b^2) \ne 0$, let $E_{a,b}$ denote the elliptic curve given by the Weierstrass equation (1). Then, given positive parameters A and B, let $\mathcal{E}(A,B)$ denote the set defined by

$$\mathcal{E}(A,B) = \{E_{a,b} \colon |a| \le A,\ |b| \le B,\ -16(4a^3+27b^2) \ne 0\}$$

In [6, 7], David and the third author established the following average value theorem (in fact a stronger version of it) for $M_E(N)$ taken over the family $\mathcal{E}(A,B)$.

Proposition 1.6. *Assume the Barban–Davenport–Halberstam estimate (Conjecture 1.5) holds for some $\eta < \frac{1}{2}$. Let ε be a positive real number, and let $A > N^{1/2+\varepsilon}$ and $B > N^{1/2+\varepsilon}$ be real numbers satisfying $AB > N^{3/2+\varepsilon}$. Then for any positive real number R,*

$$\frac{1}{\#\mathcal{E}(A,B)} \sum_{E\in\mathcal{E}(A,B)} M_E(N) = \frac{K^*(N)}{\log N} + O_{\eta,\varepsilon,R}\left(\frac{1}{(\log N)^R}\right).$$

Remarks.

(1) It is not necessary to assume that Conjecture 1.5 holds for a fixed $\eta < 1/2$. It is enough to assume that it holds for $Y = \sqrt{X}/(\log X)^{\beta+2}$.

(2) The originally published formula in [6] contained an error in the definition of $K^*(N)$, which was corrected in [7] to the form given in Definition 1.1. See the end of Section 2 for further discussion of the original version of $K^*(N)$.

(3) The proof of Proposition 1.6 given in [6] is restricted to odd values of N, but further work by Chandee, Koukoulopoulos, David, and Smith [4] establishes the proposition for even values of N as well.

We note, as in [16], that computing the average value of $M_E(N)$ over the integers $N \le x$ is easily seen to be equivalent to the prime number theorem. In particular,

$$\sum_{N\le x} M_E(N) = \sum_{p\le(\sqrt{x}+1)^2} \#\{N \le x \colon \#E(\mathbb{F}_p) = N\} = \pi(x) + O\left(\sqrt{x}\right). \tag{8}$$

Similarly, the average value of $M_E(N)$ taken over the integers $N \le x$ that satisfy a congruence condition is equivalent to an appropriate application of the Chebotarev density theorem. For example, if the 2-division field of E is an S_3-extension of $\mathbb{Q}$, then the Chebotarev density theorem implies that

$$\sum_{\substack{N\le x\\ N \text{ odd}}} M_E(N) \sim \frac{1}{3}\frac{x}{\log x}.$$

(The calculation of the constant $\frac{1}{3}$ reduces to the fact that two thirds of the elements of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, which is the automorphism group of $E[2]$, have even trace.) If E is given by the Weierstrass equation (1), the 2-division field is easily seen to be the splitting field of the polynomial $X^3 + aX + b$. Since almost all cubics (when ordered by height) have S_3 as their Galois groups, it seems reasonable to conjecture that

$$\frac{1}{\#\mathcal{E}(A,B)} \sum_{\substack{N\le x\\ N \text{ odd}}} \sum_{E\in\mathcal{E}(A,B)} M_E(N) = \frac{x}{3\log x} + O\left(\frac{x}{(\log x)^2}\right), \tag{9}$$

provided that A and B are growing fast enough with respect to x. A precise version of this conjecture was established by Banks and Shparlinski [3, Theorem 19]. (In fact, their theorem shows that an analogous estimate holds with the condition "N odd" replaced by "$m \nmid N$", for any given integer m.) The asymptotic result (9), together with the result of Theorem 1.2 for odd N, shows that if we average the two sides of the equation in Proposition 1.6, we obtain consistent results (unconditionally). Similarly, the result of Theorem 1.2 for all N allows us to infer the asymptotic formula

$$\frac{1}{\#\mathcal{E}(A,B)}\sum_{N\le x}\sum_{E\in\mathcal{E}(A,B)} M_E(N) = \frac{x}{\log x} + O\biggl(\frac{x}{(\log x)^2}\biggr),$$

which is consistent with equation (8). We can therefore, if we wish, view Theorem 1.2 as additional evidence for the conclusion of Proposition 1.6.

A similar problem arises if we consider only primes p. Computing the average value of $M_E(p)$ over the primes $p \le x$ is easily seen to be equivalent to the famous Koblitz conjecture [15]:

Conjecture 1.7 (Koblitz)**.** *Given an elliptic curve E defined over the rational field $\mathbb{Q}$, there exists a constant $C(E)$ with the property that as $x \to \infty$,*

$$\sum_{\substack{p\le x\\ p\ prime}} M_E(p) \sim C(E)\frac{x}{(\log x)^2}.$$

The constant $C(E)$ appearing in Koblitz's conjecture may be zero, in which case the asymptotic is interpreted to mean that there are only finitely many primes p such that $M_E(p) > 0$. An obvious obstruction to there being infinitely many primes with $M_E(p) > 0$ is for E to be isogenous to a curve possessing nontrivial rational torsion. It was once thought that this was the only case when $C(E) = 0$, but this turned out to be false; see [23, Section 1.1] for an explicit counterexample due to Nathan Jones.

The main theorem of [2] may be reinterpreted to say that the asymptotic formula

$$\begin{aligned}\frac{1}{\#\mathcal{E}(A,B)}\sum_{\substack{p\le x\\ p\text{ prime}}}\sum_{E\in\mathcal{E}(A,B)} M_E(p) &= \tfrac{2}{3}C_2 J\int_2^x \frac{dt}{(\log t)^2} + O_A\biggl(\frac{x}{(\log x)^A}\biggr) \qquad (10)\\ &= \tfrac{2}{3}C_2 J\frac{x}{(\log x)^2} + O\biggl(\frac{x}{(\log x)^3}\biggr)\end{aligned}$$

holds unconditionally for A and B growing fast enough with respect to x. Jones [14] has averaged the explicit formula for $C(E)$ over the family $\mathcal{E}(A,B)$ and shown that the result is consistent with the above formula. We view this as providing good evidence for the Koblitz conjecture. Equation (10), together with our Theorem 1.3, shows that we obtain consistent results (unconditionally) when we average the two sides of the equation in Proposition 1.6 over the primes $N \le x$. Thus all of the conjectures and conditional theorems mentioned above reinforce one another's validity.

We note that the asymptotic formulas (9) and (10), in which we average over odd integers N or primes p up to x, both hold for a much wider range of A and B than is suggested by Proposition 1.6. In particular, Banks and Shparlinski [3] developed a character-sum argument based on a large sieve inequality to show that one may take $A, B > x^\epsilon$ and $AB > x^{1+\epsilon}$ in elliptic-curve averaging problems of this sort, when the average number of elliptic curve isomorphism classes modulo p satisfying the desired property is somewhat large. Baier [1] was able to adapt this technique to make similar improvements to the required length of the average in the (fixed trace) Lang–Trotter problem, where the average number of classes modulo p is significantly smaller. Given Baier's result, it seems possible that Proposition 1.6, in which the odd integer N is fixed, could itself be shown to hold provided that $A, B > N^\epsilon$ (note that such an improvement would still seem to require that $AB > N^{3/2+\epsilon}$ rather than the weaker condition $AB > N^{1+\epsilon}$). As we are primarily concerned with the multiplicative function K^* herein, however, we have not pursued this line of thinking.

The remainder of the article is organized as follows. We begin by establishing Theorem 1.2 in Section 2. Briefly, we approximate the function $K^*(N)$ by a similar function whose values depend only upon the small primes dividing N and $N-1$; we then calculate the average value of this truncated function by partitioning the numbers being averaged over into "configurations" based on local data about N and $N-1$ at these small primes. We prove the related Theorem 1.3 in Section 3; here the calculation of the main term is simpler since the argument of K^* is always a prime, while the estimation of the error term is more complicated due to the need to invoke results on the distribution of primes in arithmetic progressions. Finally, we establish Theorem 1.4 in Section 4 by studying the moments of K^*.

Notation. As above, we employ the Landau–Bachmann o and O notation, as well as the associated Vinogradov symbols $\ll$, $\gg$ with their usual meanings; any dependence of implied constants on other parameters is denoted with subscripts. We reserve the letters ℓ and p for prime variables. For each natural number n, we let $P(n)$ denote the largest prime factor of n, with the convention that $P(1)=1$. The natural number n is said to be *y-friable* (sometimes called *y-smooth*) if $P(n)\le y$. We write $\Psi(x,y)$ for the number of y-friable integers not exceeding x. By a *partition* of a set S, we mean any collection of disjoint sets whose union is S; we do *not* require that all of the sets in the collection be nonempty.

2. THE AVERAGE VALUE OF K^*

For notational convenience, set $R(N):=N/\phi(N)$, so that $K^*(N)=K(N)R(N)$. By definition, $K(N)$ is a product over primes, while $R(N)=\prod_{\ell\mid N}(1-1/\ell)^{-1}$ can also be viewed as such a product. Moreover, it is the small primes that have the largest influence on the magnitude of these products. This suggests it might be useful to study the truncated functions K_z and R_z defined by

$$K_z(N):=\prod_{\substack{p\nmid N\\ p\le z}}\left(1-\frac{\left(\frac{N-1}{p}\right)^2p+1}{(p-1)^2(p+1)}\right)\prod_{\substack{p\mid N\\ p\le z}}\left(1-\frac{1}{p^{\nu_p(N)}(p-1)}\right),$$

and

$$R_z(N):=\prod_{\substack{p\mid N\\ p\le z}}(1-1/p)^{-1}.$$

We give the proof of the first half of Theorem 1.2, concerning the average of $K(N)R(N)$ over all N, in complete detail. The proof of the second claim, concerning the average over odd N, can be proved in the same way; the necessary changes to the argument are indicated briefly at the end of this section.

The first half of Theorem 1.2 will be deduced from a corresponding estimate for the mean value of $K_z(N)R_z(N)$:

Proposition 2.1. *Let $x\ge 3$, and set $z:=\frac{1}{10}\log x$. We have*

$$\sum_{N\le x}K_z(N)R_z(N)=x+O(x^{3/4}).$$

We will establish this proposition at the end of this section (it follows upon combining Lemmas 2.7 and 2.8). At this point, we show how Theorem 1.2 can be deduced from the proposition.

Proof of Theorem 1.2, assuming Proposition 2.1. It suffices to show that with $z = \frac{1}{10}\log x$,

$$\sum_{\substack{N\le x\\ N \text{ odd}}} \big|K_z(N)R_z(N) - K(N)R(N)\big| \ll x/z. \tag{11}$$

Now $0 \le K(N) \le K_z(N) \le 1$ and $0 \le R_z(N) \le R(N)$, so that

$$\begin{aligned}|K_z(N)R_z(N) - K(N)R(N)| &\le |K_z(N)||R_z(N) - R(N)| + |K_z(N) - K(N)|R(N)\\ &\le (R(N) - R_z(N)) + (K_z(N) - K(N))R(N).\end{aligned}$$

Thus, it is enough to show that the sums up to x of $R(N) - R_z(N)$ and $(K_z(N) - K(N))R(N)$ are also $\ll x/z$. As we are looking only for upper bounds, we may extend these sums over all $N \le x$ and not only odd N.

Write $R(N) = \sum_{d|n} g(d)$ for an auxiliary function g. By a straightforward calculation with the Möbius inversion formula, we see that g vanishes except at squarefree integers d, in which case $g(d) = 1/\phi(d)$. Hence, for all real $t > 0$,

$$\begin{aligned}\sum_{N\le t} R(N) = \sum_{N\le t}\sum_{d|N} g(d) &= \sum_{d\le t}\frac{1}{\phi(d)}\sum_{\substack{N\le t\\ d|N}} 1\\ &\le \sum_{d\le t}\frac{t}{d\phi(d)}\\ &\le t\sum_{d=1}^{\infty}\frac{1}{d\phi(d)}\\ &= t\prod_p\left(1 + \frac{1}{p(p-1)} + \frac{1}{p^3(p-1)} + \dots\right) \ll t,\end{aligned} \tag{12}$$

so that $R(N)$ is bounded on average. Now writing $R_z(N) = \sum_{d|n} g_z(d)$ for an auxiliary function $g_z(d)$, one finds that g_z vanishes except on squarefree z-friable integers d, in which case again $g_z(d) = 1/\phi(d)$. In particular, $g(d) - g_z(d)$ is nonnegative for all d, and $g(d) - g_z(d) = 0$ when $d \le z$. We deduce that

$$\begin{aligned}\sum_{N\le x}(R(N) - R_z(N)) = \sum_{N\le x}\sum_{d|N}(g(d) - g_z(d)) &\le \sum_{N\le x}\sum_{\substack{d|N\\ d>z}}\frac{1}{\phi(d)}\\ &= \sum_{z<d\le x}\sum_{\substack{N\le x\\ d|N}}\frac{1}{\phi(d)} \le \sum_{d>z}\frac{x}{d\phi(d)}.\end{aligned}$$

Partitioning this last sum into dyadic intervals, we have

$$\begin{aligned}\sum_{N\le x}(R(N)-R_z(N)) \le \sum_{k=1}^{\infty}\sum_{2^{k-1}z<d\le 2^k z}\frac{x}{d\phi(d)} &= x\sum_{k=1}^{\infty}\sum_{2^{k-1}z<d\le 2^k z}\frac{R(d)}{d^2}\\ &\le x\sum_{k=1}^{\infty}\frac{1}{(2^{k-1}z)^2}\sum_{d\le 2^k z}R(d)\\ &\ll x\sum_{k=1}^{\infty}\frac{1}{(2^{k-1}z)^2}2^k z\\ &\ll \frac{x}{z}\sum_{k=1}^{\infty}\frac{1}{2^k}\ll\frac{x}{z},\end{aligned}$$

where we used the estimate (12) in the second-to-last inequality. This proves the desired upper bound for the partial sums of $R(N)-R_z(N)$.

The partial sums of $(K_z(N)-K(N))R(N)$ are easier. Since each factor appearing in the products defining K_z and K has the form $1-O(1/\ell^2)$, it follows that $K(N)/K_z(N)\ge 1-O\left(\sum_{\ell>z}1/\ell^2\right)\ge 1-O(1/z)$. Thus, $K_z(N)-K(N)=K_z(N)(1-K(N)/K_z(N))\le 1-K(N)/K_z(N)\ll 1/z$. It follows that

$$\sum_{N\le x}(K_z(N)-K(N))R(N)\ll\frac{1}{z}\sum_{N\le x}R(N)\ll\frac{x}{z},$$

using the estimate (12) once more in the last step. This completes the proof of Theorem 1.2, assuming Proposition 2.1. □

In the remainder of this section, we concentrate on proving Proposition 2.1. Our strategy, already alluded to in the introduction, is to partition the integers $N\le x$ according to local data at small primes. We choose the partition so that the values $K_z(N)$ and $R_z(N)$ are constant along each set belonging to the partition (which we call a *configuration*). For the remainder of this section, we continue to assume that $x\ge 3$ and that $z=\frac{1}{10}\log x$.

Definition 2.2. We define the *configuration space* $\mathscr{S}$ as the set of all 4-tuples of the form

$$(\mathcal{A},\mathcal{B},\mathcal{C},\{e_\ell\}_{\ell\in\mathcal{B}}),$$

where the sets $\mathcal{A},\mathcal{B},\mathcal{C}$ partition the set of primes up to z, and the e_ℓ are positive integers. (Although $\mathscr{S}$ depends upon z and hence x, we will not include this dependence in the notation.)

To each $N\le x$, we can associate a unique configuration in the following manner.

Definition 2.3. Given $N\le x$, define three subsets of the primes in $[2,z]$ by setting $\mathcal{A}:=\{\ell\le z:\ell\nmid N(N-1)\}$, $\mathcal{B}:=\{\ell\le z:\ell\mid N\}$, and $\mathcal{C}:=\{\ell\le z:\ell\mid N-1\}$. For each $\ell\in\mathcal{B}$, set $e_\ell:=\nu_\ell(N)$. Then $\sigma=(\mathcal{A},\mathcal{B},\mathcal{C},\{e_\ell\}_{\ell\in\mathcal{B}})\in\mathscr{S}$ is called the *configuration* σ corresponding to N and is denoted σ_N.

Remark. One checks easily that the value $K_z(N)R_z(N)$ depends only on $\sigma=\sigma_N$. Thus, we often abuse notation by referring to $K_z(\sigma)$ and $R_z(\sigma)$ instead of $K_z(N)$ and $R_z(N)$.

We can rewrite the sum considered in Proposition 2.1 in the form

$$\sum_{N\le x} K_z(N)R_z(N) = \sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1. \tag{13}$$

In the next lemma, we estimate the inner sum on the right-hand side of (13) in two ways.

Lemma 2.4. *For each $\sigma\in\mathscr{S}$, we have*

$$\sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 = d_\sigma x + O(x^{1/5}), \tag{14}$$

where

$$d_\sigma := \Big(\prod_{\ell\in\mathcal{A}}(1-2/\ell)\Big)\Big(\prod_{\ell\in\mathcal{B}}\frac{1}{\ell^{e_\ell}}(1-1/\ell)\Big)\Big(\prod_{\ell\in\mathcal{C}}\frac{1}{\ell}\Big). \tag{15}$$

We also have the crude upper bound

$$\sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 \le x\prod_{\ell\in\mathcal{B}}\ell^{-e_\ell} \tag{16}$$

for any $\sigma\in\mathscr{S}$.

Proof. The condition that $\sigma_N=\sigma$ is equivalent to a congruence condition on N modulo

$$m_\sigma := \left(\prod_{\ell\in\mathcal{A}\cup\mathcal{C}}\ell\right)\left(\prod_{\ell\in\mathcal{B}}\ell^{e_\ell+1}\right). \tag{17}$$

Indeed, $\sigma_N=\sigma$ precisely when N belongs to a union of $\prod_{\ell\in\mathcal{A}}(\ell-2)\prod_{\ell\in\mathcal{B}}(\ell-1)$ congruence classes modulo m_σ. This implies that

$$\sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 = \frac{x}{m_\sigma}\prod_{\ell\in\mathcal{A}}(\ell-2)\prod_{\ell\in\mathcal{B}}(\ell-1) + O\Big(\prod_{\ell\in\mathcal{A}\cup\mathcal{B}}\ell\Big) = d_\sigma x + O\Big(\prod_{\ell\le z}\ell\Big).$$

By our choice of z and the prime number theorem, $\prod_{\ell\le z}\ell < x^{1/5}$ for large x, and so we have established the formula (14). To justify the inequality (16), it suffices to observe that if $\sigma_N=\sigma$, then $\prod_{\ell\in\mathcal{B}}\ell^{e_\ell}$ divides N. □

The modulus m_σ, defined in (17), will continue to play a key role in subsequent arguments. It will be convenient to know that m_σ nearly determines σ; this is the substance of our next result.

Lemma 2.5. *For each natural number m, the number of $\sigma\in\mathscr{S}$ with $m_\sigma=m$ is $O(x^{1/4})$.*

Proof. Suppose that $m_\sigma=m$, where $\sigma=(\mathcal{A},\mathcal{B},\mathcal{C},\{e_\ell\}_{\ell\in\mathcal{B}})$. Since the sets $\mathcal{A},\mathcal{B},\mathcal{C}$ partition the primes up to z, the number of possibilities for these sets is $3^{\pi(z)}=\exp(O(\log x/\log\log x))=x^{o(1)}$. Having chosen these sets, the exponents e_ℓ, for $\ell\in\mathcal{B}$, are determined by the prime factorization of m. This proves the lemma with $\frac{1}{4}$ replaced by any positive ϵ. □

We next investigate two sums over m_σ for future use in estimating error terms.

Lemma 2.6. *For each $\sigma\in\mathscr{S}$, define m_σ by* (17)*. Then for all $x\ge3$,*

$$x^{6/5}\log\log x\sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma>x}}\frac{1}{m_\sigma} + x^{1/5}\log\log x\sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}}1 \ll x^{3/4}. \tag{18}$$

Proof. We proceed by Rankin's method:

$$\begin{aligned}
x^{6/5}\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma>x}} \frac{1}{m_\sigma} &+ x^{1/5}\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} 1 \\
&\le x^{6/5}\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma>x}} \left(\frac{m_\sigma}{x}\right)^{7/8}\frac{1}{m_\sigma} + x^{1/5}\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} \left(\frac{x}{m_\sigma}\right)^{1/8} \\
&= x^{13/40}\log\log x \sum_{\sigma\in\mathscr{S}} \frac{1}{m_\sigma^{1/8}}.
\end{aligned}$$

Every value of m_σ is z-friable, and there are at most $x^{1/4}$ configurations $\sigma\in\mathscr{S}$ for every possible value of m_σ by Lemma 2.5. Therefore

$$\begin{aligned}
x^{13/40}\log\log x \sum_{\sigma\in\mathscr{S}} \frac{1}{m_\sigma^{1/8}} &\ll x^{13/40}\log\log x\cdot x^{1/4} \sum_{m\ z\text{-friable}} \frac{1}{m^{1/8}} \\
&= x^{23/40}\log\log x \prod_{p\le z}\left(1+\frac{1}{p^{1/8}}+\frac{1}{p^{1/4}}+\cdots\right) \\
&= x^{23/40}\log\log x \prod_{p\le z}\left(1-\frac{1}{p^{1/8}}\right)^{-1}.
\end{aligned}$$

Each factor in the product is at most $(1-2^{-1/8})^{-1} < 13$, and so the product is less than $13^{\pi(z)} = 13^{O(\log x/\log\log x)} = x^{o(1)}$. Thus the left-hand side of equation (18) is $\ll x^{23/40+o(1)}\log\log x \ll x^{3/4}$ as claimed. □

The next lemma relates the mean value of $K_z(N)R_z(N)$, taken over odd N, to the sum of $K_z(\sigma)R_z(\sigma)d_\sigma$, taken over all configurations σ.

Lemma 2.7. *For all $x\ge 3$,*

$$\sum_{N\le x} K_z(N)R_z(N) = x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma + O(x^{3/4}).$$

Proof. We begin by noting that the upper bounds

$$0\le K(N)\le K_z(N)\le 1 \quad\text{and}\quad 0\le R_z(N)\le R(N)\le \prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} \ll \log\log x \tag{19}$$

are valid for all $N\le x$. We write

$$\begin{aligned}
\sum_{N\le x} K_z(N)R_z(N) &= \sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 \\
&= \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 + \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma>x}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 \\
&= \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} K_z(\sigma)R_z(\sigma)(d_\sigma x + O(x^{1/5})) + O\Bigg(\sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma>x}} K_z(\sigma)R_z(\sigma)x\prod_{\ell\in\mathcal{B}}\ell^{-e_\ell}\Bigg)
\end{aligned}$$

by Lemma 2.4. Using the upper bounds (19) for K_z and R_z, we deduce after extending the first sum to infinity that

$$\sum_{N\le x} K_z(N)R_z(N) = x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma + O\Bigg(x\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma>x}} d_\sigma\Bigg)$$
$$+ O\Bigg(x^{1/5}\log\log x\sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} 1 + x\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma>x}}\prod_{\ell\in\mathcal{B}}\ell^{-e_\ell}\Bigg);$$

since the inequality $d_\sigma \le \prod_{\ell\in\mathcal{B}}\ell^{-e_\ell}$ follows from the definition (15), the first error term is dominated by the second. Because $\prod_{\ell\in\mathcal{B}}\ell^{-e_\ell} = m_\sigma^{-1}\prod_{\ell\le z}\ell < m_\sigma^{-1}x^{1/5}$ once x is large, this error term is $\ll x^{3/4}$ by Lemma 2.6, and the proof is complete. □

In view of Lemma 2.7, Proposition 2.1 is a consequence of the following remarkable identity:

Lemma 2.8. *We have*

$$\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma = 1.$$

Proof. Referring back to the definitions of K_z and R_z, we see that for $\sigma\in\mathscr{S}$,

$$K_z(\sigma)R_z(\sigma) = \left(\prod_{\ell\in\mathcal{A}}\left(1-\frac{1}{(\ell-1)^2}\right)\right)\left(\prod_{\ell\in\mathcal{B}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right)\left(1-\frac{1}{\ell}\right)^{-1}\right)\times$$
$$\left(\prod_{\ell\in\mathcal{C}}\left(1-\frac{1}{(\ell-1)^2(\ell+1)}\right)\right). \quad (20)$$

Multiplying by the expression (15) for d_σ, we find that

$$K_z(\sigma)R_z(\sigma)d_\sigma = \left(\prod_{\ell\in\mathcal{A}}\frac{\ell-2}{\ell-1}\right)^2\left(\prod_{\ell\in\mathcal{B}}\frac{1}{\ell^{e_\ell}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right)\right)\left(\prod_{\ell\in\mathcal{C}}\frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}\right). \quad (21)$$

Recall that σ is a 4-tuple with entries $\mathcal{A},\mathcal{B},\mathcal{C}$, and $\{e_\ell\}_{\ell\in\mathcal{B}}$. We sum the expression (21) over the possibilities for $\{e_\ell\}$. We have

$$\sum_{\substack{\{e_\ell\}\\ \text{each } e_\ell\ge1}}\left(\prod_{\ell\in\mathcal{B}}\frac{1}{\ell^{e_\ell}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right)\right) = \prod_{\ell\in\mathcal{B}}\left(\sum_{e_\ell=1}^{\infty}\frac{1}{\ell^{e_\ell}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right)\right).$$

By a short computation,

$$\sum_{e_\ell=1}^{\infty}\frac{1}{\ell^{e_\ell}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right) = \frac{\ell^2-2}{(\ell+1)(\ell-1)^2}.$$

Thus, if we now fix only $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ and sum over all corresponding configurations σ, we have

$$\sum_{\substack{\sigma\in\mathscr{S}\\ \mathcal{A},\mathcal{B},\mathcal{C}\text{ fixed}}} K_z(\sigma)R_z(\sigma)d_\sigma = \biggl(\prod_{\ell\in\mathcal{A}}\frac{\ell-2}{\ell-1}\biggr)^2\biggl(\prod_{\ell\in\mathcal{B}}\frac{\ell^2-2}{(\ell+1)(\ell-1)^2}\biggr)\biggl(\prod_{\ell\in\mathcal{C}}\frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}\biggr)$$
$$= \biggl(\prod_{\ell\in\mathcal{A}}P_{\mathcal{A}}(\ell)\biggr)\biggl(\prod_{\ell\in\mathcal{B}}P_{\mathcal{B}}(\ell)\biggr)\biggl(\prod_{\ell\in\mathcal{C}}P_{\mathcal{C}}(\ell)\biggr), \qquad (22)$$

where for notational convenience we have defined

$$P_{\mathcal{A}}(\ell) = \biggl(\frac{\ell-2}{\ell-1}\biggr)^2, \quad P_{\mathcal{B}}(\ell) = \frac{\ell^2-2}{(\ell+1)(\ell-1)^2}, \quad P_{\mathcal{C}}(\ell) = \frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}. \qquad (23)$$

To finish the proof, we sum the right-hand side of equation (22) over all possibilities for $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$. The only condition on the sets $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ is that they partition the set of primes not exceeding z. Hence,

$$\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma = \sum_{\substack{\mathcal{A},\mathcal{B},\mathcal{C}\text{ disjoint}\\ \mathcal{A}\cup\mathcal{B}\cup\mathcal{C}=\{\ell\le z\}}} \biggl(\prod_{\ell\in\mathcal{A}}P_{\mathcal{A}}(\ell)\biggr)\biggl(\prod_{\ell\in\mathcal{B}}P_{\mathcal{B}}(\ell)\biggr)\biggl(\prod_{\ell\in\mathcal{C}}P_{\mathcal{C}}(\ell)\biggr)$$
$$= \prod_{\ell\le z}\bigl(P_{\mathcal{A}}(\ell)+P_{\mathcal{B}}(\ell)+P_{\mathcal{C}}(\ell)\bigr).$$

However, $P_{\mathcal{A}}(\ell)+P_{\mathcal{B}}(\ell)+P_{\mathcal{C}}(\ell)=1$, identically! This completes the proof of the lemma, and so also of Proposition 2.1. □

As already remarked above, the first half of Theorem 1.2 follows immediately upon combining Lemmas 2.7 and 2.8.

Proof of the second half of Theorem 1.2. The condition that N is odd amounts to the requirement that $2\in\mathcal{C}$ in the configuration notation of this section. If we carry this requirement through the proofs of Lemmas 2.7 and 2.8, the bulk of the argument is essentially unchanged, but the new conclusions are that

$$\sum_{\substack{N\le x\\ 2\nmid N}} K_z(N)R_z(N) = x\sum_{\substack{\sigma\in\mathscr{S}\\ 2\in\mathcal{C}}} K_z(\sigma)R_z(\sigma)d_\sigma + O(x^{3/4})$$

and

$$\sum_{\substack{\sigma\in\mathscr{S}\\ 2\in\mathcal{C}}} K_z(\sigma)R_z(\sigma)d_\sigma = \sum_{\substack{\mathcal{A},\mathcal{B},\mathcal{C}\text{ disjoint}\\ \mathcal{A}\cup\mathcal{B}\cup\mathcal{C}=\{\ell\le z\}\\ 2\in\mathcal{C}}} \biggl(\prod_{\ell\in\mathcal{A}}P_{\mathcal{A}}(\ell)\biggr)\biggl(\prod_{\ell\in\mathcal{B}}P_{\mathcal{B}}(\ell)\biggr)\biggl(\prod_{\ell\in\mathcal{C}}P_{\mathcal{C}}(\ell)\biggr)$$
$$= P_C(2)\prod_{2<\ell\le z}\bigl(P_{\mathcal{A}}(\ell)+P_{\mathcal{B}}(\ell)+P_{\mathcal{C}}(\ell)\bigr) = P_C(2).$$

(We assume in going from the first line to the second that $z\ge 2$, i.e., that $x\ge e^{20}$.) Since $P_C(2)=\frac{1}{3}$, the second half of Theorem 1.2 follows. □

Most mathematical coincidences have explanations, of course, and the magical-seeming $P_{\mathcal{A}}(\ell)+P_{\mathcal{B}}(\ell)+P_{\mathcal{C}}(\ell)=1$ is no different. One might guess that $P_{\mathcal{A}}(\ell)$, $P_{\mathcal{B}}(\ell)$, and $P_{\mathcal{C}}(\ell)$ are probabilities of certain events occurring, and this is exactly right: as γ ranges over all elements of $\mathrm{GL}_2(\mathbb{F}_\ell)$, the expression $\det(\gamma) + 1 - \operatorname{tr}(\gamma)$ is congruent to 0 (mod ℓ) with probability $P_{\mathcal{B}}(\ell)$, congruent to 1 (mod ℓ) with probability $P_{\mathcal{C}}(\ell)$, and congruent to each of the $\ell - 2$ other residue classes with probability $P_{\mathcal{A}}(\ell)/(\ell-2)$. (See [8, equation (2.2)] for this computation, as well as for the precise connection to elliptic curves.)

We conclude this section by saying a few words about the function that was originally published in [6], which we will here call K° to avoid confusion with the corrected function K^*:

$$K^\circ(N) =$$
$$\frac{N}{\phi(N)} \prod_{p\nmid N} \left(1 - \frac{\left(\frac{N-1}{p}\right)^2 p + 1}{(p-1)^2(p+1)}\right) \prod_{\substack{p\mid N \\ 2\nmid \nu_p(N)}} \left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right) \prod_{\substack{p\mid N \\ 2\mid \nu_p(N)}} \left(1 - \frac{p - \left(\frac{-N_p}{p}\right)}{p^{\nu_p(N)+1}(p-1)}\right),$$

where $N_p = N/p^{\nu_p(N)}$ is the p-free part of N. This function is even further from being a multiplicative function than K^*, since its value can depend even on the residue class modulo p of the p-free part of N. Nevertheless, our techniques can in fact determine the average value of the function K° as well.

To investigate the average of K°, we would expand the notion of a configuration to a sextuple $(\mathcal{A}, \mathcal{B}_1, \mathcal{B}_2, \mathcal{C}, \{e_\ell\}_{\ell\in\mathcal{B}_1\cup\mathcal{B}_2}, \{a_\ell\}_{\ell\in\mathcal{B}_2})$, where $\mathcal{A}, \mathcal{B}_1, \mathcal{B}_2, \mathcal{C}$ partition the set of primes up to z, the e_ℓ are positive integers, and the a_ℓ are integers satisfying $1 \le a_\ell \le \ell - 1$. We would modify Definition 2.3 by setting $\mathcal{B}_1 := \{\ell \le z : 2 \nmid e_\ell\}$ and $\mathcal{B}_2 := \{\ell \le z : 2 \mid e_\ell\}$ and, for $\ell \in \mathcal{B}_2$, choosing $a_\ell \in \{1, \dots, \ell-1\}$ so that $a_\ell \equiv N/\ell^{e_\ell} \pmod{\ell}$. The analogue of equation (21) would be

$$K_z^\circ(\sigma) d_\sigma = \left(\prod_{\ell\in\mathcal{A}} \frac{\ell-2}{\ell-1}\right)^2 \left(\prod_{\ell\in\mathcal{C}} \frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}\right) \times$$
$$\left(\prod_{\ell\in\mathcal{B}_1} \frac{1}{\ell^{e_\ell}} \left(1 - \frac{1}{\ell^{e_\ell}(\ell-1)}\right)\right) \left(\prod_{\ell\in\mathcal{B}_2} \frac{1}{\ell^{e_\ell}(\ell-1)} \left(1 - \frac{\ell - \left(\frac{-a_\ell}{\ell}\right)}{\ell^{e_\ell+1}(\ell-1)}\right)\right).$$

We would then hold $\mathcal{A}, \mathcal{B}_1, \mathcal{B}_2, \mathcal{C}$, and the e_ℓ fixed and sum over all $\prod_{\ell\in\mathcal{B}_2}(\ell-1)$ possibilities for the a_ℓ; this has the effect of replacing the Legendre symbol $\left(\frac{-a_\ell}{\ell}\right)$ by its average value 0. At this point in the argument, the factors corresponding to primes in $\mathcal{B}_1$ and $\mathcal{B}_2$ would be identical, and the calculation would soon dovetail with equation (22).

We felt these few details of the determination of the average value of K° were worth mentioning, as an example of the wider applicability of our method and the more complicated configuration spaces that can be used.

3. The average of K^* over primes

In this section we establish Theorem 1.3. The main component of the proof is the following asymptotic formula for the sum of the multiplicative function F evaluated on shifted primes.

Proposition 3.1. *Let F be the multiplicative function defined in equation* (6)*, and let J be the constant defined in equation* (4)*. For any $x > 2$ and for any positive real number A,*

$$\sum_{p\le x} F(p-1) = J\pi(x) + O_A(x/(\log x)^A).$$

Proof. Write $F(n) = \sum_{d|n} g(d)$ for an auxiliary function g (not the same function as in the proof of Theorem 1.2), which is also multiplicative. By a direct computation with the Möbius inversion formula, g vanishes unless d is squarefree. Moreover, $g(2) = -\frac{1}{3}$, while for odd primes ℓ,

$$g(\ell) = \frac{1}{(\ell-2)(\ell+1)}. \tag{24}$$

Writing $\pi(x; d, 1)$ for the number of primes $p \le x$ with $p \equiv 1 \pmod{d}$, we have

$$\begin{aligned} \sum_{p\le x} F(p-1) &= \sum_{p\le x} \sum_{d|p-1} g(d) \\ &= \sum_{d\le(\log x)^A} g(d)\pi(x; d, 1) + \sum_{(\log x)^A < d \le x} g(d)\pi(x; d, 1). \end{aligned} \tag{25}$$

We first consider the second sum on the right-hand side. Trivially, $\pi(x; d, 1) < x/d$, and so

$$\left| \sum_{(\log x)^A < d\le x} g(d)\pi(x; d, 1) \right| \le x \sum_{d > (\log x)^A} \frac{|g(d)|}{d}. \tag{26}$$

When $g(d)$ is nonvanishing, the formula (24) yields

$$d^2 g(d) \ll \prod_{\ell | d,\ \ell>2} \frac{\ell^2}{\ell^2-\ell-2} \ll \prod_{\ell|d} \left(1 - \frac{1}{\ell}\right)^{-1} = \frac{d}{\phi(d)},$$

and hence $g(d) \ll 1/d\phi(d)$ for all values of d. In particular, using the crude lower bound $\phi(d) \gg d^{1/2}$ (compare with the precise [18, Theorem 2.9, page 55]), we find that $g(d) \ll d^{-3/2}$. Thus, equation (26) gives

$$\sum_{(\log x)^A < d\le x} g(d)\pi(x; d, 1) \ll x \sum_{d>(\log x)^A} d^{-5/2} \ll x(\log x)^{-3A/2},$$

and so equation (25) becomes

$$\sum_{p\le x} F(p-1) = \sum_{d\le(\log x)^A} g(d)\pi(x; d, 1) + O\big(x(\log x)^{-3A/2}\big). \tag{27}$$

To deal with the remaining sum, we invoke the Siegel–Walfisz theorem [18, Corollary 11.21, page 381]. That theorem implies that for a certain absolute constant $c > 0$,

$$\begin{aligned} \sum_{d\le(\log x)^A} g(d)\pi(x; d, 1) &= \sum_{d\le(\log x)^A} g(d)\left(\frac{\pi(x)}{\phi(d)} + O_A\big(x\exp(-c\sqrt{\log x})\big)\right) \\ &= \pi(x) \sum_{d\le(\log x)^A} \frac{g(d)}{\phi(d)} + O_A\left(x\exp(-c\sqrt{\log x}) \sum_{d=1}^{\infty} |g(d)|\right) \\ &= \pi(x) \sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)} \\ &\qquad + O_A\left(\pi(x) \sum_{d>(\log x)^A} \frac{|g(d)|}{\phi(d)} + x\exp(-c\sqrt{\log x}) \sum_{d=1}^{\infty} |g(d)|\right). \end{aligned}$$

In the error term, we again use the crude bounds $g(d) \ll d^{-3/2}$ and $\phi(d) \gg d^{1/2}$, obtaining

$$\sum_{d \le (\log x)^A} g(d)\pi(x;d,1) = \pi(x) \sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)} + O_A\big(\pi(x)(\log x)^{-A} + x\exp(-c\sqrt{\log x}) \cdot 1\big),$$

whereupon equation (27) becomes

$$\sum_{p \le x} F(p-1) = \pi(x) \sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)} + O_A\big(x(\log x)^{-A}\big).$$

Finally, the constant in this main term is an absolutely convergent sum of a multiplicative function, and hence it can be expressed as the Euler product

$$\begin{aligned}\sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)} &= \prod_{\ell} \left(1 + \frac{g(p)}{\phi(p)} + \frac{g(p^2)}{\phi(p^2)} + \cdots\right) \\ &= \frac{2}{3} \prod_{\ell > 2} \left(1 + \frac{1}{(\ell-1)(\ell-2)(\ell+1)}\right) = \frac{2}{3}J,\end{aligned}$$

by equation (24). This completes the proof of the proposition. □

Proof of Theorem 1.3. We first claim that the asymptotic formula (2) for K^* follows easily from the same asymptotic formula for K. Indeed, for each prime p, we have $K^*(p) = K(p)p/(p-1) = K(p) + O(K(p)/p)$. Because each local factor in Definition 1.1 is of the form $1 + O(p^{-2})$, we see that K is absolutely bounded. Thus

$$\sum_{p \le x} K^*(p) = \sum_{p \le x} K(p) + O\bigg(\sum_{p \le x} \frac{1}{p}\bigg) = \sum_{p \le x} K(p) + O(\log\log x),$$

and so it suffices to establish the asymptotic formula (2) for K.

For each odd prime p, the decomposition (5) gives $K(p) = C_2 F(p-1)G(p)$, where F and G are defined in equations (6) and (7), respectively. Again, all local factors in these definitions are of the form $1 + O(p^{-2})$; hence $G(p) = 1 + O(1/p^2)$ and F is absolutely bounded. Therefore,

$$\begin{aligned}\sum_{p \le x} K(p) &= \sum_{p \le x} C_2 F(p-1)G(p) \\ &= C_2 \sum_{p \le x} F(p-1) + O\bigg(1 + \sum_{p \le x} \frac{F(p-1)}{p^2}\bigg) \\ &= C_2 \sum_{p \le x} F(p-1) + O(1),\end{aligned}$$

and so the desired asymptotic formula (2) is a direct consequence of Proposition 3.1. □

4. The distribution function of K^*

The goal of this section is to establish the existence of the distribution function of $K^*(N)$. We do so by bounding the moments of $K^*(N)$:

$$\mu_k := \lim_{x \to \infty} \frac{1}{x} \sum_{N \le x} K^*(N)^k. \tag{28}$$

We describe below how Theorem 1.4 follows from Proposition 4.3. Before we can bound these moments, however, we must prove that the moments even exist. In Theorem 1.2 we determined that $\mu_1 = 1$, and the same method of determining μ_k applies in general.

Proposition 4.1. *For every natural number k, the limit* (28) *defining μ_k exists.*

Proof. Following the proof of Proposition 2.1, we obtain (with minimal changes to the argument) that for each fixed k,

$$\sum_{N\le x}(K_z(N)R_z(N))^k = x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)^k R_z(\sigma)^k d_\sigma + O_k(x^{3/4}), \tag{29}$$

where $z = \frac{1}{10}\log x$ and d_σ is defined in equation (15). Note that for $N \le x$,

$$\begin{aligned}\big(K_z(N)R_z(N)\big)^k &- \big(K(N)R(N)\big)^k \\ &\ll_k \max\big\{K(N)R(N), K_z(N)R_z(N)\big\}^{k-1}\cdot\big|K(N)R(N) - K_z(N)R_z(N)\big| \\ &\ll_k (\log\log x)^{k-1}\cdot\big|K(N)R(N) - K_z(N)R_z(N)\big|\end{aligned}$$

by the bounds in equation (19); therefore

$$\begin{aligned}\sum_{N\le x} K^*(N)^k &= \sum_{N\le x}(K_z(N)R_z(N))^k + \Bigg(\sum_{N\le x}\big((K(N)R(N))^k - (K_z(N)R_z(N))^k\big)\Bigg) \\ &= \sum_{N\le x}(K_z(N)R_z(N))^k + O_k\Bigg((\log\log x)^{k-1}\sum_{N\le x}\big|K(N)R(N) - K_z(N)R_z(N)\big|\Bigg).\end{aligned}$$

Using equation (29) in the main term and the estimate (11) in the error term, we obtain

$$\begin{aligned}\sum_{N\le x} K^*(N)^k &= x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)^k R_z(\sigma)^k d_\sigma + O_k(x^{3/4} + (\log\log x)^{k-1}x/z) \\ &= x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)^k R_z(\sigma)^k d_\sigma + O_k\bigg(\frac{x}{\log x}(\log\log x)^{k-1}\bigg).\end{aligned}$$

Dividing both sides by x and passing to the limit, we deduce that

$$\mu_k = \lim_{x\to\infty}\sum_{\sigma\in\mathscr{S}} K_z(\sigma)^k R_z(\sigma)^k d_\sigma, \tag{30}$$

provided that this limit exists.

To compute the sum over σ in (30), we follow the proof of Lemma 2.8; however, the details are somewhat messier. With the four components $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\{e_\ell\}_{\ell\in\mathcal{B}}$ of σ as before, we write down the expansion for $K_z(\sigma)^k R_z(\sigma)^k d_\sigma$ analogous to (21). This expansion is made up of three pieces, which are products over primes ℓ in $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$. The $\mathcal{B}$ product depends additionally on the tuple $\{e_\ell\}_{\ell\in\mathcal{B}}$. We sum over all possibilities for $\{e_\ell\}_{\ell\in\mathcal{B}}$ to remove this dependence. After straightforward but uninspiring computations, we find that fixing only $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$,

$$\sum_\sigma K_z(\sigma)^k R_z(\sigma)^k d_\sigma = \Bigg(\prod_{\ell\in\mathcal{A}} P_{\mathcal{A}}(\ell)\Bigg)\Bigg(\prod_{\ell\in\mathcal{B}} P_{\mathcal{B}}(\ell)\Bigg)\Bigg(\prod_{\ell\in\mathcal{C}} P_{\mathcal{C}}(\ell)\Bigg),$$

where (we suppress the dependence on k in the notation on the left-hand sides)

$$\begin{aligned}
P_{\mathcal{A}}(\ell) &= (1-\tfrac{2}{\ell})^{k+1}(1-\tfrac{1}{\ell})^{-2k}, \\
P_{\mathcal{B}}(\ell) &= \left(1-\frac{1}{\ell}\right)^{1-k}\sum_{d=1}^{\infty}\frac{1}{\ell^d}\left(1-\frac{1}{\ell^d(\ell-1)}\right)^k, \qquad (31)\\
P_{\mathcal{C}}(\ell) &= \frac{1}{\ell}\left(1-\frac{1}{(\ell-1)^2(\ell+1)}\right)^k.
\end{aligned}$$

(Note that when $k=1$, these expressions reduce to the expressions in equation (23).) To compute the sum appearing in (30), we sum over $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$, keeping in mind that these sets partition the primes in $[2,z]$. We find that

$$\sum_{\sigma\in\mathscr{S}} K_z(\sigma)^k R_z(\sigma)^k d_\sigma = \prod_{\ell\le z}\left(P_{\mathcal{A}}(\ell)+P_{\mathcal{B}}(\ell)+P_{\mathcal{C}}(\ell)\right),$$

and so from equation (30),

$$\mu_k = \prod_{\ell}\left(P_{\mathcal{A}}(\ell)+P_{\mathcal{B}}(\ell)+P_{\mathcal{C}}(\ell)\right). \qquad (32)$$

It remains to show that this product converges. From their definitions (31), we find that

$$\begin{aligned}
P_{\mathcal{A}}(\ell) &= 1-2/\ell+O_k(1/\ell^2),\\
P_{\mathcal{B}}(\ell) &= 1/\ell+O_k(1/\ell^2),\\
P_{\mathcal{C}}(\ell) &= 1/\ell+O_k(1/\ell^2).
\end{aligned}$$

It follows that each term in the product from equation (32) is $1+O(1/\ell^2)$; consequently, that product converges, which completes the proof of the proposition. □

Remarks. For any given k, we can explicitly compute $P_{\mathcal{A}}$, $P_{\mathcal{B}}$, and $P_{\mathcal{C}}$ and thus write down an exact expression for μ_k as an infinite product over primes. For example, taking $k=2$, we find that

$$\mu_2 = \prod_{\ell}\left(1+\frac{\ell^5-\ell^3-2\ell^2-2\ell-1}{(\ell-1)^4(\ell+1)^2(\ell^2+\ell+1)}\right)\approx 1.261605.$$

Now that we know these moments μ_k exist, we proceed to establish an upper bound for them as a function of k. The following result, well known in the theory of probability (see, for example, [9, Theorem 3.3.12, page 123]), allows us to pass from such an upper bound to the existence of a limiting distribution function.

Lemma 4.2. *Let $F_1, F_2, \ldots$ be a sequence of distribution functions. Suppose that for each positive integer k, the limit $\lim_{n\to\infty}\int u^k\,dF_n(u)=\mu_k$ exists. If*

$$\limsup_{k\to\infty}\frac{\mu_{2k}^{1/2k}}{2k}<\infty,$$

then there is a unique distribution function F possessing the μ_k as its moments, and F_n converges weakly to F.

We will apply Lemma 4.2 with

$$F_n(u) := \frac{\#\{m\le n\colon K^*(m)\le u\}}{\#\{m\le n\}},$$

for which

$$\lim_{n\to\infty}\int u^k\,dF_n(u)=\lim_{n\to\infty}\frac{1}{n}\sum_{m\le n}K^*(m)^k=\mu_k$$

(so that the uses of μ_k in equation (28) and Lemma 4.2 are consistent). In light of Lemma 4.2, Theorem 1.4 is a consequence of the following upper bound.

Proposition 4.3. *The moments μ_k defined in equation* (28) *satisfy* $\log\mu_k\ll k\log\log k$. *In particular,* $(\mu_{2k}^{1/2k})/2k\ll(\log k)^A/k$ *for some constant A.*

Proof. Recall that $R(N)$ denotes the function $N/\phi(N)$. The number μ_k is the kth moment of the function $K(N)R(N)$, and that function is bounded pointwise by $R(N)$. So μ_k is bounded above by μ'_k, where

$$\mu'_k:=\lim_{x\to\infty}\frac{1}{x}\sum_{N\le x}R(N)^k.$$

Thus, it suffices to establish the estimate $\log\mu'_k\ll k\log\log k$.

By a result known already to Schur (see [19, page 194]; see also [18, Exercise 14, page 42]), we have that for each k,

$$\mu'_k=\prod_p\left(1-\frac{1}{p}+\frac{1}{p}\Big(1-\frac{1}{p}\Big)^{-k}\right)=\prod_p\left(1+\frac{1}{p}\bigg(\Big(\frac{p}{p-1}\Big)^k-1^k\bigg)\right).$$

By the mean value theorem,

$$\begin{aligned}1+\frac{1}{p}\bigg(\Big(\frac{p}{p-1}\Big)^k-1^k\bigg)&=1+O\bigg(\frac{k}{p(p-1)}\Big(\frac{p}{p-1}\Big)^{k-1}\bigg)\\&=1+O\bigg(\frac{k}{p^2}\Big(1+\frac{1}{p-1}\Big)^{k-1}\bigg)\\&<1+O\bigg(\frac{k}{p^2}\exp\Big(\frac{k-1}{p-1}\Big)\bigg),\end{aligned}$$

and so

$$\mu'_k<\prod_{p\le k}\left(1+O\bigg(\frac{k}{p^2}\exp\Big(\frac{k-1}{p-1}\Big)\bigg)\right)\prod_{p>k}\left(1+O\bigg(\frac{k}{p^2}\exp\Big(\frac{k-1}{p-1}\Big)\bigg)\right).\tag{33}$$

In the first product, we use the crude inequality

$$1+O\bigg(\frac{k}{p^2}\exp\Big(\frac{k-1}{p-1}\Big)\bigg)<1+O\bigg(k\exp\Big(\frac{k}{p-1}\Big)\bigg)\ll k\exp\Big(\frac{k}{p-1}\Big),$$

so that for some absolute constant C,

$$\begin{aligned}\prod_{p\le k}\left(1+O\bigg(\frac{k}{p^2}\exp\Big(\frac{k-1}{p-1}\Big)\bigg)\right)&\le\prod_{p\le k}Ck\exp\Big(\frac{k}{p-1}\Big)\\&\le(Ck)^{\pi(k)}\exp\Big(k\sum_{p\le k}\frac{1}{p-1}\Big)\\&=\exp(O(k))\exp(O(k\log\log k)).\end{aligned}$$

In the second product, the exponential factor is uniformly bounded, and so

$$\begin{aligned}\prod_{p>k}\left(1+O\left(\frac{k}{p^2}\exp\left(\frac{k-1}{p-1}\right)\right)\right) &= \prod_{p>k}\left(1+O\left(\frac{k}{p^2}\right)\right)\\ &< \prod_{p>k}\left(\exp\left(O\left(\frac{k}{p^2}\right)\right)\right)\\ &\le \exp\left(O\left(\sum_p \frac{k}{p^2}\right)\right) = \exp(O(k)).\end{aligned}$$

In light of these last two estimates, equation (33) yields $\mu_k' \le \exp(O(k\log\log k))$ as required. □

Remarks. It is worthwhile to make a few remarks about the behavior of $D(u)$. Let $u_0 := \frac{2}{3}C_2$. We can view equation (20), with $z=\infty$, as providing us with a conveniently factored Euler product expansion of $K^*(N)$. Comparing the terms of this expansion with those in the product expansion for C_2, one sees that $K^*(N) > u_0$ for all N. In fact, one finds that $K^*(N)$ is bounded away from u_0 unless all of the small odd primes belong to $\mathcal{A}$, i.e., unless $N(N-1)$ possesses no small odd prime factors. Conversely, if $N(N-1)$ has no small odd prime factors, an averaging argument shows that $K^*(N)$ is usually close to u_0. In this way, one proves that $D(u_0)=0$ while $D(u)>0$ for $u>u_0$.

Since $K(N)$ is absolutely bounded and bounded away from zero, several results on $D(u)$ follow immediately from corresponding results for the distribution function of $N/\phi(N)$, whose behavior has been studied by Erdős [11] and Weingartner [21, 22]. In particular, from [11, Theorem 1], we see that $D(u) > 1-\exp(-\exp(Cu))$ for a certain constant $C>0$ and all large u.

Finally, we remark that there is an alternative, more arithmetic approach to the proof of Theorem 1.4, based on ideas and results of Erdős [10] and Shapiro [20]. This approach allows us to show that the distribution function $D(u)$ of Theorem 1.4 is continuous everywhere and strictly increasing for $u>u_0$. We omit the somewhat lengthy arguments for these claims.

ACKNOWLEDGEMENTS

We thank Igor Shparlinski for bringing the reference [3] to our attention. We also thank the anonymous referee for a careful reading of the manuscript.

REFERENCES

[1] S. Baier, *A remark on the Lang-Trotter conjecture*, New Directions in Value-Distribution Theory of Zeta and L-Functions, Ber. Math., Shaker Verlag, Aachen, 2009, pp. 11–18.

[2] A. Balog, A. Cojocaru, and C. David, *Average twin prime conjecture for elliptic curves*, Amer. J. Math. **133** (2011), no. 5, 1179–1229.

[3] W. D. Banks and I. E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math. **173** (2009), 253–277.

[4] V. Chandee, C. David, D. Koukoulopoulos, and E. Smith, *Elliptic curves over finite fields with a given group structure*, in preparation.

[5] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[6] C. David and E. Smith, *Elliptic curves with a given number of points over finite fields*, Compositio Math. **149** (2013), 175–203.

[7] C. David and E. Smith, *Corrigendum to "Elliptic curves with a given number of points over finite fields"*, to appear; online as part of `arXiv:1108.3539v4 [math.NT]`.

[8] C. David and J. Wu, *Pseudoprime reductions of elliptic curves*, Canadian J. Math. **64** (2012), 81–101.

[9] R. Durrett, *Probability: theory and examples*, 4th ed., Cambridge Series in Statistical and Probabilistic Mathematics, Cambridge University Press, Cambridge, 2010.

[10] P. Erdős, *On the density of some sequences of numbers* I–III, J. London Math. Soc. **10** (1935), 120–125, **12** (1937), 7–11, and **13** (1938), 119–127.

[11] ———, *Some remarks about additive and multiplicative functions*, Bull. Amer. Math. Soc. **52** (1946), 527–537.

[12] E. Fouvry and M. Ram Murty, *On the distribution of supersingular primes*, Canadian J. Math. **48** (1996), 81–104.

[13] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper* I–III, J. Reine Angew. Math. **175** (1936), 55–62, 69–88, and 193–207.

[14] N. Jones, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685–710.

[15] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165.

[16] E. Kowalski, *Analytic problems for elliptic curves*. J. Ramanujan Math. Soc. **21** (2006), no. 1, 19–114.

[17] A. Languasco, A. Perelli, and A. Zaccagnini, *On the Montgomery–Hooley Theorem in short intervals*, Mathematika **56** (2010), 231–243.

[18] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[19] I. J. Schoenberg, *Über die asymptotische Verteilung reeler Zahlen mod* 1, Math. Z. **28** (1928), 171–199.

[20] H. N. Shapiro, *Addition of functions in probabilistic number theory*, Comm. Pure Appl. Math. **26** (1973), 55–84.

[21] A. Weingartner, *The distribution functions of $\sigma(n)/n$ and $n/\phi(n)$*, Proc. Amer. Math. Soc. **135** (2007), 2677–2681 (electronic).

[22] ———, *The distribution functions of $\sigma(n)/n$ and $n/\phi(n)$, II*, J. Number Theory **132** (2012), 2907–2921.

[23] D. Zywina, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, ROOM 121, 1984 MATHEMATICS ROAD, VANCOUVER, BC, V6T 1Z2, CANADA
E-mail address: gerg@math.ubc.ca

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, BOYD GRADUATE STUDIES RESEARCH CENTER, ATHENS, GA 30602, USA
E-mail address: pollack@uga.edu

DEPARTMENT OF MATHEMATICS, LIBERTY UNIVERSITY, 1971 UNIVERSITY BLVD, MSC BOX 710052, LYNCHBURG, VA 24502, USA
E-mail address: ecsmith13@liberty.edu