VARIATIONS ON A THEME OF ROMANOFF

M. RAM MURTY[1]
Mathematics Department
McGill University
Montréal
Canada
E-mail: murty@math.mcgill.ca

MICHAEL ROSEN[2]
Mathematics Department
Brown University
Providence, RI 02912
USA
E-mail: michael_rosen@brown.edu

JOSEPH H. SILVERMAN[3]
Mathematics Department
Brown University
Providence, RI 02912
USA
E-mail: joseph_silverman@brown.edu

Received 21 August 1995

1991 Mathematics Subject Classification: 11A07 11G10 11R04

Fix an integer $a \geq 2$. For each $m \geq 1$, let $f_a(m)$ be the smallest power f so that $a^f \equiv 1 \pmod{m}$. We give explicit upper bounds for the series $\sum_m 1/mf_a(m)^\epsilon$ and $\sum_p \log(p)/pf_a(p)^\epsilon$, generalizing and strengthening results of Romanoff, Landau, Erdös and Turan. We also prove analogous results over number fields and for abelian varieties.

Introduction

Let $a \geq 2$ be an integer, and for each positive integer m, let

$$f_a(m) = \min\{f \geq 1 : a^f \equiv 1 \pmod{m}\}.$$

(If $\gcd(a,m) > 1$, we set $f_a(m) = \infty$.) Romanoff [12] proved that the series $\sum_{m\geq 1} 1/mf_a(m)$ converges. The dependence on a was made explicit by Landau [9],

[1]Research partially supported by NSERC grant OGP0009418.
[2]Research partially supported by NSF DMS-9209063.
[3]Research partially supported by NSF DMS-9121727.

International Journal of Mathematics Volume 7, No. 3 (1996) 373–391

who proved an upper bound of the form $C(\log\log a)^2$, and this was improved by Erdös and Turan [6,7] who proved for every $\varepsilon > 0$,

$$\sum_{m\geq 1} \frac{1}{m f_a(m)^\varepsilon} \leq C_1(\varepsilon)\log\log a\,. \tag{1}$$

(See also [4] for some related work of Erdös.) In this paper we will give a simplified proof of the Erdös–Turan result (1) which leads to the more precise estimate

$$\sum_{m\geq 1} \frac{1}{m f_a(m)^\varepsilon} \leq e^\gamma \log\log a + 2e^\gamma \varepsilon^{-1} + C_2 \tag{2}$$

with an absolute constant C_2. Here $\gamma \approx 0.577216$ is Euler's constant. We will also show that the $e^\gamma \log\log a$ cannot be improved, and we will give an estimate for an analgous sum over primes:

$$\sum_{p} \frac{\log p}{p f_a(p)^\varepsilon} \leq \log\log a + 2\varepsilon^{-1} + C_3\,. \tag{3}$$

There are a number of ways to extend and generalize (2) and (3). For example, we can replace the element a with a free subgroup $\Gamma \subset K^*$ of rank r in a number field K with ring of integers R. Then $f_a(m)$ becomes

$$f_\Gamma(\mathfrak{m}) = \#\,\mathrm{Image}(\Gamma \longrightarrow R/\mathfrak{m})\,.$$

(If some element of Γ is not relatively prime to $\mathfrak{m}$, set $f_\Gamma(\mathfrak{m}) = \infty$.) We will prove

$$\sum_{\mathfrak{m}\neq(0)} \frac{1}{N\mathfrak{m}\cdot f_\Gamma(\mathfrak{m})^\varepsilon} \leq e^\gamma \kappa_K \log\log H_K(\Gamma) + \left(1+\frac{1}{r}\right) e^\gamma \kappa_K \varepsilon^{-1} + C_4(K,r)\,, \tag{4}$$

$$\sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}\cdot f_\Gamma(\mathfrak{p})^\varepsilon} \leq \log\log H_K(\Gamma) + \left(1+\frac{1}{r}\right)\varepsilon^{-1} + C_5(K,r)\,, \tag{5}$$

where κ_K is the residue of $\zeta_K(s)$ at $s=1$ and $H_K(\Gamma)$ is a certain height associated to Γ.

We can also replace the multiplicative group K^* with an abelian variety A/K. Much of the argument is the same, so we will just prove the analogue of (5). Thus let $\Gamma \subset A(K)$ be a free subgroup of rank r, and for each prime ideal $\mathfrak{p}$ let

$$f_\Gamma(\mathfrak{p}) = \#\,\mathrm{Image}(\Gamma \longrightarrow A \bmod \mathfrak{p})\,.$$

(If A has bad reduction at $\mathfrak{p}$, one can either set $f_\Gamma(\mathfrak{p}) = \infty$ or work on the Néron model of A.) We will prove that

$$\sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}\cdot f_\Gamma(\mathfrak{p})^\varepsilon} \leq \log \hat{h}_K(\Gamma) + \left(1+\frac{2}{r}\right)\varepsilon^{-1} + C_6(A/K)\,, \tag{6}$$

where $\hat{h}_K(\Gamma)$ is a certain canonical height associated to Γ. Notice that the quantity $(1+1/r)\varepsilon^{-1}$ in (5) has been replaced by a $(1+2/r)\varepsilon^{-1}$ in (6). This occurs because the logarithm function $\log(a^f)$ is linear in f, while the canonical height $\hat{h}_K(fP)$ is quadratic in f.

We will now briefly describe the contents of this paper. In the first section we prove (2). This serves to illustrate the general method in the simplest setting. In Sec. 2 we work with finitely generated groups in number fields and prove (4) and (5). Section 3 contains a proof of the abelian variety estimate (6). In the last section we show how the explicit dependence on ε in (2), (3), (4), (5), and (6) can be used to give density estimates. For example, we will use (2) and (3) to prove that for any $\theta > 0$ the sets

$$\{m \geq 1 : f_a(m) \leq m^\theta\} \quad \text{and} \quad \{p : f_a(p) \leq p^\theta\}$$

have (upper) Dirichlet densities at most $57\theta/16$ and 2θ respectively.

We close this introduction with a brief remark. An important application of Romanoff's theorem [12] is its use in the proof of Bilharz' theorem [2] concerning the function field analogue of Artin's conjecture on primitive roots. Let $\mathbb{F}_q$ be a finite field with q elements, let $A = \mathbb{F}_q[T]$, and let $a \in A$ be a non-constant polynomial which is not an ℓth power for any $\ell | q-1$. Bilharz shows that the Dirichlet density of the prime ideals in A for which a is a primitive root is given by the sum $\sum_m \mu(m)/mf_q(m)$. The absolute convergence of this sum is a consequence of Romanoff's theorem. That the sum is positive follows from a theorem of Heilbronn. Bilharz's full result is even more general than this.

1. A Refinement of Erdös–Turan

In this section we will prove the following refinement of the theorem of Erdös and Turan [6,7].

Theorem 1.1. *Let $a \geq 2$ be an integer, let $\varepsilon > 0$, and for each integer $m \geq 1$, define $f_a(m)$ by*

(a) $$f_a(m) = \min\{f \geq 1 : a^f \equiv 1 \pmod{m}\}.$$

$$\sum_{m=1}^{\infty} \frac{1}{mf_a(m)^\varepsilon} \leq e^\gamma \log\log a + 2e^\gamma \varepsilon^{-1} + O(1).$$

(b) *Let $N \geq 2$ and $a = 1 + \mathrm{LCM}[1, 2, \ldots, N]$. Then*

$$\sum_{m=1}^{\infty} \frac{1}{mf_a(m)^\varepsilon} \geq e^\gamma \log\log a + O(\log\log\log a) \qquad \text{as} \quad N \to \infty.$$

(*In both parts, $\gamma \approx 0.577216$ is Euler's constant and the $O(1)$ constants are absolute and effectively computable.*)

Remark. Notice that $f_a(m) < m$ for all m with $\gcd(a,m) = 1$, so we have

$$\sum_{m=1}^{\infty} \frac{1}{m f_a(m)^{\varepsilon}} \geq \sum_{\substack{m \geq 1 \\ \gcd(a,m)=1}} \frac{1}{m^{1+\varepsilon}} = \prod_{p \mid a} \left(1 - \frac{1}{p^{1+\varepsilon}}\right) \zeta(1+\varepsilon) .$$

This shows that the series grows at least like $C(a)\varepsilon^{-1}$ as $\varepsilon \to 0$. It would be interesting to compute the exact value of $\varepsilon \sum 1/m f_a(m)^{\varepsilon}$ as $\varepsilon \to 0$ (if the limit exists).

The first step in proving Theorem 1.1 is the following elementary consequence of Mertens' theorem.

Lemma 1.2. *For all integers $n \geq 2$,*

$$\sum_{d \mid n} \frac{1}{d} \leq e^{\gamma} \log\log n + O(1) .$$

Proof. This follows from Mertens' theorem [8, Theorem 429] and a standard argument looking at large primes and small primes. (See also [8, Theorem 323].) We will prove a more general number field version in the next section (Corollary 2.3), so we do not include a proof here. □

During the proof of Theorem 1.1 we will need to consider the following two sums:

$$d_a(f) = \sum_{\substack{m \geq 1 \\ f_a(m) = f}} \frac{1}{m}, \qquad D_a(x) = \sum_{f \leq x} d_a(f) .$$

Lemma 1.3. *For all $x \geq 1$,*

$$D_a(x) \leq 2e^{\gamma} \log x + e^{\gamma} \log\log a + O(1) .$$

Proof. Let

$$A(x) = \prod_{f \leq x} (a^f - 1) .$$

The trivial estimate

$$A(x) = \prod_{f \leq x} (a^f - 1) \leq \prod_{f \leq x} a^f \leq a^{x(x+1)/2} \leq a^{x^2}$$

gives

$$\log\log A(x) \leq 2\log x + \log\log a . \tag{7}$$

We also observe that

$$f_a(m) \le x \iff a^f \equiv 1 \pmod{m} \text{ for some } f \le x \Longrightarrow m | A(x). \tag{8}$$

We compute

$$\begin{aligned} D_a(x) &= \sum_{f \le x} d_a(f) = \sum_{f \le x} \sum_{\substack{m \ge 1 \\ f_a(m) = f}} \frac{1}{m} \quad \text{by definition of } D_a,\ d_a \\ &= \sum_{\substack{m \ge 1 \\ f_a(m) \le x}} \frac{1}{m} \le \sum_{m | A(x)} \frac{1}{m} \quad \text{from (8)} \\ &\le e^\gamma \log\log A(x) + O(1) \quad \text{from Lemma 1.2} \\ &\le e^\gamma (2 \log x + \log\log a) + O(1) \quad \text{from (7)}. \end{aligned}$$

This completes the proof of Lemma 1.3. □

We are now ready to prove Theorem 1.1.

Proof (of Theorem 1.1). Let S_a be the sum we are trying to estimate. We rewrite S_a as

$$S_a = \sum_{m=1}^{\infty} \frac{1}{m f_a(m)^\varepsilon} = \sum_{f=1}^{\infty} \frac{1}{f^\varepsilon} \sum_{\substack{m \ge 1 \\ f_a(m) = f}} \frac{1}{m} = \sum_{f=1}^{\infty} \frac{d_a(f)}{f^\varepsilon}.$$

Lemma 1.3 tells us that

$$\lim_{x \to \infty} \frac{1}{x^\varepsilon} \sum_{f \le x} d_a(f) = \lim_{x \to \infty} \frac{1}{x^\varepsilon} \cdot D_a(x) = 0,$$

so we can apply Abel summation to compute

$$\begin{aligned} S_a &= \int_1^\infty D_a(t) \cdot \frac{\varepsilon}{t^{1+\varepsilon}}\, dt \quad \text{(Abel summation [1, Theorem 4.2])} \\ &\le \int_1^\infty \frac{(2e^\gamma \log t + e^\gamma \log\log a + O(1))\varepsilon}{t^{1+\varepsilon}}\, dt \quad \text{(from Lemma 1.3)} \\ &= 2e^\gamma \varepsilon^{-1} + e^\gamma \log\log a + O(1) \quad \text{(elementary calculus)}. \end{aligned}$$

This completes the proof of Theorem 1.1(a).

To prove (b), we let $a = 1 + \mathrm{LCM}[1, \ldots, N]$. Notice that $f_a(m) = 1$ for all m dividing $a - 1$, so we have

$$S_a \ge \sum_{m | a-1} \frac{1}{m} = \sum_{m | \,\mathrm{LCM}[1, \ldots, N]} \frac{1}{m} = e^\gamma \log N + O(\log\log N),$$

where the last equality is an exercise using Mertens' theorem. On the other hand, the prime number theorem says that

$$\psi(N) = \log \mathrm{LCM}[1, \ldots, N] \sim N,$$

so $\log N = \log(a-1) + o(1)$. Substituting this in above gives the desired result. □

Remark. Erdös [4] has proven estimates of the form

$$\sum_{d \mid a^f - 1} \frac{1}{d} \leq C_4(a) \log\log f.$$

Such estimates are clearly closely related to the results in this paper. He also conjectures (in our notation) that

$$D_a(x) \sim C_5(a) \log x \qquad \text{and proves that} \qquad \lim_{f \to \infty} d_a(f) = 0.$$

More precisely, Erdös only considers the case $a = 2$, but the general case should follow similarly. Pomerance (private communication) has suggested that the constant $C_5(a)$ should equal $\phi(a)/a$.

Remark. Sometimes it is useful to have estimates like those in Theorem 1.1 for sums involving $f_a(m)$ over squarefree integers m, see for example [12]. Using exactly the same methods, it is not hard to show that

$$\sum_{m=1}^{\infty} \frac{\mu(m)^2}{m f_a(m)^{\varepsilon}} \leq \frac{e^{\gamma}}{\zeta(2)} (\log\log a + 2\varepsilon^{-1}) + O(1),$$

where the notation is as in Theorem 1.1. We will leave the details to the reader.

2. Bounds for $\mathbb{G}_m$ over Number Fields

In this section we are going to generalize Theorem 1.1 by estimating an analogous sum for finitely generated subgroups of the multiplicative group of a number field. We set the following notation, which will be used throughout the remainder of this paper.

K	a number field of degree d.
R	the ring of integers of K.
κ_K	the residue of $\zeta_K(s)$ at $s = 1$. Thus $\kappa_K = 2^{r_1}(2\pi)^{r_2} h_K R_K / w_K D_K^{1/2}$, where r_1, r_2 are the number of real and complex embeddings of K, h_K is the class number of K, R_K is the regulator of K, w_K is the number of roots of unity in K, and D_K is the absolute discriminant of $K/\mathbb{Q}$.
H_K	Weil height on K (see [10, Ch. 3, Sec. 1]).
Γ	a free finitely generated subroup of K^* of rank $r \geq 1$.

$H_K(\Gamma)$ the minimum value of $3H_K(a_1)\cdots H_K(a_r)$ over all sets of generators $\{a_1,\dots,a_r\}$ for Γ. (The factor of 3 is included merely to ensure that $H_K(\Gamma)\geq 3$, so the quantity $\log\log H_K(\Gamma)$ will be positive.)

For each non-zero integral ideal $\mathfrak{m}$ of K, we define

$$f_\Gamma(\mathfrak{m})=\begin{cases}\#\,\mathrm{Image}(\Gamma\longrightarrow R/\mathfrak{m}) & \text{if } \mathrm{ord}_{\mathfrak{p}}(a)=0 \text{ for all } \mathfrak{p}|\mathfrak{m} \text{ and all } a\in\Gamma,\\ \infty & \text{otherwise.}\end{cases}$$

Finally, we will use functions which have the following four properties:

$$\left[\begin{array}{ll}\text{(i)} & G:[1,\infty)\to[0,1].\\ \text{(ii)} & G \text{ is continuously differentiable and non-increasing.}\\ \text{(iii)} & G(1)=1.\\ \text{(iv)} & \int_1^\infty G(x)/x\,dx<\infty.\end{array}\right] \qquad (*)$$

For example, the functions $x^{-\varepsilon}$ and $(1+\log x)^{-1-\varepsilon}$ satisfy condition $(*)$.

We are now ready to state our main result.

Theorem 2.1. *With notation as above, let $G(x)$ be a function satisfying $(*)$. Then the following estimates hold, where the first sum is over non-zero integral ideals of K and the second sum is over prime ideals of K :*

$$\sum_{\mathfrak{m}\neq(0)}\frac{G\big(f_\Gamma(\mathfrak{m})\big)}{N\mathfrak{m}}\leq e^\gamma\kappa_K\log\log H_K(\Gamma)+e^\gamma\kappa_K\left(1+\frac{1}{r}\right)\int_1^\infty\frac{G(x)}{x}dx+O_K(r) \qquad (9)$$

$$\sum_{\mathfrak{p}}G\big(f_\Gamma(\mathfrak{p})\big)\frac{\log N\mathfrak{p}}{N\mathfrak{p}}\leq\log\log H_K(\Gamma)+\left(1+\frac{1}{r}\right)\int_1^\infty\frac{G(x)}{x}dx+O_K(r)\,. \qquad (10)$$

Remark. We observe that if we take $G(x)=x^{-\varepsilon}$, then (9) and (10) become the inequalities (4) and (5) stated in the introduction. If we further take $K=\mathbb{Q}$ and $\Gamma=\langle a\rangle$, then (9) and (10) become (2) and (3). So Theorem 2.1 contains all of the inequalities stated in the introduction except for the estimate (6) dealing with abelian varieties which we will prove in the next section.

We begin with a number field version of Mertens' theorem and a useful corollary.

Proposition 2.2. *For all $x\geq 1$,*

$$\prod_{N\mathfrak{p}\leq x}\left(1-\frac{1}{N\mathfrak{p}}\right)^{-1}=e^\gamma\kappa_K\log x+O_K(1)\quad\text{(Mertens' theorem)} \qquad (11)$$

$$\sum_{N\mathfrak{p}\leq x}\frac{\log N\mathfrak{p}}{N\mathfrak{p}}=\log x+O_K(1)\,. \qquad (12)$$

Here $\gamma\approx 0.577216$ is Euler's constant.

Proof. These are standard results over $\mathbb{Q}$, although Mertens' theorem is usually stated merely as an asymptotic estimate instead of with the $O(1)$. See for example [8, Theorem 429] for (11) and [8, Theorem 425] for (12). These proofs can be adapted to the number field case and the stronger Mertens' estimate proven by making use of well-known properties of the Dedekind zeta function $\zeta_K(s)$. See [13] for details. □

Corollary 2.3. *Let* $\mathfrak{n}$ *be a non-zero integral ideal in* K *with norm* $N\mathfrak{n} \geq 2$. *Then*

$$\sum_{\mathfrak{d}|\mathfrak{n}} \frac{1}{N\mathfrak{d}} \leq e^{\gamma}\kappa_K \log\log N\mathfrak{n} + O_K(1) \tag{13}$$

$$\sum_{\mathfrak{p}|\mathfrak{n}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq \log\log N\mathfrak{n} + O_K(1)\,. \tag{14}$$

Proof. Let

$$f(\mathfrak{n}) = \#\{\mathfrak{p} : \mathfrak{p}|\mathfrak{n} \text{ and } N\mathfrak{p} > \log N\mathfrak{n}\}\,.$$

We begin with the "large" primes. Thus

$$N\mathfrak{n} \geq \prod_{\substack{\mathfrak{p}|\mathfrak{n} \\ N\mathfrak{p}>\log N\mathfrak{n}}} N\mathfrak{p} \geq (\log N\mathfrak{n})^{f(\mathfrak{n})}, \qquad \text{so} \quad f(\mathfrak{n}) \leq \frac{\log N\mathfrak{n}}{\log\log N\mathfrak{n}}\,.$$

This allows us to estimate

$$\begin{aligned}\prod_{\substack{\mathfrak{p}|\mathfrak{n} \\ N\mathfrak{p}>\log N\mathfrak{n}}} \left(1-\frac{1}{N\mathfrak{p}}\right)^{-1} &\leq \left(1-\frac{1}{\log N\mathfrak{n}}\right)^{-f(\mathfrak{n})} \\ &\leq \left(1-\frac{1}{\log N\mathfrak{n}}\right)^{-\log N\mathfrak{n}/\log\log N\mathfrak{n}} \\ &= 1+O\left(\frac{1}{\log\log N\mathfrak{n}}\right). \end{aligned} \tag{15}$$

Similarly we estimate

$$\sum_{\substack{\mathfrak{p}|\mathfrak{n} \\ N\mathfrak{p}>\log N\mathfrak{n}}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq f(\mathfrak{n})\frac{\log\log N\mathfrak{n}}{\log N\mathfrak{n}} \leq 1\,. \tag{16}$$

Next we consider the "small" primes. Using Mertens' theorem (11), we compute

$$\prod_{\substack{\mathfrak{p}|\mathfrak{n} \\ N\mathfrak{p}\leq\log N\mathfrak{n}}} \left(1-\frac{1}{N\mathfrak{p}}\right)^{-1} \leq \prod_{N\mathfrak{p}\leq\log N\mathfrak{n}} \left(1-\frac{1}{N\mathfrak{p}}\right)^{-1} = e^{\gamma}\kappa_K \log\log N\mathfrak{n}+O_K(1)\,. \tag{17}$$

Similarly using (12) we find

$$\sum_{\substack{\mathfrak{p}|\mathfrak{n} \\ N\mathfrak{p}\le \log N\mathfrak{n}}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \le \sum_{N\mathfrak{p}\le \log N\mathfrak{n}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \log\log N\mathfrak{n} + O_K(1)\,. \tag{18}$$

Now multiplying (15) and (17) gives

$$\sum_{\mathfrak{d}|\mathfrak{n}} \frac{1}{N\mathfrak{d}} \le \prod_{\mathfrak{p}|\mathfrak{n}} \left(1 - \frac{1}{N\mathfrak{p}}\right)^{-1} \le (e^{\gamma}\kappa_K \log\log N\mathfrak{n} + O_K(1))\left(1 + O\left(\frac{1}{\log\log N\mathfrak{n}}\right)\right)$$

$$= e^{\gamma}\kappa_K \log\log N\mathfrak{n} + O_K(1)\,,$$

which is exactly (13). Similarly, adding (16) and (18) gives (14). This completes the proof of Corollary 2.3.

The next result provides the crucial estimate needed for the proof of Theorem 2.1.

Proposition 2.4. *For all* $x \ge 1$,

$$\sum_{\substack{\mathfrak{m}\ne(0) \\ f_\Gamma(\mathfrak{m})\le x}} \frac{1}{N\mathfrak{m}} \le e^{\gamma}\kappa_K \log\log H_K(\Gamma) + e^{\gamma}\kappa_K\left(1 + \frac{1}{r}\right)\log x + O_K(r) \tag{19}$$

$$\sum_{\substack{\mathfrak{p} \\ f_\Gamma(\mathfrak{p})\le x}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \le \log\log H_K(\Gamma) + \left(1 + \frac{1}{r}\right)\log x + O_K(r)\,. \tag{20}$$

Proof. Fix generators $a_1, \dots, a_r$ for Γ so that $H_K(\Gamma) = 3H_K(a_1)\cdots H_K(a_r)$. For $y \ge 1$, let

$$\Gamma(y) = \{a_1^{n_1}\cdots a_r^{n_r} \in \Gamma : |n_1|, \dots, |n_r| \le y\}\,.$$

For any $a \in K^*$, write the ideal $(a-1)$ as a quotient of integral ideals,

$$(a-1) = \mathfrak{a}_a\mathfrak{d}_a^{-1}\,.$$

We define an ideal $\mathfrak{A}_\Gamma(y)$ by

$$\mathfrak{A}_\Gamma(y) = \prod_{a\in\Gamma(y),\, a\ne 1} \mathfrak{a}_a\,.$$

Our first job is to prove the following claim.

Claim 1: If $f_\Gamma(\mathfrak{m}) \le x$, then $\mathfrak{m}|\mathfrak{A}_\Gamma(x^{1/r}+2)$.

Note that if $f_\Gamma(\mathfrak{m}) < \infty$, then every element of Γ is relatively prime to $\mathfrak{m}$, so we can reduce them modulo $\mathfrak{m}$. Consider the map

$$\Gamma(y) \longrightarrow R/\mathfrak{m}, \qquad a \longmapsto a \bmod \mathfrak{m}.$$

The image has order

$$\#(\Gamma \bmod \mathfrak{m}) = f_\Gamma(\mathfrak{m})$$

by definition. On the other hand, if $y \geq 1$, then $\Gamma(y)$ has order

$$\#\Gamma(y) = \#\{a_1^{n_1} \cdots a_r^{n_r} \in \Gamma : |n_1|, \ldots, |n_r| \leq y\} \geq (2y-1)^r.$$

Hence if we set $y = \frac{1}{2}x^{1/r} + 1$, then we have a strict inequality

$$\#\Gamma(y) > \#(\Gamma \bmod \mathfrak{m}),$$

so we can find distinct elements $a, b \in \Gamma(y)$ with the same image. Then

$$ab^{-1} \in \Gamma(2y) \qquad \text{and} \qquad ab^{-1} \equiv 1 \pmod{\mathfrak{m}},$$

so $\mathfrak{m} | \mathfrak{a}_{ab^{-1}}$. Therefore $\mathfrak{m} | \mathfrak{A}_\Gamma(2y)$, which completes the proof of Claim 1.

Using Claim 1 and the inequalities (13) and (14) of Corollary 2.3, we find that

$$\sum_{\substack{\mathfrak{m} \neq (0) \\ f_\Gamma(\mathfrak{m}) \leq x}} \frac{1}{N\mathfrak{m}} \leq \sum_{\mathfrak{m} | \mathfrak{A}_\Gamma(x^{1/r}+2)} \frac{1}{N\mathfrak{m}} \leq e^\gamma \kappa_K \log\log N\mathfrak{A}_\Gamma(x^{1/r}+2) + O_K(1) \tag{21}$$

$$\sum_{\substack{\mathfrak{p} \\ f_\Gamma(\mathfrak{p}) \leq x}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq \sum_{\mathfrak{p} | \mathfrak{A}_\Gamma(x^{1/r}+2)} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq \log\log N\mathfrak{A}_\Gamma(x^{1/r}+2) + O_K(1). \tag{22}$$

To complete the proof of Proposition 2.4, we need an upper bound for $N\mathfrak{A}_\Gamma(y)$ as described in our second claim.

Claim 2: $N\mathfrak{A}_\Gamma(y) \leq 2^{d(3y)^r} H_K(\Gamma)^{(3y)^{r+1}}$.

To prove this claim we use elementary properties of height functions. Let $a \in K$ with $a \neq 1$. Then [10, pp. 51,53] tells us that

$$H_K(a-1) = H_K\left(\frac{1}{a-1}\right) = N\mathfrak{a}_a \prod_{v \in M_K^\infty} \max\{1, \|a-1\|_v\} \geq N\mathfrak{a}_a. \tag{23}$$

We will also need the triangle inequality in the form

$$H_K(u+v) \leq 2^d H_K(u) H_K(v) \qquad \text{for all } u, v \in K. \tag{24}$$

Hence

$$\begin{aligned}
N\mathfrak{A}_\Gamma(y) &= \prod_{a\in\Gamma(y),\, a\neq 1} N\mathfrak{a}_a \quad \text{(definition of } \mathfrak{A}_\Gamma(y)\text{)} \\
&\le \prod_{a\in\Gamma(y)} H_K(a-1) \quad \text{(from (23))} \\
&\le \prod_{a\in\Gamma(y)} 2^d H_K(a) \quad \text{(from (24))} \\
&= \prod_{|n_1|\le y} \cdots \prod_{|n_r|\le y} 2^d H_K(a_1^{n_1}\cdots a_r^{n_r}) \quad \text{(definition of } \Gamma(y)\text{)} \\
&\le \prod_{|n_1|\le y} \cdots \prod_{|n_r|\le y} 2^d H_K(a_1)^{|n_1|}\cdots H_K(a_r)^{|n_r|} \\
&\le 2^{d(2y+1)^r} (H_K(a_1)\cdots H_K(a_r))^{(2y+1)^{r-1}y(y+1)} \\
&\le 2^{d(3y)^r} H_K(\Gamma)^{(3y)^{r+1}} .
\end{aligned}$$

This completes the proof of Claim 2.

We now apply Claim 2 with $y = x^{1/r} + 2$ and take the double logarithm of both sides to obtain the estimate

$$\begin{aligned}
\log\log N\mathfrak{A}_\Gamma(x^{1/r}+2) &\le \log\{d(3x^{1/r}+6)^r \log 2 + (3x^{1/r}+6)^{r+1}\log H_K(\Gamma)\} \\
&= (r+1)\log(3x^{1/r}+6) + \log\left(\frac{d\log 2}{3x^{1/r}+6} + \log H_K(\Gamma)\right) \\
&\le \left(1+\frac{1}{r}\right)\log x + \log\log H_K(\Gamma) + O_K(r) . \qquad (25)
\end{aligned}$$

Substituting (25) into (21) gives (19), and substituting (25) into (22) gives (20). This completes the proof of Proposition 2.4. □

We have now assembled all of the tools needed to prove Theorem 2.1.

Proof (of Theorem 2.1). To ease notation, we let

$$d_\Gamma(f) = \sum_{\substack{\mathfrak{m}\neq(0)\\ f_\Gamma(\mathfrak{m})=f}} \frac{1}{N\mathfrak{m}}, \qquad D_\Gamma(x) = \sum_{f\le x} d_\Gamma(f) = \sum_{\substack{\mathfrak{m}\neq(0)\\ f_\Gamma(\mathfrak{m})\le x}} \frac{1}{N\mathfrak{m}} .$$

Proposition 2.4 tells us that $D_\Gamma(x) \ll \log x$, so the fact that $G(x)$ satisfies $(*)$ implies that

$$\lim_{x\to\infty} G(x) D_\Gamma(x) = 0 .$$

This allows us to apply Abel summation in the following calculation:

$$\sum_{\mathfrak{m}\neq(0)} \frac{G(f_\Gamma(\mathfrak{m}))}{N\mathfrak{m}} = \sum_{f=1}^{\infty} \sum_{\substack{\mathfrak{m}\neq(0)\\ f_\Gamma(\mathfrak{m})=f}} \frac{G(f)}{N\mathfrak{m}} = \sum_{f=1}^{\infty} G(f) d_\Gamma(f)$$

$$= -\int_1^\infty D_\Gamma(t) G'(t)\, dt \quad \text{(Abel summation [1, Theorem 4.2])}$$

$$\leq -\int_1^\infty \left\{ \varepsilon^\gamma \kappa_K \log\log H_K(\Gamma) + e^\gamma \kappa_K \left(1+\frac{1}{r}\right) \log t \right.$$

$$\left. + O_K(r) \right\} G'(t)\, dt \quad \text{(from (19). Note } G'(t) < 0.\text{)}$$

$$= e^\gamma \kappa_K \log\log H_K(\Gamma) + e^\gamma \kappa_K \left(1+\frac{1}{r}\right) \int_1^\infty \frac{G(t)}{t} dt + O_K(r)$$

(properties $(*)$ of G and integration by parts)

This completes the proof of the first inequality (9) of Theorem 2.1. The proof of the second inequality (10) is entirely similar, so we just briefly sketch. Thus we let

$$\tilde{d}_\Gamma(f) = \sum_{\substack{\mathfrak{p}\\ f_\Gamma(\mathfrak{p})=f}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}}, \qquad \tilde{D}_\Gamma(x) = \sum_{f\leq x} \tilde{d}_\Gamma(f) = \sum_{\substack{\mathfrak{p}\\ f_\Gamma(\mathfrak{p})=f}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}}. \tag{26}$$

Then

$$\sum_{\mathfrak{p}} G(f_\Gamma(\mathfrak{p})) \frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \sum_{f=1}^{\infty} G(f) \tilde{d}_\Gamma(f) = -\int_1^\infty \tilde{D}_\Gamma(t) G'(t)\, dt$$

$$\leq -\int_1^\infty \left\{ \log\log H_K(\Gamma) + \left(1+\frac{1}{r}\right) \log t + O_K(r) \right\} G'(t)\, dt$$

$$= \log\log H_K(\Gamma) + \left(1+\frac{1}{r}\right) \int_1^\infty \frac{G(t)}{t} dt + O_K(r). \qquad \square$$

3. Bounds for Abelian Varieties

In this section we will prove an estimate for series associated to abelian varieties analogous to the series (26) of Theorem 2.1. We let K be a number field and R its ring of integers as in Sec. 2, and we set the following additional notation for this section.

A/K an abelian variety defined over K.

$\mathcal{A}/R$ a Néron model for A/K.

$\hat{h}_K$ the logarithmic canonical height on $A(K)$, relative to K, associated to a very ample symmetric divisor.

Γ a free finitely generated subgroup of $A(K)$ of rank $r \geq 1$.

$\hat{h}_K(\Gamma)$ the minimum value of $\hat{h}_K(P_1)+\cdots+\hat{h}_K(P_r)+1$ over all sets of generators $\{P_1, \ldots, P_r\}$ for Γ. (Note $\hat{h}_K(\Gamma) \geq 1$.)

For each prime ideal $\mathfrak{p}$ of K, let

$$f_\Gamma(\mathfrak{p}) = \#\,\text{Image}(\Gamma \longrightarrow \mathcal{A} \bmod \mathfrak{p})\,.$$

Theorem 3.1. *With notation as above, let $G(x)$ be a function satisfying the properties $(*)$ described in Sec. 2. Then*

$$\sum_{\mathfrak{p}} G(f_\Gamma(\mathfrak{p}))\frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq \log \hat{h}_K(\Gamma) + \left(1+\frac{2}{r}\right)\int_1^\infty \frac{G(x)}{x}dx + O_{A/K}(r)\,. \tag{27}$$

We begin with an abelian analogue of Proposition 2.4.

Proposition 3.2. *For all $x \geq 1$,*

$$\sum_{\substack{\mathfrak{p} \\ f_\Gamma(\mathfrak{p}) \leq x}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq \log \hat{h}_K(\Gamma) + \left(1+\frac{2}{r}\right)\log x + O_{A/K}(r)\,. \tag{28}$$

Proof. Fix generators $P_1, \ldots, P_r$ for Γ so that $\hat{h}_K(\Gamma) = \hat{h}_K(P_1)+\cdots+\hat{h}_K(P_r)+1$. For $y \geq 1$, let

$$\Gamma(y) = \{n_1P_1 + \cdots + n_rP_r \in \Gamma : |n_1|, \ldots, |n_r| \leq y\}\,.$$

For any point $P \in A(K)$, $P \neq O$, define an ideal $\mathfrak{a}_P$ by

$$\mathfrak{a}_P = \prod_{\substack{\mathfrak{p} \\ P \equiv O \pmod{\mathfrak{p}}}} \mathfrak{p}\,.$$

That is, $\mathfrak{a}_P$ is the product of all prime ideals such that P reduces to the identity element on $\mathcal{A} \bmod \mathfrak{p}$. Then we define another ideal

$$\mathfrak{A}_\Gamma(y) = \prod_{P \in \Gamma(y),\, P \neq O} \mathfrak{a}_P\,.$$

We begin with the following claim.

Claim 1: If $f_\Gamma(\mathfrak{p}) \leq x$, then $\mathfrak{p} | \mathfrak{A}_\Gamma(x^{1/r}+2)$.

We consider the map

$$\Gamma(y) \longrightarrow \mathcal{A} \bmod \mathfrak{p}\,, \qquad P \longmapsto P \bmod \mathfrak{p}\,.$$

The image has order $\#(\Gamma \bmod \mathfrak{p}) = f_\Gamma(\mathfrak{p})$ by definition. But for $y \geq 1$, $\Gamma(y)$ has at least $(2y-1)^r$ elements. Hence if we set $y = \frac{1}{2}x^{1/r} + 1$, then there is a strict inequality $\#\Gamma(y) > \#(\Gamma \bmod \mathfrak{p})$. Therefore we can find distinct elements P, $Q \in \Gamma(y)$ with the same image modulo $\mathfrak{p}$. Then

$$P - Q \in \Gamma(y) \qquad \text{and} \qquad P - Q \equiv O \pmod{\mathfrak{p}},$$

so $\mathfrak{p} | \mathfrak{a}_{P-Q}$. Therefore $\mathfrak{p} | \mathfrak{A}_\Gamma(2y)$, which completes the proof of Claim 1.

Using Claim 1 and inequality (14) of Corollary 2.3, we find that

$$\sum_{\substack{\mathfrak{p} \\ f_\Gamma(\mathfrak{p}) \leq x}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq \sum_{\mathfrak{p} | \mathfrak{A}_\Gamma(x^{1/r}+2)} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \leq \log\log N\mathfrak{A}_\Gamma(x^{1/r}+2) + O_K(1). \tag{29}$$

To complete the proof of Proposition 3.2, we need an upper bound for $N\mathfrak{A}_\Gamma(y)$ as described in our second claim.

Claim 2: $\log N\mathfrak{A}_\Gamma(y) \leq (6y)^{r+2}\hat{h}_K(\Gamma) + O_{A/K}((3y)^r)$.

To prove this claim, we first observe that since $\hat{h}_K$ is defined relative to a very ample symmetric divisor D, we may assume that this divisor contains the zero element O of A. Then the canonical local height functions on A at a place $\mathfrak{p}$ satisfies

$$\hat{\lambda}_\mathfrak{p}(P) \geq -c_\mathfrak{p} \qquad \text{for all } P \in A(K). \tag{30}$$

$$\hat{\lambda}_\mathfrak{p}(P) \geq \log N\mathfrak{p} - c_\mathfrak{p} \quad \text{if } P \equiv O \pmod{\mathfrak{p}}. \tag{31}$$

Here the $c_\mathfrak{p}$'s are M_K-constants which depend on A/K. That is, they are non-negative constants for each place $\mathfrak{p}$ of K, and all but finitely many of them are zero. Now adding (30) and (31) over all places of K and using the definition of $\mathfrak{a}_P$, we find that

$$\hat{h}_K(P) = \sum_\mathfrak{p} \hat{\lambda}_\mathfrak{p}(P) \geq \sum_{\substack{\mathfrak{p} \\ P \equiv O \pmod{\mathfrak{p}}}} \log N\mathfrak{p} - \sum_\mathfrak{p} c_\mathfrak{p} = \log N\mathfrak{a}_P + O_{A/K}(1). \tag{32}$$

Remark 3.2.1. For general facts about canonical local height functions, see [10, Ch. 11]. The lower bound (30) is a general property of local heights relative to positive divisors [10, Ch. 10, Proposition 3.1]. Further, (31) is an immediate consequence of [10, Ch. 11, Theorem 5.1], since if $P \equiv O \pmod{\mathfrak{p}}$, then $P \bmod \mathfrak{p}$ lies on $D \bmod \mathfrak{p}$. Note that we are normalizing the local heights so that $\hat{h}_K(P) = \sum_v \hat{\lambda}_v(P)$. Also, we should mention that (30) is really only valid for points P not on the support of D. So we should really choose divisors $D_1, \ldots, D_n$ with $D_i \sim D$ and $\cap |D_i| = \{O\}$ and consider (30) for each D_i. We will ignore this technicality.

Remark 3.2.2. For elliptic curves, it is possible to prove (32) in a much more elementary fashion. Thus let E/K be an elliptic curve and let x, y be coordinate

functions for a Weierstrass equation for E/K. For any $P \in E(K)$, $P \neq O$, write the fractional ideal $(x(P))$ as $\mathfrak{b}_P\mathfrak{d}_P^{-1}$. Then $P \equiv O \pmod{\mathfrak{p}}$ for all but finitely many prime ideals $\mathfrak{p}|\mathfrak{d}_P$, so $\mathfrak{a}_P|\mathfrak{d}_P$. (More precisely, this is true for all primes for which the given Weierstrass equation is minimal.) Then standard properties of the canonical height [14, VIII.9.3] give

$$\hat{h}_K(P) = h(x(P)) + O_{E/K}(1) \geq \log N\mathfrak{d}_P + O_{E/K}(1) \geq \log N\mathfrak{a}_P + O_{E/K}(1).$$

We now resume the proof of Claim 2. We compute

$$\begin{aligned}
\log N\mathfrak{A}_\Gamma(y) &= \sum_{P\in\Gamma(y),\, P\neq O} \log N\mathfrak{a}_P \\
&\leq \sum_{P\in\Gamma(y)} (\hat{h}_K(P) + O_{A/K}(1)) \quad \text{(from (34))} \\
&= \sum_{|n_1|\leq y} \cdots \sum_{|n_r|\leq y} (\hat{h}_K(n_1P_1 + \cdots + n_rP_r) + O_{A/K}(1)) \\
&\leq \sum_{|n_1|\leq y} \cdots \sum_{|n_r|\leq y} (rn_1^2\hat{h}_K(P_1) + \cdots + rn_r^2\hat{h}_K(P_r) + O_{A/K}(1)) \\
&\qquad \text{(since } \hat{h}_K \text{ is a positive definite quadratic form)} \\
&\leq r(2y+1)^{r-1}\frac{y(y+1)(2y+1)}{6}(\hat{h}_K(P_1) + \cdots + \hat{h}_K(P_r)) \\
&\quad + O_{A/K}((2y+1)^r) \\
&\leq (6y)^{r+2}\hat{h}_K(\Gamma) + O_{A/K}((3y)^r).
\end{aligned}$$

This completes the proof of Claim 2.

We now apply Claim 2 with $y = x^{1/r} + 2$ and take the logarithm of both sides to obtain

$$\begin{aligned}
\log\log N\mathfrak{A}_\Gamma(x^{1/r}+2) &\leq \log\{(6x^{1/r}+12)^{r+2}\hat{h}_K(\Gamma) + O_{A/K}((3x^{1/r}+6)^r)\} \\
&= (r+2)\log(6x^{1/r}+12) + \log\left(\hat{h}_K(\Gamma) + O_{A/K}\left(\frac{1}{2^r y^2}\right)\right) \\
&\leq \left(1+\frac{2}{r}\right)\log x + \log\hat{h}_K(\Gamma) + O_{A/K}(r). \qquad (33)
\end{aligned}$$

Substituting (33) into (29) gives (28), which completes the proof of Proposition 3.2. □

We can now use Proposition 3.2 to prove Theorem 3.1 in exactly the same way that Proposition 2.4 was used to prove Theorem 2.1.

Proof (of Theorem 3.1). Let $\tilde{d}_\Gamma(f)$ and $\tilde{D}_\Gamma(x)$ be defined by the formulas (26) in Sec. 2, although now Γ is a subgroup of $A(K)$ rather than a subgroup of K^*. Then

$\tilde{D}_\Gamma(x) \ll \log x$ from Proposition 3.2, so $\lim_{x\to\infty} G(x)\tilde{D}_\Gamma(x) = 0$. This justifies our use of Abel summation in the following calculation:

$$\sum_{\mathfrak{p}} G(f_\Gamma(\mathfrak{p}))\frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \sum_{f=1}^{\infty} \sum_{\substack{\mathfrak{p} \\ f_\Gamma(\mathfrak{p})=f}} G(f)\frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \sum_{f=1}^{\infty} G(f)\tilde{d}_\Gamma(f)$$

$$= -\int_1^\infty \tilde{D}_\Gamma(t)G'(t)\,dt \quad \text{(Abel summation [1, Theorem 4.2])}$$

$$\le -\int_1^\infty \left\{ \log \hat{h}_K(\Gamma) + \left(1+\frac{2}{r}\right)\log t + O_{A/K}(r)\right\} G'(t)\,dt$$

(from (28))

$$= \log \hat{h}_K(\Gamma) + \left(1+\frac{2}{r}\right)\int_1^\infty \frac{G(t)}{t}dt + O_{A,K}(r)\,.$$

(properties $(*)$ of G and integration by parts)

This completes the proof of Theorem 3.1. □

4. Application to Densities

In this section we will apply our earlier estimates to give bounds for the Dirichlet density of various sets. We let K be a number field as usual. For any set $\mathcal{S}$ of non-zero integral ideals of K, we define the *upper Dirichlet density of* $\mathcal{S}$ to be the quantity

$$\delta(\mathcal{S}) = \limsup_{s\to 1^+} \frac{\sum_{\mathfrak{m}\in\mathcal{S}} N\mathfrak{m}^{-s}}{\sum_{\mathfrak{m}\neq(0)} N\mathfrak{m}^{-s}} = \limsup_{s\to 1^+} \frac{s-1}{\kappa_K}\sum_{\mathfrak{m}\in\mathcal{S}} \frac{1}{N\mathfrak{m}^s}\,.$$

(Here κ_K is the residue of $\zeta_K(s)$ at $s=1$, see Sec. 2.)

We can use Theorem 2.1 to estimate the Dirichlet density of the ideals $\mathfrak{m}$ for which $f_\Gamma(\mathfrak{m})$ is small.

Theorem 4.1. *With notation as in Sec. 2, for each real number* $0 \le \theta \le 1$ *we let*

$$\mathcal{S}_\Gamma(\theta) = \{\textit{ideals } \mathfrak{m} \neq (0) \textit{ such that } f_\Gamma(\mathfrak{m}) \le N\mathfrak{m}^\theta\}\,.$$

Then

$$\delta(\mathcal{S}_\Gamma(\theta)) \le e^\gamma\left(1+\frac{1}{r}\right)\theta\,.$$

In particular, if $\Gamma = \langle a\rangle$ *has rank* 1, *then* $\delta(\mathcal{S}_\Gamma(\theta)) \le 2e^\gamma\theta < 57\theta/16$.

Proof. We begin by applying inequality (9) of Theorem 2.1 with $G(x) = x^{-\varepsilon}$ to obtain the estimate

$$\sum_{\mathfrak{m}\neq(0)} \frac{1}{N\mathfrak{m}\cdot f_\Gamma(\mathfrak{m})^\varepsilon} \le e^\gamma\kappa_K\left(1+\frac{1}{r}\right)\varepsilon^{-1} + O_{K,\Gamma}(1)\,. \tag{34}$$

Notice that the big-O constant includes the term depending on Γ, but it is independent of ε.

Now we write $s = 1 + \varepsilon$ and compute

$$\begin{aligned}
\sum_{\mathfrak{m}\in\mathcal{S}_\Gamma(\theta)} \frac{1}{N\mathfrak{m}^s} &= \sum_{\mathfrak{m}\in\mathcal{S}_\Gamma(\theta)} \frac{1}{N\mathfrak{m}} \cdot \frac{1}{N\mathfrak{m}^\varepsilon} \\
&\le \sum_{\mathfrak{m}\in\mathcal{S}_\Gamma(\theta)} \frac{1}{N\mathfrak{m}} \cdot \frac{1}{f_\Gamma(\mathfrak{m})^{\varepsilon/\theta}} \quad \text{since } f_\Gamma(\mathfrak{m}) \le N\mathfrak{m}^\theta \text{ for } \mathfrak{m} \in \mathcal{S}_\Gamma(\theta) \\
&\le \sum_{\mathfrak{m}\neq(0)} \frac{1}{N\mathfrak{m}} \cdot \frac{1}{f_\Gamma(\mathfrak{m})^{\varepsilon/\theta}} \\
&\le e^\gamma \kappa_K \left(1 + \frac{1}{r}\right) \frac{\theta}{\varepsilon} + O_{K,\Gamma}(1) \quad \text{from (34)} \\
&= e^\gamma \kappa_K \left(1 + \frac{1}{r}\right) \frac{\theta}{s-1} + O_{K,\Gamma}(1) .
\end{aligned}$$

Now multiply both sides by $(s-1)/\kappa_K$ and take the lim sup as $s \to 1^+$. The left-hand side gives the upper Dirichlet density, so we find that

$$\delta(\mathcal{S}_\Gamma(\theta)) \le e^\gamma \left(1 + \frac{1}{r}\right)\theta .$$

This completes the proof of Theorem 4.1. (For the last statement, we just note that $2e^\gamma < 57/16$.) □

We can use Theorems 2.1 and 3.1 in a similar fashion to bound the primes for which $f_\Gamma(\mathfrak{p})$ can be small. In this case it is more convenient to use the *upper logarithmic Dirichlet density* of a set of primes $\mathcal{P}$, which is defined to be

$$\tilde{\delta}(\mathcal{P}) = \limsup_{s\to 1^+} \frac{\displaystyle\sum_{\mathfrak{p}\in\mathcal{P}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^s}}{\displaystyle\sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^s}} = \limsup_{s\to 1^+} (s-1) \sum_{\mathfrak{p}\in\mathcal{P}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}^s} .$$

Theorem 4.2. *With notation as in Sec. 2 or 3, let*

$$\mathcal{P}_\Gamma(\theta) = \{\text{primes } \mathfrak{p} \text{ of } K \text{ such that } f_\Gamma(\mathfrak{p}) \le N\mathfrak{p}^\theta\} .$$

(a) *Let $\Gamma \subset K^*$ be a free subgroup of K^* as in Sec. 2. Then*

$$\tilde{\delta}(\mathcal{P}_\Gamma(\theta)) \le \left(1 + \frac{1}{r}\right)\theta .$$

(b) *Let $\Gamma \subset A(K)$ be a free subgroup of the Mordell–Weil group of an abelian variety as in Sec. 3. Then*

$$\tilde{\delta}(\mathcal{P}_\Gamma(\theta)) \le \left(1 + \frac{2}{r}\right)\theta .$$

Remark. Notice that if we take $K = \mathbb{Q}$ and $\Gamma = \langle a \rangle$ in Theorem 4.2(a), we find that the set

$$\{\text{primes } p \text{ such that } f_a(p) \le p^\theta\} \tag{35}$$

has upper logarithmic Dirichlet density at most 2θ. In particular, we can make the density as small as desired by taking θ sufficiently small. Using more advanced methods, Erdös and Murty [5] have shown that if $\theta < 1/2$, then the set (35) has density 0.

Proof. Taking $G(x) = x^{-\varepsilon}$ in inequality (10) of Theorem 2.1 gives

$$\sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p} \cdot f_\Gamma(\mathfrak{p})^\varepsilon} \le \left(1 + \frac{1}{r}\right)\varepsilon^{-1} + O_{K,\Gamma}(1) \tag{36}$$

for the multiplicative group case. Similarly, using $G(x) = x^{-\varepsilon}$ in inequality (27) of Theorem 3.1 gives

$$\sum_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p} \cdot f_\Gamma(\mathfrak{p})^\varepsilon} \le \left(1 + \frac{2}{r}\right)\varepsilon^{-1} + O_{A/K,\Gamma}(1) \tag{37}$$

for the abelian variety case. Now both parts of Theorem 4.2 can be proven in exactly the same way as Theorem 4.1 by using (36) and (37) in place of (34). □

Addendum. After this article was accepted for publication, Carl Pomerance was kind enough to draw our attention to his paper [11] and to another paper of Erdös [3]. In [3], Erdös gives an argument which shows (in our notation) that

$$D_2(x) \le (e^\gamma + o(1)) \log x .$$

Using this estimate in our Theorem 1.1 would allow us to replace the term $2e^\gamma\varepsilon^{-1}$ with $e^\gamma\varepsilon^{-1}$. Using a more elaborate argument, Pomerance [11] proves the existence of a positive constant c so that

$$D_2(x) \le \left(e^\gamma - c + o(1)\right) \log x .$$

Pomerance suggests (private communication) that in this case the correct constant is $\frac{1}{2}$, and more generally that one should have

$$D_a(x) \sim \frac{\phi(a)}{a} \log x \quad \text{as} \quad x \to \infty .$$

Pomerance's article also contains much interesting information concerning the normal, minimal, and maximal orders of $d_a(f)$ as a function of f.

References

1. T. Apostol, *Introduction to Analytic Number Theory*, UTM, Springer-Verlag, 1976.
2. H. Bilharz, *Primdivisoren mit vorgegebener Primitivwürzel*, Math. Annalen **114** (1937), 476–492.
3. P. Erdös, *On some problems of Bellman and a theorem of Romanoff*, J. Chinese Math. Soc. **1** (1951), 409–421.
4. P. Erdös, *On the sum* $\sum_{d|2^n-1} d^{-1}$, Israel J. Math. **9** (1971), 43–48.
5. P. Erdös and R. Murty, *On the order of a* (mod p), unpublished.
6. P. Erdös and P. Turan, *Ein zahlentheoretischer Satz*, Bull. de l'institut de Math. et Mêc. a l'université Konybycheff de Tomsk **I** (1935), 101–103.
7. P. Erdös and P. Turan, *Über die vereinfachung eines Landauschen Satzes*, Bull. de l'institut de Math. et Mêc. a l'université Konybycheff de Tomsk **I** (1935), 144–147.
8. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Oxford Univ. Press, 1975.
9. E. Landau, *Verschärfung eines Romanoffschen Satzes*, Acta Arith. (1935), 43–62.
10. S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.
11. C. Pomerance, *On primitive divisors of Mersenne numbers*, Acta Arithmetica **XLVI** (1986), 355–367.
12. N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. **109** (1934), 668–678.
13. M. Rosen, *A generalization of Mertens' theorem*, preprint, 1995.
14. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, 1986.