ON TELHCIRID'S THEOREM ON ARITHMETIC PROGRESSIONS

GAUTAMI BHOWMIK AND YUTA SUZUKI

Abstract. In this paper, we study the distribution of the digital reverses of prime numbers, which we call the *reversed primes*. We prove the infinitude of reversed primes in any arithmetic progression whenever the base is sufficiently large. We indeed prove an effective Siegel–Walfisz type result for reversed primes, which has a larger admissible level of modulus than the classical case.

1. Introduction

The investigation of various digital properties like sums of digits or representations with missing digits has been popular in the last twenty years. Though the distribution of primes with special digital properties are difficult problems in general, there are some impressive results established on the infinitude of certain primes. In the context of digital problems, we take $g \in \mathbb{Z}_{\geq 2}$ to be the base of the radix representation and write the base-g representation of $n \in \mathbb{N}$ as

$$n = \sum_{0 \leq i < N} n_i g^i \quad \text{with} \quad n_0, \dots, n_{N-1} \in \{0, \dots, g-1\} \text{ and } n_{N-1} \neq 0, \tag{1.1}$$

where we say the integer n or its representation is of the length N.

In this context, Mauduit and Rivat [6] proved that, for any base $g \geq 2$, there are infinitely many primes whose sum of digits satisfy a given congruence condition and Maynard [7] showed that, for any base $g \geq 10$, there are infinitely many primes which do not have one given digit in their digital representation. In this paper, we study the digital *reverse* of integers and establish a new infinitude of such primes.

For the base-g representation (1.1) of a positive integer n, we write

$$\overleftarrow{n} \coloneqq \sum_{0 \leq i < N} n_{N-i-1} g^i = \sum_{0 \leq i < N} n_i g^{N-i-1}, \tag{1.2}$$

and call it the *digital reverse* of n. In particular, we call the digital reverse $\overleftarrow{p}$ of a prime number p a *reversed prime*. Our aim is to obtain *Telhcirid's theorem on arithmetic progressions*. More precisely, we prove, for any sufficiently large base g, the infinitude of reversed primes in a given arithmetic progression except in the degenerate cases where the infinitude does not hold for trivial reasons. We indeed have a quantitative version of this result, an analog of the classical Siegel–Walfisz theorem for reversed primes, which could be called the *Zsiflaw–Legeis theorem*.

We avoid the irregular behavior of the cardinality of integers with special digital properties by considering only the integers of a fixed length N. Namely, for $N \geq 1$, we count integers in the set

$$\mathcal{G}_N \coloneqq \{g^{N-1} \leq n < g^N \mid n \not\equiv 0 \pmod{g}\}$$

2020 *Mathematics Subject Classification.* Primary: 11A63; Secondary: 11N05, 11N69.
Key words and phrases. Prime numbers, arithmetic progressions, reversed radix representation.

of all positive integers of length N with non-zero lowest digit. Note that there is no prime with zero as the lowest digit except g itself. Also, note that the operator $\overleftarrow{*}$ is an involution on $\mathcal{G}_N$. For $a, q \in \mathbb{Z}$ with $q \geq 1$, we then define

$$\overleftarrow{\pi}_N(a,q) \coloneqq \sum_{\substack{p \in \mathcal{G}_N \\ \overleftarrow{p} \equiv a \pmod q}} 1,$$

which is the counting function for reversed primes of length N in the arithmetic progression $a \pmod q$, analogous to the classical $\pi(x,a,q)$ that counts the number of primes up to a real number x in congruence classes. There are a few straightforward connections between the arithmetic properties of a positive integer n and $\overleftarrow{n} \pmod q$. First, for $n \in \mathcal{G}_N$, we have

$$\overleftarrow{n} \equiv g^{N-1} n \pmod{g^2-1} \tag{1.3}$$

since $g^{-1} \equiv g \pmod{g^2-1}$. Second, for $\nu \in \mathbb{N}$, the residue $\overleftarrow{n} \pmod{g^\nu}$ is determined by the first ν leading digits of n. However, besides these, one may find no obvious connection between n and $\overleftarrow{n} \pmod q$. Therefore, by leaving the $(\mathrm{mod}\ (q,(g^2-1)g^N))$ condition as it is and expecting the remaining to behave randomly, one may expect

$$\overleftarrow{\pi}_N(a,q) = \frac{(q,(g^2-1)g^N)}{q} \sum_{\substack{p \in \mathcal{G}_N \\ \overleftarrow{p} \equiv a \pmod{(q,(g^2-1)g^N)}}} 1 + \overleftarrow{R}_N(a,q)$$

with a small remainder term $\overleftarrow{R}_N(a,q)$ provided q is not too large compared to g^N so that (q,g^N) is determined by q and (q,g). Similar to the classical Siegel–Walfisz type theorem for $\pi(x,a,q)$, here we prove a pointwise estimate for the remainder term $\overleftarrow{R}_N(a,q)$.

Theorem 1.1. *For $g, a, q \in \mathbb{Z}$ with $g, q \geq 2$, there exists a constant $c \in (0,1)$ such that*

$$\overleftarrow{\pi}_N(a,q) = \frac{(q,(g^2-1)g^N)}{q} \sum_{\substack{p \in \mathcal{G}_N \\ \overleftarrow{p} \equiv a \pmod{(q,(g^2-1)g^N)}}} 1 + O\bigg(g^N \exp\bigg(-c \cdot \frac{N}{\log q}\bigg)\bigg)$$

provided

$$\alpha_g \coloneqq \frac{\log(\frac{2}{\pi}\log\cot\frac{\pi}{2g} + \frac{1}{g\sin\frac{\pi}{2g}} + 1)}{\log g} < \frac{1}{5} \quad \textit{or equivalently,} \quad g \geq 31699 \tag{1.4}$$

and

$$q \leq \exp\bigg(c \cdot \frac{N}{\log N}\bigg), \tag{1.5}$$

where the constant c and the implicit constant depend only on g and are effectively computable.

For the monotonicity of α_g and the inequality $\alpha_{31699} < \frac{1}{5}$, see Remark 10.4.

By (1.3), if $(a, q, g^2-1) > 1$, a prime p with $\overleftarrow{p} \equiv a \pmod{(q,g^2-1)}$ is a prime divisor of q. Also, the lowest digit of any reversed prime $\overleftarrow{p}$ is non-zero, so there is no prime p with $\overleftarrow{p} \equiv a \pmod{(q,g)}$ if $g \mid (a,q)$. Except for these degenerate cases, where there are only finitely many reversed primes in the arithmetic progression $a \pmod q$, we can use some form of the effective prime number theorem in arithmetic progressions in Theorem 1.1 to obtain the following asymptotic formula.

Corollary 1.2 (Zsiflaw–Legeis theorem). *Under the same setting as in Theorem 1.1, we have*

$$\overleftarrow{\pi}_N(a,q) = \frac{\rho_g(a,q)}{q}\frac{g^N}{\log g^N}\left(1+O\left(\frac{1}{N}\right)\right) + O(g^N\exp(-c\sqrt{N}))$$

provided $g \geq 31699$ *and*

$$q \leq \exp(c\sqrt{N}), \tag{1.6}$$

where $c \in (0,1)$ *is some constant, the coefficient* $\rho_g(a,q)$ *is given by*

$$\rho_g(a,q) \coloneqq \begin{cases} \left(1-\mathbb{1}_{(q,g)|a}\dfrac{(q,g)}{g}\right)\displaystyle\prod_{p|(q,g^2-1)}\left(\frac{p}{p-1}\right) & \text{if } (a,q,g^2-1)=1 \text{ and } g\nmid(a,q), \\ 0 & \text{otherwise} \end{cases}$$

and c *and the implicit constant depend only on* g *and are effectively computable.*

This asymptotic formula implies the following infinitude:

Corollary 1.3 (Telhcirid's theorem on arithmetic progressions). *For* $g,a,q \in \mathbb{Z}$ *with*

$$g \geq 31699, \quad q \geq 1, \quad (a,q,g^2-1)=1, \quad g\nmid(a,q),$$

there are infinitely many primes p *such that* $\overleftarrow{p} \equiv a \pmod{q}$.

It is interesting to observe that if $(a,q,g^2-1)=1$ and $g\nmid(a,q)$, Corollary 1.2 implies

$$\overleftarrow{\pi}_N(a,q) \sim \frac{\rho_g(a,q)}{a}\frac{g^N}{\log g^N} \quad \text{as } N\to\infty$$

in the range

$$q \leq o(\exp(c\sqrt{N})N^{-1}) \quad \text{as } N\to\infty$$

which is much wider than the classical range $q \leq N^A$ for the Siegel–Walfisz theorem with a constant A. (Note that the main variable, say x, of the Siegel–Walfisz theorem corresponds to g^N here and so $\log x$ corresponds to N.) Indeed, from a technical point of view, we do not use the Siegel–Walfisz theorem at all, which makes Theorem 1.1 effective. Note that when we deduce Corollary 1.2 from Theorem 1.1, we use the prime number theorem in arithmetic progressions with the modulus $(q,g^2-1) \ll_g 1$ and so there is no effect of the Siegel zeros provided that we do not care about the dependence of the error term on the base g. One may think of Theorem 1.1 as partial evidence that primality and digital reversing are uncorrelated to each other.

We now mention some preceding results on the digital reverse of primes. A positive integer n is called a *palindrome* if $n = \overleftarrow{n}$. If such an n is a prime, e.g. 101, it is called a *palindromic prime*. The infinitude of palindromic primes is conjectured and remains one of the difficult problems on the digital properties of primes. In this context, Col [2] proved that the density of palindromic primes among palindromes less than x is $\ll (\log x)^{-1}$ as is expected, and improved the earlier result of Banks, Hart and Sakata [1]. We note that these papers contain Siegel–Walfisz type results for palindromes, [1, Corollary 4.5] and [2, Théorème 1].

Further, as in more classical unsolved problems of prime numbers, there exist partial results with almost primes instead of primes for their digital properties. We call an integer n an r-almost prime if n has at most r prime factors counted with multiplicity. For example, Tuxanidy and Panario [11, Theorem 1.4], proved that there are infinitely many palindromic 6-almost primes for any fixed base g, which improved the result of Col [2, Corollaire 2]. There is a similar but weaker conjecture on

the digital property of primes. A prime number p is called a *reversible prime* if $\overleftarrow{p}$ is also a prime. Again it is not known whether there are infinitely many reversible primes. Note that a palindromic prime is automatically a reversible prime and so the infinitude of reversible primes would follow from the infinitude of palindromic primes. A partial result on the infinitude of reversible primes, recently obtained by Dartyge, Martin, Rivat, Shparlinski and Swaenepoel [3], states that there are infinitely many integers n such that both n and $\overleftarrow{n}$ are 8-almost primes in base $g = 2$. The fact that their result on reversible primes is weaker than that of palindromic primes is probably caused by the ineffectiveness of the two-dimensional sieve used there.

One of the main ingredients of Theorem 1.1 is the discrete circle method used by Maynard [8]. The size restriction on the base g is caused by the same reason as in [8], i.e. the weakness of the L^1 bound (Lemma 5.3) for small base g (note that C_g is a constant depending on g in Lemma 5.3 but its M-th power is not negligible) even though our L^1 bound is better than Maynard's bound [8, Lemma 5.1, p. 10]. For the specific technical questions we have built, for example, on exponential sum techniques available in the recent works [2, 3, 5, 6, 11].

2. Notation

Besides those introduced in the main body, we use the following notations.

Throughout the paper, A, H, P, Q, R, X denote positive real numbers, t, u, x, z, α, β, δ, ε, η, θ, κ, λ denote real numbers, d, n, q, r, J, K, L, M, N, ν denote positive integers, i, j, k denote non-negative integers and a, b, h, ℓ, m, v denote integers. The letter p is reserved for prime numbers. The letter c is used for positive constants which can take different values line by line.

For a real number x, we let $e(x) \coloneqq \exp(2\pi i x)$, while $[x]$ denotes the integer part of x, i.e. the greatest integer $\leq x$ and $\|x\| \coloneqq \min_{n\in\mathbb{Z}} |x-n|$ denotes the distance between x and its nearest integer.

For a positive integer q, the symbol

$$\sideset{}{^*}\sum_{a \pmod q}$$

stands for the sum over reduced residues (mod q).

Throughout the paper, $g \geq 2$ is an integer used as the base of radix representation. For a positive integer n with the base-g representation (1.1), we define its digital reverse $\overleftarrow{n}$ by (1.2). We let

$$C_g \coloneqq \frac{2}{\pi}\log\cot\frac{\pi}{2g} + \frac{1}{g\sin\frac{\pi}{2g}} + 1 \quad \text{and} \quad \alpha_g \coloneqq \frac{\log C_g}{\log g} = \frac{\log(\frac{2}{\pi}\log\cot\frac{\pi}{2g} + \frac{1}{g\sin\frac{\pi}{2g}} + 1)}{\log g}. \tag{2.1}$$

For $N \in \mathbb{Z}_{\geq 3}$ and $\alpha, \beta \in \mathbb{R}$, we use the exponential sums

$$F_N(\alpha,\beta) \coloneqq \sum_{n\in\mathcal{G}_N} e(\alpha n + \beta\overleftarrow{n}) \quad \text{and} \quad S_N(\alpha) \coloneqq \sum_{1\leq p<g^N} e(\alpha p).$$

For $N \in \mathbb{Z}_{\geq 3}$, let us write

$$\Phi_N(\alpha,\beta) \coloneqq \prod_{i=1}^{N-2} \phi(\alpha g^i + \beta g^{N-i-1}) \quad \text{with} \quad \phi(\alpha) \coloneqq \sum_{0\leq n<g} e(\alpha n).$$

The arithmetic function $\varphi(n)$ stands for the Euler totient function.

For integers $n_1, \dots, n_r$, we write $(n_1, \dots, n_r)$ for the greatest common divisor of $n_1, \dots, n_r$.

For a logical formula P, we write $\mathbb{1}_P$ for the indicator function of P.

If a theorem or a lemma is stated with the phrase "where the implicit constant depends on $a, b, c, \ldots$", then every implicit constant in the corresponding proof may also depend on $a, b, c, \ldots$ without being specifically mentioned.

3. Auxiliary lemmas on the exponential sum with digital reverse

We first prove some basic properties of the exponential sums $F_N(\alpha, \beta)$ and $\Phi_N(\alpha, \beta)$.

Proposition 3.1. *We have $F_N(\alpha, \beta) = F_N(\beta, \alpha)$ and $\Phi_N(\alpha, \beta) = \Phi_N(\beta, \alpha)$.*

Proof. The first equation is obvious since the digit reverse is indeed an involution on $\mathfrak{G}_N$. The latter one is obtained by changing the variable via $i \rightsquigarrow N - i - 1$ as

$$\Phi_N(\alpha, \beta) = \prod_{i=1}^{N-2} \phi(\alpha g^i + \beta g^{N-i-1}) = \prod_{i=1}^{N-2} \phi(\beta g^i + \alpha g^{N-i-1}) = \Phi_N(\beta, \alpha).$$

Thus, we obtain the assertion. □

Proposition 3.2. *For $N \in \mathbb{Z}_{\geq 3}$, we have*

$$|F_N(\alpha, \beta)| \leq g^2 |\Phi_N(\alpha, \beta)| = g^2 \prod_{i=1}^{N-2} |\phi(\alpha g^i + \beta g^{N-i-1})|.$$

Proof. By writing $n \in \mathfrak{G}_N$ as

$$n = \sum_{0 \leq i < N} n_i g^i \quad \text{with} \quad n_0, \ldots, n_{N-1} \in \{0, \ldots, g-1\} \text{ and } n_0, n_{N-1} \neq 0,$$

we have

$$\begin{aligned}
F_N(\alpha, \beta) &= \sum_{1 \leq n_0 < g} \sum_{0 \leq n_1, \ldots, n_{N-2} < g} \sum_{1 \leq n_{N-1} < g} e\Bigg(\alpha \sum_{i=0}^{N-1} n_i g^i + \beta \sum_{i=0}^{N-1} n_{N-i-1} g^i\Bigg) \\
&= \sum_{1 \leq n_0 < g} \sum_{0 \leq n_1, \ldots, n_{N-2} < g} \sum_{1 \leq n_{N-1} < g} e\Bigg(\alpha \sum_{i=0}^{N-1} n_i g^i + \beta \sum_{i=0}^{N-1} n_i g^{N-i-1}\Bigg) \\
&= \sum_{1 \leq n_0 < g} \sum_{0 \leq n_1, \ldots, n_{N-2} < g} \sum_{1 \leq n_{N-1} < g} \prod_{i=0}^{N-1} e((\alpha g^i + \beta g^{N-i-1}) n_i) \\
&= \Bigg(\sum_{1 \leq n_0 < g} e((\alpha + \beta g^{N-1}) n_0)\Bigg) \times \Bigg(\sum_{1 \leq n_{N-1} < g} e((\alpha g^{N-1} + \beta) n_{N-1})\Bigg) \\
&\qquad \times \prod_{i=1}^{N-2} \Bigg(\sum_{0 \leq n_i < g} e((\alpha g^i + \beta g^{N-i-1}) n_i)\Bigg).
\end{aligned}$$

Bounding the sum over n_0, n_{N-1} trivially gives the inequality. □

Proposition 3.3. *For $M, N \in \mathbb{Z}$ with $3 \le M \le N-1$, we have*
$$\Phi_N(\alpha,\beta) = \Phi_M(\alpha, g^{N-M}\beta)\cdot \Phi_{N-M+2}(g^{M-2}\alpha,\beta).$$

Proof. We have
$$\Phi_N(\alpha,\beta) = \prod_{i=1}^{N-2}\phi(\alpha g^i + \beta g^{N-i-1}) = \prod_{i=1}^{M-2}\phi(\alpha g^i + \beta g^{N-i-1}) \prod_{i=M-1}^{N-2}\phi(\alpha g^i + \beta g^{N-i-1}).$$
We then have
$$\prod_{i=1}^{M-2}\phi(\alpha g^i + \beta g^{N-i-1}) = \prod_{i=1}^{M-2}\phi(\alpha g^i + g^{N-M}\beta g^{M-i-1}) = \Phi_M(\alpha, g^{N-M}\beta)$$
and by changing the variable via $i \rightsquigarrow i+M-2$, we have
$$\prod_{i=M-1}^{N-2}\phi(\alpha g^i + \beta g^{N-i-1}) = \prod_{i=1}^{(N-M+2)-2}\phi(g^{M-2}\alpha g^i + \beta g^{(N-M+2)-i-1}) = \Phi_{N-M+2}(g^{M-2}\alpha,\beta).$$
This completes the proof. □

4. The L^∞-bound

In this section, we prove the pointwise or L^∞-bound for $\Phi_N(\alpha,\beta)$ which will be used for the major arc estimate of $\overleftarrow{R}_N(a,q)$. Some of the following results on exponential sums related to digital problems are known but, for the ease of readers, we reprove most of them.

Proposition 4.1. *We have*
$$\phi(\alpha) = e\left(\frac{g-1}{2}\alpha\right)\frac{\sin \pi g\alpha}{\sin \pi\alpha}.$$

Proof. This is an easy computation with the sum formula for geometric progression. □

Proposition 4.2. *For $\alpha \in \mathbb{R}$ and $u \in [0,g]$, we have*
$$\left|\sum_{u\le n<g} e(n\alpha)\right| \le \min\left(g, \frac{1}{|\sin \pi\alpha|}\right) \quad \text{and so} \quad |\phi(\alpha)| \le \min\left(g, \frac{1}{|\sin \pi\alpha|}\right).$$

Proof. The bound $\le g$ is trivial. For the other bound, we have
$$\left|\sum_{u\le n<g} e(n\alpha)\right| = \left|\frac{e(g\alpha)-e(u\alpha)}{e(\alpha)-1}\right| \le \frac{1}{|\sin \pi\alpha|}.$$
Thus, we obtain the assertion. □

Proposition 4.3. *For $\alpha \in \mathbb{R}$ and $u \in [0, g]$, we have*

$$\left|\sum_{u \le n < g} ne(n\alpha)\right| \le g \min\left(g, \frac{1}{|\sin \pi\alpha|}\right), \quad \text{and so} \quad |\phi'(\alpha)| \le 2\pi g \min\left(g, \frac{1}{|\sin \pi\alpha|}\right).$$

Proof. We have

$$\left|\sum_{u \le n < g} ne(n\alpha)\right| = \left|\sum_{u \le n < g} e(n\alpha) \sum_{1 \le m \le n} 1\right| = \left|\sum_{1 \le m < g} \sum_{\max(m,u) \le n < g} e(n\alpha)\right| \le g \max_{0 \le v < g} \left|\sum_{v \le n < g} e(n\alpha)\right|.$$

Then the assertion follows from Proposition 4.2. □

Proposition 4.4 ([11, Lemma 5.6])**.** *For $\|\alpha\| \le \frac{1}{g}$, we have*

$$|\phi(\alpha)| \le g \exp\left(-\frac{\pi^2}{6}(g^2 - 1)\|\alpha\|^2\right).$$

Proof. For $\|\alpha\| = \frac{1}{g}$, Proposition 4.1 shows $|\phi(\alpha)| = 0$ and the assertion is trivial. Otherwise, by

$$\sin \pi z = \pi z \prod_{n \ge 1} \left(1 - \frac{z^2}{n^2}\right), \quad \log(1 - x) = -\sum_{k=1}^{\infty} \frac{x^k}{k} \quad \text{for } |x| < 1$$

and Proposition 4.1, since $\|\alpha\| < \frac{1}{g}$, we have

$$|\phi(\alpha)| = \frac{\sin \pi g\|\alpha\|}{\sin \pi\|\alpha\|} = g \prod_{n \ge 1} \left(1 - \frac{g^2\|\alpha\|^2}{n^2}\right)\left(1 - \frac{\|\alpha\|^2}{n^2}\right)^{-1} = g \exp\left(-\sum_{k=1}^{\infty} \frac{\zeta(2k)}{k}(g^{2k} - 1)\|\alpha\|^{2k}\right).$$

Since the terms of the above series are non-negative, the assertion follows. □

Proposition 4.5 ([5, Lemme 5])**.** *Let $\delta \in [0, \frac{2}{3g}]$. Then, for $\|\alpha\| \ge \delta$, we have $|\phi(\alpha)| \le |\phi(\delta)|$.*

Proof. We first prove a preliminary estimate. By the infinite product expansion of the sine function,

$$\frac{\sin \pi t}{\sin \frac{2\pi t}{3}} = \frac{3}{2} \prod_{n \ge 1} \frac{1 - \frac{t^2}{n^2}}{1 - \frac{4}{9}\frac{t^2}{n^2}} = \frac{3}{2} \prod_{n \ge 1} \left(\frac{9}{4} - \frac{\frac{5}{4}}{1 - \frac{4}{9}\frac{t^2}{n^2}}\right)$$

so that the function $t \mapsto \frac{\sin \pi t}{\sin \frac{2\pi t}{3}}$ is decreasing for $t \in [0, 1]$. We thus have

$$\left(\sin \frac{\pi}{g}\right)\left|\phi\left(\frac{2}{3g}\right)\right| = \left(\sin \frac{\pi}{g}\right)\frac{\sin \frac{2\pi}{3}}{\sin \frac{2\pi}{3g}} = \left(\sin \frac{2\pi}{3}\right)\frac{\sin \frac{\pi}{g}}{\sin \frac{2\pi}{3g}} \ge \left(\sin \frac{2\pi}{3}\right)\frac{\sin \frac{\pi}{2}}{\sin \frac{\pi}{3}} = 1$$

and so

$$\left|\phi\left(\frac{2}{3g}\right)\right| \ge \left(\sin \frac{\pi}{g}\right)^{-1}. \tag{4.1}$$

Also, for $0 \le t \le \frac{1}{g}$, note that

$$|\phi(t)| = \frac{\sin \pi gt}{\sin \pi t} = g \prod_{n \ge 1} \frac{1 - \frac{g^2t^2}{n^2}}{1 - \frac{t^2}{n^2}}$$

is decreasing in t. We now prove the assertion. When $\delta \le \|\alpha\| \le \frac{1}{g}$, we have

$$|\phi(\alpha)| = |\phi(\|\alpha\|)| \le |\phi(\delta)|$$

by the monotonicity of $|\phi(t)|$ for $t \in [0, \frac{1}{g}]$. When $\frac{1}{g} \le \|\alpha\| \le \frac{1}{2}$, we have

$$|\phi(\alpha)| = |\phi(\|\alpha\|)| = \frac{\sin \pi g\|\alpha\|}{\sin \pi\|\alpha\|} \le (\sin \pi\|\alpha\|)^{-1} \le \left(\sin \frac{\pi}{g}\right)^{-1} \le \left|\phi\left(\frac{2}{3g}\right)\right|$$

from the inequality (4.1). Since $0 \le \delta \le \frac{2}{3g} \le \frac{1}{g}$, we have

$$|\phi(\alpha)| \le \left|\phi\left(\frac{2}{3g}\right)\right| \le |\phi(\delta)|$$

by the monotonicity of $|\phi(t)|$ for $t \in [0, \frac{1}{g}]$. This completes the proof. □

Lemma 4.6 ([11, Lemma 4.8]). *For any $\alpha, \beta, \kappa, \lambda \in \mathbb{R}$, we have*

$$\max(\|\alpha g^{\kappa} + \beta g^{\lambda}\|, \|\alpha g^{\kappa+1} + \beta g^{\lambda-1}\|) \ge \frac{\|\alpha(g^2-1)g^{\kappa}\|}{g+1}.$$

Proof. We have

$$(\alpha g^{\kappa} + \beta g^{\lambda}) - g(\alpha g^{\kappa+1} + \beta g^{\lambda-1}) = -\alpha(g^2-1)g^{\kappa}.$$

By the triangle inequality for $\|*\|$, we have

$$\begin{aligned}\|\alpha(g^2-1)g^{\kappa}\| &\le \|\alpha g^{\kappa} + \beta g^{\lambda}\| + g\|\alpha g^{\kappa+1} + \beta g^{\lambda-1}\| \\ &\le (g+1)\max(\|\alpha g^{\kappa} + \beta g^{\lambda}\|, \|\alpha g^{\kappa+1} + \beta g^{\lambda-1}\|).\end{aligned}$$

Thus the assertion follows. □

Lemma 4.7 (cf. [11, Lemma 4.8]). *For any $\alpha, \beta, \kappa, \lambda \in \mathbb{R}$, we have*

$$|\phi(\alpha g^{\kappa} + \beta g^{\lambda})| \cdot |\phi(\alpha g^{\kappa+1} + \beta g^{\lambda-1})| \le g^2 \exp\left(-\frac{\pi^2}{6}\frac{g-1}{g+1}\|(g^2-1)g^{\kappa}\alpha\|^2\right).$$

Proof. We have

$$\begin{aligned}&|\phi(\alpha g^{\kappa} + \beta g^{\lambda})\phi(\alpha g^{\kappa+1} + \beta g^{\lambda-1})| \\ &= |\phi(\min(\|\alpha g^{\kappa} + \beta g^{\lambda}\|, \|\alpha g^{\kappa+1} + \beta g^{\lambda-1}\|))\phi(\max(\|\alpha g^{\kappa} + \beta g^{\lambda}\|, \|\alpha g^{\kappa+1} + \beta g^{\lambda-1}\|))| \\ &\le g|\phi(\max(\|\alpha g^{\kappa} + \beta g^{\lambda}\|, \|\alpha g^{\kappa+1} + \beta g^{\lambda-1}\|))|.\end{aligned} \tag{4.2}$$

By Lemma 4.6, we have

$$\max(\|\alpha g^{\kappa} + \beta g^{\lambda}\|, \|\alpha g^{\kappa+1} + \beta g^{\lambda-1}\|) \ge \frac{\|(g^2-1)g^{\kappa}\alpha\|}{g+1}$$

and also we have

$$\frac{\|(g^2-1)g^{\kappa}\alpha\|}{g+1} \le \frac{1}{2g} \le \frac{2}{3g}.$$

Thus, by using Proposition 4.5 with

$$\delta := \frac{\|(g^2-1)g^{\kappa}\alpha\|}{g+1}$$

in (4.2), we have

$$|\phi(\alpha g^{\kappa}+\beta g^{\lambda})|\cdot|\phi(\alpha g^{\kappa+1}+\beta g^{\lambda-1})| \le g\left|\phi\left(\frac{\|(g^2-1)g^{\kappa}\alpha\|}{g+1}\right)\right|. \tag{4.3}$$

Since

$$0 \le \frac{\|(g^2-1)g^{\kappa}\alpha\|}{g+1} \le \frac{1}{2},$$

we have

$$\left\|\frac{\|(g^2-1)g^{\kappa}\alpha\|}{g+1}\right\| = \frac{\|(g^2-1)g^{\kappa}\alpha\|}{g+1} \le \frac{1}{g}.$$

Thus, by using Proposition 4.4 in (4.3), we arrive at

$$|\phi(\alpha g^{\kappa}+\beta g^{\lambda})|\cdot|\phi(\alpha g^{\kappa+1}+\beta g^{\lambda-1})| \le g^2\exp\left(-\frac{\pi^2}{6}\frac{g-1}{g+1}\|(g^2-1)g^{\kappa}\alpha\|^2\right).$$

This completes the proof. □

Lemma 4.8 (cf. [3, Lemma 2.7]). *For $\alpha\in\mathbb{R}\setminus\mathbb{Z}$, we have*

$$\|g^{i_0}\alpha\| \ge \frac{1}{g+1} \quad \textit{with} \quad i_0 \coloneqq \left[\frac{\log\frac{g}{(g+1)\|\alpha\|}}{\log g}\right].$$

Proof. We have

$$g^{i_0}\|\alpha\| \ge g^{\frac{\log\frac{g}{(g+1)\|\alpha\|}}{\log g}-1}\|\alpha\| = \frac{1}{g}\frac{g}{(g+1)\|\alpha\|}\cdot\|\alpha\| = \frac{1}{g+1}$$

and

$$g^{i_0}\|\alpha\| \le g^{\frac{\log\frac{g}{(g+1)\|\alpha\|}}{\log g}}\|\alpha\| \le \frac{g}{(g+1)\|\alpha\|}\cdot\|\alpha\| = 1-\frac{1}{g+1}.$$

The result now follows since $\|g^{i_0}\alpha\| = \|g^{i_0}\|\alpha\|\|$. □

Lemma 4.9. *For $N\in\mathbb{Z}_{\ge 4}$ and $\alpha,\beta\in\mathbb{R}$, we have*

$$|\Phi_N(\alpha,\beta)| \le g^{N-2}\exp\left(-\frac{\pi^2}{12}\frac{g-1}{g+1}\sum_{i=1}^{N-3}\|(g^2-1)g^i\alpha\|^2\right).$$

Proof. By pairing the consecutive terms, we have

$$\begin{aligned}|\Phi_N(\alpha,\beta)| &= \prod_{i=1}^{N-2}|\phi(\alpha g^i+\beta g^{N-i-1})|^{\frac{1}{2}}\prod_{i=1}^{N-2}|\phi(\alpha g^i+\beta g^{N-i-1})|^{\frac{1}{2}}\\ &= \prod_{i=1}^{N-2}|\phi(\alpha g^i+\beta g^{N-i-1})|^{\frac{1}{2}}\prod_{i=0}^{N-3}|\phi(\alpha g^{i+1}+\beta g^{(N-i-1)-1})|^{\frac{1}{2}}.\end{aligned}$$

By estimating the terms for $i=0,N-2$ trivially, we get

$$|\Phi_N(\alpha,\beta)| \le g\prod_{i=1}^{N-3}|\phi(\alpha g^i+\beta g^{N-i-1})|^{\frac{1}{2}}|\phi(\alpha g^{i+1}+\beta g^{(N-i-1)-1})|^{\frac{1}{2}}.$$

By Lemma 4.7, we obtain the assertion. □

Lemma 4.10 (L^∞-bound (cf. [3, Lemma 2.8])). *For $N \in \mathbb{Z}$, $\alpha \in \mathbb{R}$ and $k, \ell, d \in \mathbb{Z}$ with*

$$N \geq 4, \quad d \geq 1, \quad (k,d) = 1, \quad d \nmid (g^2-1)g^N k,$$

we have

$$\Phi_N\left(\alpha, \frac{k}{d} + \frac{\ell}{g^3-g}\right) \ll g^N \exp\left(-c_\infty \cdot \frac{N}{\log d}\right)$$

with some constant $c_\infty = c_\infty(g) \in (0,1)$, where the implicit constant depends only on g.

Proof. Note that $d \nmid (g^2-1)g^N k$ implies $d \geq 2$. By Proposition 3.1, Lemma 4.9 and

$$\frac{\ell}{g^3-g}(g^2-1)g^i \in \mathbb{Z} \quad \text{for } i \geq 1,$$

we have

$$\begin{aligned} \left|\Phi_N\left(\alpha, \frac{k}{d} + \frac{\ell}{g^3-g}\right)\right| &= \left|\Phi_N\left(\frac{k}{d} + \frac{\ell}{g^3-g}, \alpha\right)\right| \\ &\leq g^{N-2} \exp\left(-\frac{\pi^2}{12}\frac{g-1}{g+1}\sum_{i=1}^{N-3}\left\|\frac{(g^2-1)g^i k}{d}\right\|^2\right). \end{aligned} \tag{4.4}$$

Let

$$J \coloneqq 1 + \left\lceil \frac{\log \frac{gd}{g+1}}{\log g} \right\rceil \geq 1, \quad L \coloneqq \left\lceil \frac{N-3}{J} \right\rceil \quad \text{and} \quad \alpha_\ell \coloneqq \frac{(g^2-1)g^{\ell J+1}k}{d}.$$

We then have

$$\sum_{i=1}^{N-3}\left\|\frac{(g^2-1)g^i k}{d}\right\|^2 \geq \sum_{0\leq \ell < L}\sum_{\ell J < i \leq (\ell+1)J}\left\|\frac{(g^2-1)g^i k}{d}\right\|^2 \geq \sum_{0\leq \ell < L}\sum_{0 \leq i < J}\|g^i \alpha_\ell\|^2. \tag{4.5}$$

Since $d \nmid (g^2-1)g^N k$, we have $\alpha_\ell \notin \mathbb{Z}$ for all $\ell \in \{0, \dots, L-1\}$ and so Lemma 4.8 is applicable to the inner sum with $\alpha \coloneqq \alpha_\ell$. Also, the same observation implies $\|\alpha_\ell\| \geq \frac{1}{d}$. For $0 \leq \ell < L$, let

$$i_{0,\ell} \coloneqq \left\lceil \frac{\log \frac{g}{(g+1)\|\alpha_\ell\|}}{\log g} \right\rceil.$$

We then have

$$0 \leq i_{0,\ell} \leq \left\lceil \frac{\log \frac{gd}{(g+1)}}{\log g} \right\rceil = J - 1.$$

Therefore, we can pick up the contribution of $i = i_{0,\ell}$ and use Lemma 4.8 in (4.5) to get

$$\sum_{i=1}^{N-3}\left\|\frac{(g^2-1)g^i k}{d}\right\|^2 \geq \sum_{0\leq \ell < L}\|g^{i_{0,\ell}}\alpha_\ell\|^2 \geq \frac{L}{(g+1)^2}. \tag{4.6}$$

By using the estimate

$$L \geq \frac{N-3}{J} - 1 \geq \frac{1}{4}\frac{N}{J} - 1 \geq \frac{1}{4}\frac{N}{1 + \frac{\log d}{\log 2}} - 1 \geq \frac{\log 2}{8}\frac{N}{\log d} - 1$$

in (4.6) and combining it with (4.4), we obtain the result. □

Lemma 4.11 (L^∞-bound). *For $N, \ell, q \in \mathbb{Z}$ with $N \geq 4$ and $q \geq 1$, we have*

$$\frac{1}{q} \sum_{\substack{0 \leq k < q \\ q \nmid (g^2-1)g^N k}} \left| \Phi_N\left(\alpha, \frac{k}{q} + \frac{\ell}{g^3 - g}\right) \right| \ll g^N \exp\left(-c_\infty \cdot \frac{N}{\log q}\right)$$

with some constant $c_\infty = c_\infty(g) \in (0,1)$, where the implicit constant depends only on g.

Proof. By classifying the values of (k, q), we have

$$\frac{1}{q} \sum_{\substack{0 \leq k < q \\ q \nmid (g^2-1)g^N k}} \left| \Phi_N\left(\alpha, \frac{k}{q} + \frac{\ell}{g^3 - g}\right) \right| = \frac{1}{q} \sum_{d \mid q} \sum_{\substack{0 \leq k < q \\ q \nmid (g^2-1)g^N k \\ (k,q) = d}} \left| \Phi_N\left(\alpha, \frac{k}{q} + \frac{\ell}{g^3 - g}\right) \right|.$$

By changing variable via $d \rightsquigarrow \frac{q}{d}$ and $k \rightsquigarrow (\frac{q}{d}) \cdot k$, we have

$$\frac{1}{q} \sum_{\substack{0 \leq k < q \\ q \nmid (g^2-1)g^N k}} \left| \Phi_N\left(\alpha, \frac{k}{q} + \frac{\ell}{g^3 - g}\right) \right| = \frac{1}{q} \sum_{d \mid q} \sideset{}{^*}\sum_{\substack{k \pmod d \\ d \nmid (g^2-1)g^N k}} \left| \Phi_N\left(\alpha, \frac{k}{d} + \frac{\ell}{g^3 - g}\right) \right|.$$

By Lemma 4.10, we have

$$\frac{1}{q} \sum_{\substack{0 \leq k < q \\ q \nmid (g^2-1)g^N k}} \left| \Phi_N\left(\alpha, \frac{k}{q} + \frac{\ell}{g^3 - g}\right) \right| \ll g^N \exp\left(-c_\infty \cdot \frac{N}{\log q}\right) \frac{1}{q} \sum_{d \mid q} \varphi(d) \ll g^N \exp\left(-c_\infty \cdot \frac{N}{\log q}\right).$$

This completes the proof. □

5. The L^1-bound

In this section we prove several L^1-bounds for $\Phi_N(\alpha, \beta)$, which will be used as ingredients for the minor arc estimate of $\overleftarrow{R}_N(a, q)$. We first consider the L^1-moment taken over fractions having some power of g as the denominator. We shall use the constant

$$C_g \coloneqq \frac{2}{\pi} \log \cot \frac{\pi}{2g} + \frac{1}{g \sin \frac{\pi}{2g}} + 1$$

defined in (2.1). Note that we have

$$C_g > 1 \tag{5.1}$$

since $\frac{\pi}{2g} \in (0, \frac{\pi}{4}]$.

Lemma 5.1 (cf. [6, Lemme 6]). *For $g \in \mathbb{Z}_{\geq 2}$ and $\theta \in \mathbb{R}$, we have*

$$\sum_{0 \leq h < g} \min\left(g, \frac{1}{|\sin \pi(\frac{h}{g} + \theta)|}\right) \leq C_g g.$$

Proof. This follows from Lemme 6 of [6] but, for the ease of readers, we give a complete proof here in the form that is enough for us. Let us write S for the left-hand side of the assertion. Since we can think of S as a sum over the residues $h \pmod g$, we can shift h to shift θ to a real number $\frac{\delta}{g}$

with $|\delta| \le \frac{1}{2}$. By changing $h \pmod g$ by $-h \pmod g$ if necessary, we can further assume $\delta \in [0, \frac{1}{2}]$. By bounding the term with $h = 0$ by g and by noting that $0 < \frac{h+\delta}{g} < 1$ for $1 \le h < g$, we have

$$S \le \sum_{1 \le h \le g-1} \frac{1}{\sin \pi(\frac{h+\delta}{g})} + g \le \sum_{1 \le h \le g-2} \frac{1}{\sin \pi(\frac{h+\delta}{g})} + \frac{1}{\sin \pi(\frac{1-\delta}{g})} + g.$$

Since the function $x \mapsto \frac{1}{\sin \pi x}$ is convex downwards for $0 < x < 1$, we have

$$\frac{1}{\sin \pi(\frac{h+\delta}{g})} \le \int_{h-\frac{1}{2}}^{h+\frac{1}{2}} \frac{du}{\sin \pi(\frac{u+\delta}{g})} \quad \text{for} \quad 1 \le h \le g-2$$

and so

$$S \le \int_{\frac{1}{2}}^{g-\frac{3}{2}} \frac{du}{\sin \pi(\frac{u+\delta}{g})} + \frac{1}{\sin \pi(\frac{1-\delta}{g})} + g =: S(\delta).$$

By the convexity of the function $x \mapsto \frac{1}{\sin \pi x}$, the function $S(\delta)$ is convex downwards with respect to $\delta \in [0, \frac{1}{2}]$. Thus, its maximum of $S(\delta)$ for $\delta \in [0, \frac{1}{2}]$ is taken at either $\delta = 0$ or $\delta = \frac{1}{2}$. We have

$$\begin{aligned} S(\tfrac{1}{2}) - S(0) &= \frac{1}{\sin \frac{\pi}{2g}} - \frac{1}{\sin \frac{\pi}{g}} + \int_{g-\frac{3}{2}}^{g-1} \frac{du}{\sin \frac{\pi u}{g}} - \int_{\frac{1}{2}}^{1} \frac{du}{\sin \frac{\pi u}{g}} \\ &\ge \frac{1}{\sin \frac{\pi}{2g}} - \frac{1}{\sin \frac{\pi}{g}} + \frac{1}{2\sin \frac{3\pi}{2g}} - \frac{1}{2\sin \frac{\pi}{2g}} \\ &= \frac{1}{2\sin \frac{\pi}{2g}} + \frac{1}{2\sin \frac{3\pi}{2g}} - \frac{1}{\sin \frac{\pi}{g}} \ge 0, \end{aligned}$$

where once again we used the convexity of $x \mapsto \frac{1}{\sin \pi x}$ in the last inequality. This shows

$$S \le S(\tfrac{1}{2}) = \int_1^{g-1} \frac{du}{\sin \frac{\pi u}{g}} + \frac{1}{\sin \frac{\pi}{2g}} + g = \frac{2}{\pi} g \log \cot \frac{\pi}{2g} + \frac{1}{\sin \frac{\pi}{2g}} + g = C_g g$$

where we have used $(\log \tan \frac{x}{2})' = \frac{1}{\sin x}$. This completes the proof. □

The next lemma is comparable to Lemma 5.1 of [8]. Our sum is simpler in the sense that we have complete exponential sums (mod g) though we have to insert a new extra shift θ_i. We also avoid taking the maximum over the less significant digits.

Lemma 5.2. *For $M \in \mathbb{Z}_{\ge 2}$ and a sequence of real numbers $(\theta_i)_{i=1}^{M-2}$, we have*

$$\sum_{0 \le h < g^M} \prod_{i=1}^{M-2} \min\Big(g, \frac{1}{|\sin \pi(hg^{-(i+1)} + \theta_i)|}\Big) \le (C_g g)^M.$$

Proof. Let S be the left-hand side of the inequality. By letting

$$h = ng^{M-1} + h_- \quad \text{with} \quad n \in \{0, \dots, g-1\} \quad \text{and} \quad h_- \in [0, g^{M-1}),$$

we can rewrite S as

$$S = \sum_{0 \le h_- < g^{M-1}} \sum_{0 \le n < g} \prod_{i=1}^{M-2} \min\Big(g, \frac{1}{|\sin \pi(ng^{M-i-2} + h_- g^{-(i+1)} + \theta_i)|}\Big).$$

However, in the above product, ng^{M-i-2} is always an integer and so

$$\begin{aligned} S &= \sum_{0\le h_-<g^{M-1}} \sum_{0\le n<g} \prod_{i=1}^{M-2} \min\biggl(g, \frac{1}{|\sin\pi(h_-g^{-(i+1)}+\theta_i)|}\biggr) \\ &= g \sum_{0\le h_-<g^{M-1}} \prod_{i=1}^{M-2} \min\biggl(g, \frac{1}{|\sin\pi(h_-g^{-(i+1)}+\theta_i)|}\biggr). \end{aligned}$$

Since $C_g > 1$ by (5.1), it thus suffices to show

$$S_M \coloneqq \sum_{0\le h<g^M} \prod_{i=1}^{M-1} \min\biggl(g, \frac{1}{|\sin\pi(hg^{-(i+1)}+\theta_i)|}\biggr) \le (C_g g)^M \tag{5.2}$$

for $M \in \mathbb{Z}_{\ge 1}$ and $(\theta_i)_{i=1}^{M-1}$. We use induction on $M \in \mathbb{Z}_{\ge 1}$.

We first consider the initial case $M = 1$. In this case, we have

$$S_1 = \sum_{0\le h<g} 1 = g \le C_g g$$

since $C_g > 1$ by (5.1). This proves (5.2) for the initial case $M = 1$.

We next assume the M-th case of (5.2) with $M \ge 1$ and show the $(M+1)$-th case of (5.2). Let us express the summation variable $h \in [0, g^{M+1})$ as

$$h = ng^M + h_- \quad \text{with} \quad n \in \{0, \dots, g-1\} \text{ and } h_- \in [0, g^M) \cap \mathbb{Z}.$$

We then have

$$S_{M+1} = \sum_{0\le h_-<g^M} \sum_{0\le n<g} \prod_{i=1}^{M} \min\biggl(g, \frac{1}{|\sin\pi(ng^{M-(i+1)}+h_-g^{-(i+1)}+\theta_i)|}\biggr).$$

In the above product, we have $ng^{M-(i+1)} \in \mathbb{Z}$ for $i = 1, \dots, M-1$. This gives

$$\begin{aligned} S_{M+1} = \sum_{0\le h_-<g^M} \prod_{i=1}^{M-1} &\min\biggl(g, \frac{1}{|\sin\pi(hg^{-(i+1)}+\theta_i)|}\biggr) \\ &\times \sum_{0\le n<g} \min\biggl(g, \frac{1}{|\sin\pi(ng^{-1}+h_-g^{-(M+1)}+\theta_M)|}\biggr). \end{aligned}$$

We can then apply Lemma 5.1 with $\theta = h_-g^{-(M+1)} + \theta_M$ to the inner sum. This gives

$$S_{M+1} \le C_g g \sum_{0\le h_-<g^M} \prod_{i=1}^{M-1} \min\biggl(g, \frac{1}{|\sin\pi(h_-g^{-(i+1)}+\theta_i)|}\biggr) \le (C_g g)^{M+1}$$

by the induction hypothesis. This completes the proof. □

Lemma 5.3 (Discrete L^1-bound). *For $M \in \mathbb{Z}_{\ge 3}$, $\theta, \beta \in \mathbb{R}$, we have*

$$\sum_{0\le h<g^M} \biggl|\Phi_M\biggl(\frac{h}{g^M}+\theta, \beta\biggr)\biggr| \le (C_g g)^M.$$

Proof. By Proposition 3.1, we have

$$\begin{aligned}\sum_{0\le h<g^M}\left|\Phi_M\left(\frac{h}{g^M}+\theta,\beta\right)\right| &= \sum_{0\le h<g^M}\left|\Phi_M\left(\beta,\frac{h}{g^M}+\theta\right)\right| \\ &\le \sum_{0\le h<g^M}\prod_{i=1}^{M-2}\left|\phi\left(\left(\frac{h}{g^M}+\theta\right)g^{M-i-1}+\beta g^i\right)\right| \\ &= \sum_{0\le h<g^M}\prod_{i=1}^{M-2}|\phi(hg^{-(i+1)}+\theta_i)|,\end{aligned}$$

where $\theta_i \coloneqq \theta g^{M-i-1}+\beta g^i$. By using Proposition 4.2 and Lemma 5.2, we have

$$\sum_{0\le h<g^M}\left|\Phi_M\left(\frac{h}{g^M}+\theta,\beta\right)\right| \le \sum_{0\le h<g^M}\prod_{i=1}^{M-2}\min\left(g,\frac{1}{|\sin\pi(hg^{-(i+1)}+\theta_i)|}\right) \le (C_g g)^M.$$

This completes the proof. □

Lemma 5.4 (Continuous L^1-bound). *For $M\in\mathbb{Z}_{\ge 3}$ and $\beta\in\mathbb{R}$, we have*

$$\int_0^1 |\Phi_M(\alpha,\beta)|d\alpha \le C_g^M.$$

Proof. We decompose the interval into g^M parts to obtain

$$\begin{aligned}\int_0^1 |\Phi_M(\alpha,\beta)|d\alpha &= \sum_{0\le h<g^M}\int_0^{\frac{1}{g^M}}\left|\Phi_M\left(\frac{h}{g^M}+\theta,\beta\right)\right|d\theta \\ &= \int_0^{\frac{1}{g^M}}\sum_{0\le h<g^M}\left|\Phi_M\left(\frac{h}{g^M}+\theta,\beta\right)\right|d\theta.\end{aligned}$$

By Lemma 5.3, we obtain

$$\int_0^1 |\Phi_M(\alpha,\beta)|d\alpha \le (C_g g)^M\int_0^{\frac{1}{g^M}} d\theta = C_g^M.$$

This completes the proof. □

Lemma 5.5 (Discrete L^1-bound for derivative). *For $M\in\mathbb{Z}_{\ge 3}$, $\beta\in\mathbb{R}$, we have*

$$\sum_{0\le h<g^M}\left|\frac{\partial\Phi_M}{\partial\alpha}\left(\frac{h}{g^M}+\theta,\beta\right)\right| \le 2\pi g^M(C_g g)^M.$$

Proof. Recall the definition

$$\Phi_M(\alpha,\beta)=\prod_{i=1}^{M-2}\phi(\alpha g^i+\beta g^{M-i-1}).$$

By taking its derivative with respect to α, we have

$$\frac{\partial \Phi_M}{\partial \alpha}(\alpha,\beta) = \sum_{i=1}^{M-2} g^i \phi'(\alpha g^i + \beta g^{M-i-1}) \prod_{\substack{j=1\\ i\neq j}}^{M-2} \phi(\alpha g^j + \beta g^{M-j-1}).$$

By using Proposition 4.2 and Proposition 4.3, we have

$$\begin{aligned}\left|\frac{\partial \Phi_M}{\partial \alpha}(\alpha,\beta)\right| &\le 2\pi \sum_{i=0}^{M-2} g^{i+1} \prod_{j=1}^{M-2} \min\left(g, \frac{1}{|\sin \pi(\alpha g^j + \beta g^{M-j-1})|}\right)\\ &\le 2\pi g^M \prod_{i=1}^{M-2} \min\left(g, \frac{1}{|\sin \pi(\alpha g^i + \beta g^{M-i-1})|}\right)\\ &= 2\pi g^M \prod_{i=1}^{M-2} \min\left(g, \frac{1}{|\sin \pi(\alpha g^{M-i-1} + \beta g^i)|}\right).\end{aligned}$$

By using this estimate, we have

$$\begin{aligned}\sum_{0\le h<g^M} \left|\frac{\partial \Phi_M}{\partial \alpha}\left(\frac{h}{g^M}+\theta,\beta\right)\right| &\le 2\pi g^M \sum_{0\le h<g^M} \prod_{i=1}^{M-2} \min\left(g, \frac{1}{|\sin \pi(\frac{h}{g^M}+\theta) g^{M-i-1} + \beta g^i)|}\right)\\ &= 2\pi g^M \sum_{0\le h<g^M} \prod_{i=1}^{M-2} \min\left(g, \frac{1}{|\sin \pi(h g^{-(i+1)} + \theta_i)|}\right)\end{aligned}$$

with $\theta_i \coloneqq \theta g^{M-i-1} + \beta g^i$. Then the assertion follows from Lemma 5.2. □

Lemma 5.6 (Continuous L^1-bound for derivative). *For $M \in \mathbb{Z}_{\ge 3}$ and $\beta \in \mathbb{R}$, we have*

$$\int_0^1 \left|\frac{\partial \Phi_M}{\partial \alpha}(\alpha,\beta)\right| d\alpha \le 2\pi g^M C_g^M.$$

Proof. We decompose the interval into g^M parts to obtain

$$\begin{aligned}\int_0^1 \left|\frac{d\Phi_M}{d\alpha}(\alpha,\beta)\right| d\alpha &= \sum_{0\le h<g^M} \int_0^{\frac{1}{g^M}} \left|\frac{\partial \Phi_M}{\partial \alpha}\left(\frac{h}{g^M}+\theta,\beta\right)\right| d\theta\\ &= \int_0^{\frac{1}{g^M}} \sum_{0\le h<g^M} \left|\frac{\partial \Phi_M}{\partial \alpha}\left(\frac{h}{g^M}+\theta,\beta\right)\right| d\theta.\end{aligned}$$

By Lemma 5.5, we obtain

$$\int_0^1 \left|\frac{\partial \Phi_M}{\partial \alpha}(\alpha,\beta)\right| d\alpha \le 2\pi g^M (C_g g)^M \int_0^{\frac{1}{g^M}} d\theta = 2\pi g^M C_g^M.$$

This completes the proof. □

6. Large sieve estimates

In this section we consider the L^1-moment taken over Farey fractions. Our main tool, as in the estimation of various large sieves, is the Gallagher–Sobolev inequality.

Lemma 6.1 (Galllagher–Sobolev inequality). *Let $f\colon [0,1] \to \mathbb{C}$ be a function of class C^1 of period 1, $\delta > 0$ and $(\alpha_i)_{i=1}^R$ be a sequence of real numbers which is δ-spaced* (mod 1)*, i.e.*

$$\|\alpha_i - \alpha_j\| \geq \delta \quad \text{for any} \quad i, j \in \{1, \dots, R\} \text{ with } i \neq j.$$

We then have

$$\sum_{i=1}^{R} |f(\alpha_i)| \leq \frac{1}{\delta} \int_0^1 |f(\alpha)| d\alpha + \frac{1}{2} \int_0^1 |f'(\alpha)| d\alpha.$$

Proof. See Lemma 1.2 of [9, p. 2]. □

Lemma 6.2 (Large sieve estimate). *For $M \in \mathbb{N}_{\geq 3}$, $R, \theta, \beta \in \mathbb{R}$ with $R \geq 2$, we have*

$$\sum_{r \leq R} \sideset{}{^*}\sum_{b \pmod r} \max_{|\eta| \leq \frac{1}{4}R^{-2}} \left| \Phi_M\left(\frac{b}{r} + \theta + \eta, \beta\right) \right| \ll (g^M + R^2) C_g^M.$$

Proof. For b, r appearing in the left-hand side, by the continuity in η, we can take $\eta_{b,r}$ such that

$$\max_{|\eta| \leq \frac{1}{4}R^{-2}} \left| \Phi_M\left(\frac{b}{r} + \theta + \eta, \beta\right) \right| = \left| \Phi_M\left(\frac{b}{r} + \theta + \eta_{b,r}, \beta\right) \right| \quad \text{and} \quad |\eta_{b,r}| \leq \tfrac{1}{4}R^{-2}. \tag{6.1}$$

For any two distinct (b, r) and (b', r') in the above sum and $m \in \mathbb{Z}$,

$$\begin{aligned} \left| \left(\frac{b}{r} + \theta + \eta_{b,r}\right) - \left(\frac{b'}{r'} + \theta + \eta_{b',r'}\right) - m \right| &\geq \left| \frac{b}{r} - \frac{b'}{r'} - m \right| - |\eta_{b,r}| - |\eta_{b',r'}| \\ &\geq \frac{1}{rr'} - \frac{1}{2R^2} \geq \frac{1}{2R^2} \end{aligned}$$

and so the real numbers

$$\frac{b}{r} + \theta + \eta_{b,r}$$

appearing in the sum are $\frac{1}{2}R^{-2}$-spaced (mod 1). Thus, Lemma 6.1 and (6.1) give

$$\begin{aligned} \sum_{r \leq R} \sideset{}{^*}\sum_{b \pmod r} \max_{|\eta| \leq \frac{1}{4}R^{-2}} \left| \Phi_M\left(\frac{b}{r} + \theta + \eta, \beta\right) \right| &= \sum_{r \leq R} \sideset{}{^*}\sum_{b \pmod r} \left| \Phi_M\left(\frac{b}{r} + \theta + \eta_{b,r}, \beta\right) \right| \\ &\ll R^2 \int_0^1 |\Phi_M(\alpha, \beta)| d\alpha + \int_0^1 \left| \frac{\partial \Phi_M}{\partial \alpha}(\alpha, \beta) \right| d\alpha. \end{aligned}$$

Then the assertion follows from Lemma 5.4 and Lemma 5.6. □

7. Hybrid bound

We now combine the results of Section 5 and Section 6 to obtain a hybrid L^1-bound.

Lemma 7.1 (Hybrid bound). *For $N \in \mathbb{Z}_{\geq 8}$, $R \geq 1$, $H \geq 4g^8$ with*

$$R^2 H \leq 4g^N$$

and $\beta \in \mathbb{R}$, we have

$$\sum_{r \leq R} \sideset{}{^*}\sum_{b \pmod r} \sum_{\substack{g^N|\eta| \leq H \\ \frac{g^N b}{r} + g^N \eta \in \mathbb{Z}}} \left| \Phi_N\left(\frac{b}{r} + \eta, \beta\right)\right| \ll g^N (R^2 H)^{\alpha_g},$$

where the exponent α_g is given by

$$\alpha_g \coloneqq \frac{\log C_g}{\log g} = \frac{\log(\frac{2}{\pi}\log\cot\frac{\pi}{2g} + \frac{1}{g\sin\frac{\pi}{2g}} + 1)}{\log g}$$

and the implicit constant depends only on g.

Proof. Let S be the left-hand side of the assertion. We take $L, M \in \mathbb{Z}$ chosen later such that

$$3 \leq L \leq N - M + 1 \quad \text{and} \quad 3 \leq M \leq N - 1. \tag{7.1}$$

We then decompose Φ_N by using Proposition 3.3 as

$$\begin{aligned}
&\Phi_N\left(\frac{b}{r} + \eta, \beta\right) \\
&= \Phi_{N-M+2}\left(\frac{b}{r} + \eta, g^{M-2}\beta\right)\Phi_M\left(g^{N-M}\left(\frac{b}{r} + \eta\right), \beta\right) \\
&= \Phi_L\left(\frac{b}{r} + \eta, g^{N-L}\beta\right)\Phi_{N-(L+M)+4}\left(g^{L-2}\left(\frac{b}{r} + \eta\right), g^{M-2}\beta\right)\Phi_M\left(g^{N-M}\left(\frac{b}{r} + \eta\right), \beta\right).
\end{aligned}$$

By using the trivial bound

$$\Phi_{N-(L+M)+4}\left(g^{L-2}\left(\frac{b}{r} + \eta\right), g^{M-2}\beta\right) \ll g^{N-(L+M)}$$

and writing $\widetilde{\beta} \coloneqq g^{N-L}\beta$, we have

$$S \ll g^{N-(L+M)} \sum_{r \leq R} \sideset{}{^*}\sum_{b \pmod r} \sum_{\substack{g^N|\eta| \leq H \\ \frac{g^N b}{r} + g^N \eta \in \mathbb{Z}}} \left|\Phi_L\left(\frac{b}{r} + \eta, \widetilde{\beta}\right)\right| \left|\Phi_M\left(g^{N-M}\left(\frac{b}{r} + \eta\right), \beta\right)\right|. \tag{7.2}$$

In this sum, by the assumption $R^2 H \leq 4g^N$, we have

$$|\eta| \leq H g^{-N} \leq 4R^{-2}.$$

We can thus estimate (7.2) as

$$S \ll g^{N-(L+M)} \sum_{r \leq R} \sideset{}{^*}\sum_{b \pmod r} \max_{|\varepsilon| \leq 4R^{-2}} \left|\Phi_L\left(\frac{b}{r} + \varepsilon, \widetilde{\beta}\right)\right| S(b, r), \tag{7.3}$$

where

$$S(b, r) \coloneqq \sum_{\substack{g^N|\eta| \leq H \\ \frac{g^N b}{r} + g^N \eta \in \mathbb{Z}}} \left|\Phi_M\left(g^{N-M}\left(\frac{b}{r} + \eta\right), \beta\right)\right|.$$

In the sum $S(b,r)$, we change variable from η to $h \coloneqq \frac{g^N b}{r} + g^N \eta \in \mathbb{Z}$. This gives

$$S(b,r) = \sum_{|h - \frac{g^N b}{r}| \le H} \left| \Phi_M\left(\frac{h}{g^M}, \beta\right)\right|.$$

We then partition the sum over h into the sums over subintervals of length g^M and apply the L^1 bound (Lemma 5.3). Since there are $\ll Hg^{-M} + 1$ such subintervals, we then obtain

$$S(b,r) \ll (1 + Hg^{-M}) \sum_{0 \le h < g^M} \left| \Phi_M\left(\frac{h}{g^M}, \beta\right)\right| \le (1 + Hg^{-M})(C_g g)^M.$$

On inserting this bound into (7.3), we get

$$S \ll g^{N-L}(1 + Hg^{-M}) C_g^M \sum_{r \le R} \sideset{}{^*}\sum_{b \pmod r} \max_{|\varepsilon| \le 4R^{-2}} \left| \Phi_L\left(\frac{b}{r} + \varepsilon, \widetilde{\beta}\right)\right|. \tag{7.4}$$

In (7.4), for each (b,r), we can take a real number $\varepsilon_{b,r}$ with

$$\sup_{|\varepsilon| \le R^{-2}} \left| \Phi_L\left(\frac{b}{r} + \varepsilon, \widetilde{\beta}\right)\right| = \left| \Phi_L\left(\frac{b}{r} + \varepsilon_{b,r}, \widetilde{\beta}\right)\right| \quad \text{with} \quad |\varepsilon_{b,r}| \le 4R^{-2}.$$

By classifying the terms according to which one of the intervals

$$\left[\frac{i}{4}R^{-2}, \frac{i+1}{4}R^{-2}\right] \quad \text{for } i \in \{-16, -15, \dots, +15, +15\}$$

contains $\varepsilon_{b,r}$, (7.4) can be bounded as

$$S \ll g^{N-L}(1 + Hg^{-M}) C_g^M \max_{|i| \le 16} \sum_{r \le R} \sideset{}{^*}\sum_{b \pmod r} \max_{|\varepsilon| \le \frac{1}{4}R^{-2}} \left| \Phi_L\left(\frac{b}{r} + \frac{i}{4}R^{-2} + \varepsilon, \widetilde{\beta}\right)\right|.$$

By Lemma 6.2, we arrive at

$$\begin{aligned} S &\ll g^{N-L}(1 + Hg^{-M})(g^L + R^2) C_g^{M+L} \\ &\ll g^N \times \max(1, R^2 g^{-L}) C_g^L \times \max(1, Hg^{-M}) C_g^M. \end{aligned} \tag{7.5}$$

When

$$\frac{C_g}{g} < 1 \tag{7.6}$$

does not hold, the bound (7.5) is weaker than the trivial bound

$$S \ll g^N R^2 H.$$

We may thus assume (7.6) to optimize our L, M. By $C_g > 1$ and (7.6), the general quantity

$$\max(1, Xg^{-K}) C_g^K \quad \text{with} \quad X \ge 1 \text{ and } K \in \mathbb{N} \tag{7.7}$$

is decreasing for $g^K \le X$ and increasing for $g^K \ge X$. Thus, (7.7) is minimized when $g^K \asymp X$. Therefore, to minimize (7.5), we try to take L, M so that

$$g^L \asymp R^2 \quad \text{and} \quad g^M \asymp H.$$

By the assumptions $R \ge 1$, $H \ge 4g^8$ and $R^2 H \le 4g^N$, we can take $M \in \mathbb{Z}_{\ge 6}$ with (7.1) such that

$$4g^{M+2} \le H < 4g^{M+3}. \tag{7.8}$$

We shall then take $L \in \mathbb{N}$ by

$$g^{L-3} \le R^2 < g^{L-2}. \tag{7.9}$$

Combined with (7.8), this choice is in the range (7.1) since

$$R \ge 1 \text{ and } 4g^{L+M-1} \le R^2 H \le 4g^N \quad \text{so that} \quad 3 \le L \le N-M+1 \text{ and } 6 \le M \le N-2$$

by the assumptions $R \ge 1$ and $R^2 H \le 4g^N$. By (7.5), we then have

$$S \ll g^N C_g^{M+L}. \tag{7.10}$$

By (7.8) and (7.9), we have

$$M = \frac{\log H}{\log g} + O(1) \quad \text{and} \quad L = \frac{\log R^2}{\log g} + O(1)$$

and so, recalling the definition of C_g, (7.10) can be bounded as

$$S \ll g^N \exp\biggl(\frac{\log C_g}{\log g} \log R^2 H\biggr) = g^N (R^2 H)^{\alpha_g}.$$

This completes the proof. □

8. Setting up the discrete circle method

We now set up the discrete circle method for the proof of Theorem 1.1. We may assume N to be large in terms of g and $q \ge 2$. By the orthogonality of additive characters, we have

$$\begin{aligned} \overleftarrow{\pi}_N(a,q) &= \frac{1}{q} \sum_{0 \le k < q} e\biggl(-\frac{ka}{q}\biggr) \sum_{p \in \mathcal{G}_N} e\biggl(\frac{k\overleftarrow{p}}{q}\biggr) \\ &= \frac{1}{q} \sum_{\substack{0 \le k < q \\ q \mid (g^2-1)g^N k}} e\biggl(-\frac{ka}{q}\biggr) \sum_{p \in \mathcal{G}_N} e\biggl(\frac{k\overleftarrow{p}}{q}\biggr) + \frac{1}{q} \sum_{\substack{0 \le k < q \\ q \nmid (g^2-1)g^N k}} e\biggl(-\frac{ka}{q}\biggr) \sum_{p \in \mathcal{G}_N} e\biggl(\frac{k\overleftarrow{p}}{q}\biggr). \end{aligned} \tag{8.1}$$

The divisibility condition can be rewritten as

$$q \mid (g^2-1)g^N k \iff \frac{q}{(q,(g^2-1)g^N)} \,\Bigm|\, k.$$

The very first term of the right-hand side of (8.1) is then rewritten as

$$\begin{aligned} &\frac{1}{q} \sum_{\substack{0 \le k < q \\ q \mid (g^2-1)g^N k}} e\biggl(-\frac{ka}{q}\biggr) \sum_{p \in \mathcal{G}_N} e\biggl(\frac{k\overleftarrow{p}}{q}\biggr) \\ &= \frac{1}{q} \sum_{0 \le k < (q,(g^2-1)g^N)} e\biggl(-\frac{ka}{(q,(g^2-1)g^N)}\biggr) \sum_{p \in \mathcal{G}_N} e\biggl(\frac{k\overleftarrow{p}}{(q,(g^2-1)g^N)}\biggr) \\ &= \frac{(q,(g^2-1)g^N)}{q} \sum_{\substack{p \in \mathcal{G}_N \\ \overleftarrow{p} \equiv a \pmod{(q,(g^2-1)g^N)}}} 1 \end{aligned}$$

by using the orthogonality backwards. Thus, (8.1) implies

$$\overleftarrow{\pi}_N(a,q)=\frac{(q,(g^2-1)g^N)}{q}\sum_{\substack{p\in\mathcal{G}_N\\ \overleftarrow{p}\equiv a \pmod{(q,(g^2-1)g^N)}}}1+\overleftarrow{R}_N(a,q)$$

with

$$\overleftarrow{R}_N(a,q)=\frac{1}{q}\sum_{\substack{0\le k<q\\ q\nmid(g^2-1)g^Nk}}e\Big(-\frac{ka}{q}\Big)\sum_{p\in\mathcal{G}_N}e\Big(\frac{k\overleftarrow{p}}{q}\Big).$$

Since the exponential sums $F_N(\alpha,\beta)$ and $S_N(\alpha)$ are extended over integers in $[0,g^N)$, again by the orthogonality of additive characters, we have

$$\begin{aligned}\overleftarrow{R}_N(a,q)&=\frac{1}{qg^N}\sum_{\substack{0\le k<q\\ q\nmid(g^2-1)g^Nk}}e\Big(-\frac{ka}{q}\Big)\sum_{0\le h<g^N}\sum_{1\le p<g^N}\sum_{n\in\mathcal{G}_N}e\Big(\frac{k\overleftarrow{n}}{q}\Big)e\Big(\frac{h(p-n)}{g^N}\Big)\\&=\frac{1}{qg^N}\sum_{\substack{0\le k<q\\ q\nmid(g^2-1)g^Nk}}e\Big(-\frac{ka}{q}\Big)\sum_{0\le h<g^N}S_N\Big(\frac{h}{g^N}\Big)F_N\Big(-\frac{h}{g^N},\frac{k}{q}\Big).\end{aligned}\tag{8.2}$$

We now employ the Farey dissection. Take real parameters P,Q satisfying

$$4g^8\le P\le Q.\tag{8.3}$$

Let us denote the set of the Farey fractions in $[0,1]$ with denominator $\le Q$ by

$$\mathscr{F}(Q):=\{(b,r)\in\mathbb{Z}^2\mid 1\le r\le Q,\ 0\le b\le r,\ (b,r)=1\}.$$

For $0\le h<g^N$, by Dirichlet's approximation, we can write

$$\frac{h}{g^N}=\frac{b}{r}+\eta\quad\text{with}\quad(b,r)\in\mathscr{F}(Q)\text{ and }|\eta|<\frac{1}{rQ}.\tag{8.4}$$

Note that then

$$\frac{g^Nb}{r}+g^N\eta=h\in\mathbb{Z}\cap\left(\frac{g^Nb}{r}-\frac{g^N}{rQ},\frac{g^Nb}{r}+\frac{g^N}{rQ}\right)\cap[0,g^N).$$

The association

$$\iota\colon\{0\le h<g^N\}\to\mathscr{I}:=\left\{(b,r,\eta)\;\middle|\;(b,r)\in\mathscr{F}(Q),\ |\eta|<\frac{1}{rQ},\ \frac{g^Nb}{r}+g^N\eta\in\mathbb{Z}\cap[0,g^N)\right\}$$

given by (8.4) is a single-valued function. Indeed, the value (b,r,η) is uniquely determined by h since $\frac{b}{r}$ and other Farey fractions are $\frac{1}{rQ}$ apart and $|\eta|<\frac{1}{rQ}$. Also, this map is injective since h is determined by (b,r,η) by (8.4). Let us introduce the major and minor arcs

$$\begin{aligned}\mathscr{I}_{\mathfrak{M}}&:=\{(b,r,\eta)\in\mathscr{I}\mid\max(r,g^N|\eta|)\le P\},\\ \mathscr{I}_{\mathfrak{m}}&:=\{(b,r,\eta)\in\mathscr{I}\mid\max(r,g^N|\eta|)>P\}\end{aligned}$$

so that $\mathscr{I}=\mathscr{I}_{\mathfrak{M}}\sqcup\mathscr{I}_{\mathfrak{m}}$. We can then decompose (8.2) as

$$|\overleftarrow{R}_N(a,q)|\le\overleftarrow{R}_{\mathfrak{M}}(q)+\overleftarrow{R}_{\mathfrak{m}}(q),\tag{8.5}$$

where

$$\overleftarrow{R}_{\mathfrak{M}}(q) \coloneqq \frac{1}{qg^N} \sum_{\substack{0\le k<q\\ q\nmid (g^2-1)g^N k}} \sum_{(b,r,\eta)\in\mathcal{I}_{\mathfrak{M}}} \left| S_N\left(\frac{b}{r}+\eta\right) F_N\left(-\left(\frac{b}{r}+\eta\right), \frac{k}{q}\right)\right|,$$

$$\overleftarrow{R}_{\mathfrak{m}}(q) \coloneqq \frac{1}{qg^N} \sum_{\substack{0\le k<q\\ q\nmid (g^2-1)g^N k}} \sum_{(b,r,\eta)\in\mathcal{I}_{\mathfrak{m}}} \left| S_N\left(\frac{b}{r}+\eta\right) F_N\left(-\left(\frac{b}{r}+\eta\right), \frac{k}{q}\right)\right|.$$

For a given $(b,r)\in\mathcal{F}(Q)$, we write

$$\mathcal{I}\left(\frac{b}{r}\right) \coloneqq \{(b,r,\eta)\in\mathcal{I}\},\quad \mathcal{I}_{\mathfrak{M}}\left(\frac{b}{r}\right) \coloneqq \{(b,r,\eta)\in\mathcal{I}_{\mathfrak{M}}\} \quad\text{and}\quad \mathcal{I}_{\mathfrak{m}}\left(\frac{b}{r}\right) \coloneqq \{(b,r,\eta)\in\mathcal{I}_{\mathfrak{m}}\}.$$

9. Major arc

We first bound the major arc contribution $\overleftarrow{R}_{\mathfrak{M}}(q)$.

Proposition 9.1. *We have $\#\mathcal{I}_{\mathfrak{M}} \ll P^3$, where the implicit constant is absolute.*

Proof. Since the association $\eta\mapsto \frac{g^N b}{r}+g^N\eta =: h$ is injective, we have

$$\#\mathcal{I}_{\mathfrak{M}} \le \sum_{r\le P}\sum_{\substack{0\le b\le r\\(b,r)=1}} \sum_{\substack{g^N|\eta|\le P\\ \frac{g^N b}{r}+g^N\eta\in\mathbb{Z}}} 1 \le \sum_{r\le P}\sum_{\substack{0\le b\le r\\(b,r)=1}} \sum_{|h-\frac{g^N b}{r}|\le P} 1 \ll P\sum_{r\le P}\sum_{\substack{0\le b\le r\\(b,r)=1}} 1 \ll P^3$$

as claimed. □

Lemma 9.2. *For $N,q\in\mathbb{N}$, we have*

$$\overleftarrow{R}_{\mathfrak{M}}(q) \ll g^N P^3 \exp\left(-c_\infty\cdot\frac{N}{\log q}\right)$$

with some constant $c_\infty = c_\infty(g)\in(0,1)$, where the implicit constant depends only on g.

Proof. We may assume $N\ge 4$. By Lemma 4.11, Proposition 9.1 and the trivial estimate for S_N,

$$\overleftarrow{R}_{\mathfrak{M}}(q) \ll \frac{1}{g^N}\cdot P^3\cdot g^N\cdot g^N \exp\left(-c_\infty\cdot\frac{N}{\log q}\right) = g^N P^3\exp\left(-c_\infty\cdot\frac{N}{\log q}\right)$$

and so the assertion follows. □

10. Minor arc

We next bound the minor arc contribution $\overleftarrow{R}_{\mathfrak{m}}(q)$.

Lemma 10.1. *For $b,r\in\mathbb{Z}$ with $r\ge 1$ and $(b,r)=1$ and $\eta\in\mathbb{R}$ with $|\eta|\le r^{-2}$, we have*

$$S_N\left(\frac{b}{r}+\eta\right) \ll (g^N r^{-\frac{1}{2}} + g^{\frac{4}{5}N} + g^{\frac{1}{2}N} r^{\frac{1}{2}})N^4,$$

where the implicit constant depends only on g.

Proof. Apply partial summation to Theorem 2.1 of [4, p. 28]. □

Lemma 10.2. *For $b, r \in \mathbb{Z}$ with $r \geq 1$ and $(b,r) = 1$ and $\eta \in \mathbb{R}$ with $|\eta| \leq r^{-2}$, we have*

$$S_N\left(\frac{b}{r} + \eta\right) \ll (g^{\frac{1}{2}N}(r|\eta|)^{-\frac{1}{2}} + g^{\frac{4}{5}N} + g^N(r|\eta|)^{\frac{1}{2}})N^4,$$

where the implicit constant depends only on g.

Proof. Apply partial summation to Lemma 4.2 of [8]. □

Lemma 10.3 (Minor arc estimate)**.** *Let $N \in \mathbb{N}$ and $4g^8 \leq P \leq Q \leq g^{\frac{1}{2}N-4}$. Assume that*

$$\alpha_g < \frac{1}{5} \quad \text{or, equivalently,} \quad g \geq 31699. \tag{10.1}$$

We then have

$$\overleftarrow{R}_{\mathfrak{m}}(q) \ll g^N(P^{2\alpha_g - \frac{1}{2}} + g^{(\alpha_g - \frac{1}{5})N} + g^{\alpha_g N}Q^{-\frac{1}{2}})N^6.$$

Proof. We may assume N to be large. By classifying the size of r dyadically, we have

$$\overleftarrow{R}_{\mathfrak{m}}(q) \ll N \sup_{\beta \in \mathbb{R}} \sup_{1 \leq R \leq Q} S(R;\beta), \tag{10.2}$$

where

$$S(R;\beta) \coloneqq \frac{1}{g^N} \sum_{R/2 \leq r \leq R} \sum_{b \pmod r}^{*} \sum_{(b,r,\eta) \in \mathcal{J}_{\mathfrak{m}}} \left| S_N\left(\frac{b}{r} + \eta\right) F_N\left(-\left(\frac{b}{r} + \eta\right), \beta\right)\right|.$$

Note that the summations

$$\sum_{b \pmod r}^{*} \quad \text{and} \quad \sum_{\substack{0 \leq b \leq r \\ (b,r)=1}}$$

do not coincide strictly when $r = 1$, but we doubled the first sum to cover the latter sum. We shall thus bound $S(R;\beta)$ for $1 \leq R \leq Q$. We further decompose as

$$S(R;\beta) \ll S_0(R;\beta) + N \sup_{4g^8 \leq H \leq 4g^N(RQ)^{-1}} S_1(R,H;\beta), \tag{10.3}$$

where

$$S_0(R;\beta) \coloneqq \frac{1}{g^N} \sum_{R/2 \leq r \leq R} \sum_{b \pmod r}^{*} \sum_{\substack{(b,r,\eta) \in \mathcal{J}_{\mathfrak{m}} \\ g^N|\eta| \leq 4g^8}} \left| S_N\left(\frac{b}{r} + \eta\right) F_N\left(-\left(\frac{b}{r} + \eta\right), \beta\right)\right|,$$

$$S_1(R,H;\beta) \coloneqq \frac{1}{g^N} \sum_{R/2 \leq r \leq R} \sum_{b \pmod r}^{*} \sum_{\substack{(b,r,\eta) \in \mathcal{J}_{\mathfrak{m}} \\ H/2 \leq g^N|\eta| \leq H}} \left| S_N\left(\frac{b}{r} + \eta\right) F_N\left(-\left(\frac{b}{r} + \eta\right), \beta\right)\right|.$$

Note that, in order to bound the range of H, we used the fact that when $S_1(R,H;\beta) \neq 0$ and $R \leq Q$, by taking a term counted in $S_1(R,H;\beta)$ and recalling the definition of $\mathcal{J}_{\mathfrak{m}}$, we have

$$H/2 \leq g^N|\eta| \leq g^N(rQ)^{-1} \leq 2g^N(RQ)^{-1} \quad \text{so that} \quad R^2H \leq RQH \leq 4g^N. \tag{10.4}$$

We bound the sums $S_0(R;\beta)$ and $S_1(R,H;\beta)$ separately.

For the sum $S_0(R;\beta)$, by the definition of $\mathcal{J}_{\mathfrak{m}}$ and (8.3), we have

$$S_0(R;\beta) = 0 \quad \text{if } R \leq P.$$

We may thus assume $P < R \le Q$. By the assumption $Q \le g^{\frac{1}{2}N-4}$, the choice $H = 4g^8$ gives

$$R^2 H \le 4g^8 Q^2 = 4g^N.$$

We can thus use Lemma 7.1 and Lemma 10.1 to get

$$\begin{aligned} S_0(R;\beta) &\ll \frac{1}{g^N}(g^N R^{-\frac{1}{2}} + g^{\frac{4}{5}N} + g^{\frac{1}{2}N}R^{\frac{1}{2}})N^4 \times \sum_{r\le R}\sideset{}{^*}\sum_{b \pmod r} \sum_{\substack{g^N|\eta|\le 4g^8 \\ \frac{g^N b}{r}+g^N\eta\in\mathbb{Z}}} \left|F_N\left(-\left(\frac{b}{r}+\eta\right),\beta\right)\right| \\ &\ll g^N(R^{2\alpha_g-\frac{1}{2}} + g^{-\frac{1}{5}N}R^{2\alpha_g} + g^{-\frac{1}{2}N}R^{2\alpha_g+\frac{1}{2}})N^4. \end{aligned}$$

Thus, by recalling $P < R \le Q$ and using (10.1), we have

$$S_0(R;\beta) \ll g^N(P^{2\alpha_g-\frac{1}{2}} + g^{-\frac{1}{5}N}Q^{2\alpha_g} + g^{-\frac{1}{2}N}Q^{2\alpha_g+\frac{1}{2}})N^4. \tag{10.5}$$

This completes the estimate of $S_0(R;\beta)$.

We next consider the sum $S_1(R,H;\beta)$. When $S_1(R,H;\beta) \ne 0$ and $R \le Q$, by taking a term counted in $S_1(R,H;\beta)$ and recalling the definition of $\mathcal{J}_{\mathfrak{m}}$, we have

$$R \le P \implies P < g^N|\eta| \le H \tag{10.6}$$

besides (10.4). We may assume $R \ge 1$ and $H \ge 4g^8$. By Lemma 7.1 and Lemma 10.2, we then get

$$\begin{aligned} S_1(R,H;\beta) &\ll \frac{1}{g^N}(g^N(RH)^{-\frac{1}{2}} + g^{\frac{4}{5}N} + g^{\frac{1}{2}N}(RH)^{\frac{1}{2}})N^4 \\ &\quad \times \sum_{r\le R}\sideset{}{^*}\sum_{b \pmod r} \sum_{\substack{g^N|\eta|\le H \\ \frac{g^N b}{r}+g^N\eta\in\mathbb{Z}}} \left|F_N\left(-\left(\frac{b}{r}+\eta\right),\beta\right)\right| \\ &\ll g^N((R^2H)^{\alpha_g}(RH)^{-\frac{1}{2}} + g^{-\frac{1}{5}N}(R^2H)^{\alpha_g} + g^{-\frac{1}{2}N}(R^2H)^{\alpha_g}(RH)^{\frac{1}{2}})N^4. \end{aligned} \tag{10.7}$$

When $R \le P$, since $P \le H \le 4g^N(RQ)^{-1}$, by using (10.1), (10.4) and (10.6) in (10.7), we have

$$S_1(R,H;\beta) \ll g^N(R^{2\alpha_g-\frac{1}{2}}P^{\alpha_g-\frac{1}{2}} + g^{-\frac{1}{5}N}(g^N RQ^{-1})^{\alpha_g} + g^{-\frac{1}{2}N}(g^N RQ^{-1})^{\alpha_g}(g^N Q^{-1})^{\frac{1}{2}})N^4$$

and so

$$S_1(R,H;\beta) \ll g^N(P^{\alpha_g-\frac{1}{2}} + g^{(\alpha_g-\frac{1}{5})N}P^{\alpha_g}Q^{-\alpha_g} + g^{\alpha_g N}P^{\alpha_g}Q^{-(\alpha_g+\frac{1}{2})})N^4 \quad \text{if } 1 \le R \le P. \tag{10.8}$$

When $R > P$, since $4g^8 \le H \le 4g^N(RQ)^{-1}$ by (10.4), by using (10.1), we can bound (10.7) as

$$\begin{aligned} S_1(R,H;\beta) &\ll g^N(R^{2\alpha_g-\frac{1}{2}} + g^{-\frac{1}{5}N}(g^N RQ^{-1})^{\alpha_g} + g^{-\frac{1}{2}N}(g^N RQ^{-1})^{\alpha_g}(g^N Q^{-1})^{\frac{1}{2}})N^4 \\ &\ll g^N(P^{2\alpha_g-\frac{1}{2}} + g^{(\alpha_g-\frac{1}{5})N} + g^{\alpha_g N}Q^{-\frac{1}{2}})N^4 \quad \text{if } P < R \le Q. \end{aligned} \tag{10.9}$$

By combining (10.8) and (10.9) and noting that

$$P^{\alpha_g-\frac{1}{2}} \le P^{2\alpha_g-\frac{1}{2}}, \quad g^{(\alpha_g-\frac{1}{5})N}P^{\alpha_g}Q^{-\alpha_g} \le g^{(\alpha_g-\frac{1}{5})N}, \quad g^{\alpha_g N}P^{\alpha_g}Q^{-(\alpha_g+\frac{1}{2})} \le g^{\alpha_g N}Q^{-\frac{1}{2}},$$

we obtain

$$S_1(R,H;\beta) \ll g^N(P^{2\alpha_g-\frac{1}{2}} + g^{(\alpha_g-\frac{1}{5})N} + g^{\alpha_g N}Q^{-\frac{1}{2}})N^4. \tag{10.10}$$

So $S_1(R,H;\beta)$ can be bounded similarly for $R > P$ and $R \le P$.

On inserting (10.5) and (10.10) into (10.3) by noting that

$$g^{-\frac{1}{5}N}Q^{2\alpha_g} \le g^{(\alpha_g-\frac{1}{5})N} \quad \text{and} \quad g^{-\frac{1}{2}N}Q^{2\alpha_g+\frac{1}{2}} \le g^{(\alpha_g-\frac{1}{4})N} \le g^{(\alpha_g-\frac{1}{5})N},$$

we have

$$S(R;\beta) \ll g^N(P^{2\alpha_g-\frac{1}{2}} + g^{(\alpha_g-\frac{1}{5})N} + g^{\alpha_g N}Q^{-\frac{1}{2}})N^5.$$

On inserting this estimate into (10.2), we obtain the assertion. □

Remark 10.4. We can check α_g is decreasing for $g \geq 9$ as follows. Write

$$C(g) \coloneqq C_g = \frac{2}{\pi}\log\cot\frac{\pi}{2g} + \frac{1}{g\sin\frac{\pi}{2g}} + 1.$$

Then, we have

$$\alpha_g = \frac{\log C(g)}{\log g} \quad \text{and so} \quad \frac{d\alpha_g}{dg} = \left(\frac{C'(g)}{C(g)} - \frac{\log C(g)}{g\log g}\right)\frac{1}{\log g}.$$

For $g \geq 9$, we have

$$\log C(g) \geq \log\left(\frac{2}{\pi}\log\cot\frac{\pi}{2g} + \frac{1}{g\sin\frac{\pi}{2g}} + 1\right) \geq \log\left(\frac{2}{\pi}\log\cot\frac{\pi}{18} + \frac{2}{\pi} + 1\right) = 1.008\ldots > 1$$

and so it suffices to show

$$C'(g)g\log g \leq C(g)$$

for $g \geq 9$. By using $\cot x \leq \frac{1}{x}$ for $x \in [0, \frac{\pi}{2}]$, We have

$$C'(g)g\log g = \left(\frac{1}{g^2\cot\frac{\pi}{2g}\sin\frac{\pi}{2g}} - \left(1 - \frac{\pi}{2g}\cot\frac{\pi}{2g}\right)\frac{1}{g^2\sin\frac{\pi}{2g}}\right)g\log g \leq \frac{2\log g}{g\sin\frac{\pi}{g}}.$$

By recalling $(\frac{\pi}{2}\log\cot\frac{\pi}{2}x)' = -\frac{2}{\sin\pi x}$, we then have

$$C(g) \geq \frac{2}{\pi}\log\cot\frac{\pi}{2g} + 1 = \frac{2}{\pi}\log\cot\frac{\pi}{2g} - \frac{2}{\pi}\log\cot\frac{\pi}{4} + 1 = \int_{\frac{1}{g}}^{\frac{1}{2}} \frac{2x}{\sin\pi x}\frac{dx}{x} + 1.$$

Since $(\frac{\sin x}{x}) = \frac{x-\tan x}{x^2}\cdot\cos x \leq 0$ and $\sin x \geq \frac{2}{\pi}x$ for $x \in [0, \frac{\pi}{4}]$, we have

$$C(g) \geq \frac{2\log g}{g\sin\frac{\pi}{g}} + 1 - \frac{2\log 2}{g\sin\frac{\pi}{g}} \geq \frac{2\log g}{g\sin\frac{\pi}{g}} + 1 - \log 2 \geq \frac{2\log g}{g\sin\frac{\pi}{g}} \geq C'(g)g\log g$$

as desired. We can check $\alpha_{31699} = 0.1999997\ldots < \frac{1}{5}$ by some numerical calculation.

11. Proof of the main theorem and corollaries

We finally prove the main theorem and its corollaries.

Proof of Theorem 1.1. In the above setting of the discrete circle method, we choose P, Q by

$$P \coloneqq \max\left(\exp\left(\frac{c_\infty}{4}\frac{N}{\log q}\right), 4g^8\right) \quad \text{and} \quad Q \coloneqq g^{\frac{1}{2}N-4}, \tag{11.1}$$

where $c_\infty \in (0,1)$ is a constant in Lemma 9.2. By Lemma 9.2, we then have

$$\overleftarrow{R}_{\mathfrak{M}}(q) \ll g^N \exp\left(-\frac{c_\infty}{4}\frac{N}{\log q}\right). \tag{11.2}$$

Also, by Lemma 10.3, noting that (1.4) and (11.1) assure the required conditions, we have

$$\overleftarrow{R}_{\mathfrak{m}}(q) \ll g^N(P^{2(\alpha_g-\frac{1}{4})} + g^{(\alpha_g-\frac{1}{5})N})N^6 \ll g^N N^6 \exp\left(-\widetilde{c}\cdot\frac{N}{\log q}\right)$$

with some $\widetilde{c} = \widetilde{c}(g) \in (0, c_\infty]$. Assuming

$$q \le \exp\left(c \cdot \frac{N}{\log N}\right) \quad \text{with} \quad c \coloneqq \frac{\widetilde{c}}{12} \in \left[0, \frac{c_\infty}{4}\right], \tag{11.3}$$

we have

$$N^6 \exp\left(-\widetilde{c} \cdot \frac{N}{\log q}\right) = \exp\left(-\widetilde{c} \cdot \frac{N}{\log q} + 6 \log N\right) \le \exp\left(-\frac{\widetilde{c}}{2} \cdot \frac{N}{\log q}\right) \le \exp\left(-c \cdot \frac{N}{\log q}\right)$$

and so

$$\overleftarrow{R}_{\mathfrak{m}}(q) \ll g^N \exp\left(-c \cdot \frac{N}{\log q}\right). \tag{11.4}$$

On inserting (11.2) and (11.4) into (8.5), we arrive at

$$\overleftarrow{R}_N(a, q) \ll g^N \exp\left(-c \cdot \frac{N}{\log q}\right)$$

provided (11.3) is true. This completes the proof. □

Proof of Corollary 1.2. The case $q = 1$ follows immediately by the prime number theorem and so we may assume $q \ge 2$. Since (1.6) is stronger than (1.5), we can use the conclusion of Theorem 1.1. Then, the remaining task is to evaluate the cardinality

$$G \coloneqq \sum_{\substack{p \in \mathscr{G}_N \\ \overleftarrow{p} \equiv a \pmod{(q, (g^2-1)g^N)}}} 1.$$

Note that the above congruence can be rephrased by the simultaneous congruences

$$\overleftarrow{p} \equiv a \pmod{(q, (g^2-1)g^N)} \iff \begin{cases} \overleftarrow{p} \equiv a \pmod{(q, g^2-1)}, \\ \overleftarrow{p} \equiv a \pmod{(q, g^N)}. \end{cases}$$

by the Chinese remainder theorem since $(g^2 - 1, g) = 1$. As stated in (1.3), we have

$$\overleftarrow{p} \equiv a \pmod{(q, g^2-1)} \iff p \equiv \overline{g}^{N-1} a \pmod{(q, g^2-1)},$$

where $\overline{g} \pmod{(q, g^2-1)}$ is the multiplicative inverse of $g \pmod{(q, g^2-1)}$, since by using $g^2 \equiv 1 \pmod{g^2-1}$, we can see that the base-g representation

$$p = \sum_{0 \le i < N} p_i g^i \quad \text{with} \quad p_0, \dots, p_{N-1} \in \{0, \dots, g-1\} \text{ and } p_0, p_{N-1} \ne 0 \tag{11.5}$$

of $p \in \mathscr{G}_N$ satisfies

$$\overleftarrow{p} \equiv \sum_{0 \le i < N} p_i g^{N-i-1} \equiv g^{N-1} \sum_{0 \le i < N} p_i g^i (g^2)^{-i} \equiv g^{N-1} \sum_{0 \le i < N} p_i g^i \equiv g^{N-1} p \pmod{g^2-1}.$$

We can thus rewrite G as

$$G = \sum_{\substack{p \in \mathscr{G}_N \\ p \equiv \overline{g}^{N-1} a \pmod{(q, g^2-1)} \\ \overleftarrow{p} \equiv a \pmod{(q, g^N)}}} 1.$$

When $(a, q, g^2-1) \ne 1$, we have

$$G \le \sum_{p \mid (a, q, g^2-1)} 1 \ll 1.$$

We may thus assume $(a, q, g^2-1)=1$. Take the smallest $N_0 \in \mathbb{N}$ such that

$$(q, g^{N_0}) = (q, g^N).$$

By noting that $\overleftarrow{n} \not\equiv 0 \pmod{g}$ for any $n \in \mathbb{N}$, we then have

$$G = \sum_{\substack{1 \le v < g^{N_0} \\ v \equiv a \pmod{(q, g^{N_0})} \\ v \not\equiv 0 \pmod{g}}} \sum_{\substack{p \in \mathcal{G}_N \\ p \equiv \overline{g}^{N-1} a \pmod{(q, g^2-1)} \\ \overleftarrow{p} \equiv v \pmod{g^{N_0}}}} 1.$$

When $g \mid (a, q)$, the above sum over v is empty and so we may assume $g \nmid (a, q)$. For the base-g expansion (11.5) of $p \in \mathcal{G}_N$, we have

$$\overleftarrow{p} \equiv v \pmod{g^{N_0}} \iff \sum_{0 \le i < N_0} p_{N-i-1} g^i \equiv v \pmod{g^{N_0}}$$

However, since v and $\sum_{0 \le i < N_0} p_{N-i-1} g^i$ both belong to $[0, g^{N_0})$, this is further equivalent to

$$\overleftarrow{p} \equiv v \pmod{g^{N_0}} \iff v = \sum_{0 \le i < N_0} p_{N-i-1} g^i \iff v_i = p_{N-i-1},$$

where the v_i are given by the base-g representation of v in the form

$$v = \sum_{0 \le i < N_0} v_i g^i \quad \text{with} \quad v_0, \dots, v_{N_0-1} \in \{0, \dots, g-1\} \text{ and } v_0 \neq 0.$$

Thus, we have $\overleftarrow{p} \equiv v \pmod{g^{N_0}}$ and $p \in \mathcal{G}_N$ if and only if

$$\sum_{N-N_0 \le i < N} p_i g^i = \sum_{0 \le i < N_0} p_{N-i-1} g^{N-i-1} = \sum_{0 \le i < N_0} v_i g^{N-i-1} =: v^*.$$

This is further equivalent to

$$p \in [v^*, v^* + g^{N-N_0})$$

since $v_0 \neq 0$ implies $v^* \ge g^{N-1}$. We can thus further rewrite G as

$$G = \sum_{\substack{1 \le v < g^{N_0} \\ v \equiv u \pmod{(q, g^{N_0})} \\ v \not\equiv 0 \pmod{g}}} \sum_{\substack{p \in [v^*, v^* + g^{N-N_0}) \\ p \equiv \overline{g}^{N-1} a \pmod{(q, g^2-1)}}} 1.$$

By using some effective prime number theorem in arithmetic progressions with modulus $(q, g^2-1) \ll 1$, e.g. Corollary 11.12 and Theorem 11.17 of [10], and using the approximation

$$\int_{v^*}^{v^* + g^{N-N_0}} \frac{dt}{\log t} = \frac{g^{N-N_0}}{\log g^N} \left(1 + O\left(\frac{1}{N}\right)\right)$$

for $1 \le v < N_0$ with $v \not\equiv 0 \pmod{g}$, we have

$$G = \frac{1}{\varphi((q, g^2-1))} \left(\sum_{\substack{1 \le v < g^{N_0} \\ v \equiv u \pmod{(q, g^{N_0})} \\ v \not\equiv 0 \pmod{g}}} 1 \right) \frac{g^{N-N_0}}{\log g^N} \left(1 + O\left(\frac{1}{N}\right)\right) + O(g^{N+N_0} \exp(-c_{\mathrm{PNT}} \sqrt{N})).$$

Since

$$\begin{aligned}\sum_{\substack{1\le v<g^{N_0}\\ v\equiv a \pmod{(q,g^{N_0})}\\ v\not\equiv 0 \pmod{g}}} 1 &= \sum_{\substack{v \pmod{g^{N_0}}\\ v\equiv a \pmod{(q,g^{N_0})}\\ v\not\equiv 0 \pmod{g}}} 1 = \sum_{\substack{v \pmod{g^{N_0}}\\ v\equiv a \pmod{(q,g^{N_0})}}} 1 - \sum_{\substack{v \pmod{g^{N_0}}\\ v\equiv a \pmod{(q,g^{N_0})}\\ v\equiv 0 \pmod{g}}} 1\\ &= \frac{g^{N_0}}{(q,g^{N_0})} - \sum_{\substack{v \pmod{g^{N_0-1}}\\ gv\equiv a \pmod{(q,g^{N_0})}}} 1\\ &= \left(1-\mathbb{1}_{(q,g)|a}\frac{(q,g)}{g}\right)\frac{g^{N_0}}{(q,g^{N_0})}\\ &= \left(1-\mathbb{1}_{(q,g)|a}\frac{(q,g)}{g}\right)\frac{g^{N_0}}{(q,g^{N})},\end{aligned}$$

we obtain

$$G = \frac{\rho_g(a,q)}{(q,(g^2-1)g^N)}\frac{g^N}{\log g^N}\left(1+O\left(\frac{1}{N}\right)\right)+O(g^{N+N_0}\exp(-c_{\mathrm{PNT}}\sqrt{N})). \tag{11.6}$$

We then estimate g^{N_0} in the remainder term. For a prime number p and a positive integer n, define $v_p(n)\in\mathbb{Z}$ by $p^{v_p(n)}\mid n$ but $p^{v_p(n)+1}\nmid n$. For any prime p, by (1.6), we then have

$$2^{v_p(q)}\le p^{v_p(q)}\le q\le \exp(c\sqrt{N}) \quad\text{and so}\quad v_p(q)\le \frac{c}{\log 2}\sqrt{N}\le N$$

by making $c<\log 2$. Then, we have

$$(q,g^{[\frac{c}{\log 2}\sqrt{N}]}) = \prod_{p|(q,g)} p^{\min(v_p(q),v_p(g)[\frac{c}{\log 2}\sqrt{N}])} = \prod_{p|(q,g)} p^{v_p(q)} = \prod_{p|(q,g)} p^{\min(v_p(q),v_p(g)N)} = (q,g^N)$$

and so $N_0\le \frac{c}{\log 2}\sqrt{N}$ by the minimality of N_0. By making c small enough so that

$$g^{\frac{c}{\log 2}\sqrt{N}}\le \exp(\tfrac{1}{2}c_{\mathrm{PNT}}\sqrt{N}) \quad\text{and}\quad c<\tfrac{1}{2}c_{\mathrm{PNT}},$$

we then have

$$g^{N+N_0}\exp(-c_{\mathrm{PNT}}\sqrt{N})\le g^N\exp(-\tfrac{1}{2}c_{\mathrm{PNT}}\sqrt{N})\le g^N\exp(-c\sqrt{N}).$$

On inserting this into (11.6) and combining it with Theorem 1.1, we obtain the assertion. □

Proof of Corollary 1.3. Assume $(a,q,g^2-1)=1$ and $g\nmid(a,q)$. If $(q,g)\mid a$, we cannot have $g\mid(q,g)$ since otherwise $g\mid(a,q)$. We thus have

$$\rho_g(a,q) = \left(1-\mathbb{1}_{(q,g)|a}\frac{(q,g)}{g}\right)\prod_{p|(q,g^2-1)}\left(\frac{p}{p-1}\right)\ge\frac{1}{g}.$$

Thus, the assertion follows by Corollary 1.2. □

Acknowledgments

The first author would like to thank Lucile Devin, Didier Lesesvre, Bruno Martin, Thi-Thu Nguyen and Martine Queffélec with whom she participated in the 2022–23 Lille-Calais *Groupe de Travail* on Maynard's paper [8]. The second author would like to express his gratitude to Laboratoire Paul Painlevé and Prof. Daniel Duverney for their generous hospitality in Lille in October–November 2023 during which the main part of this work was carried out. The second author was supported by JSPS KAKENHI Grant Number JP21K13772.

Ethical Statement

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. W. D. Banks, D. N. Hart, and M. Sakata, *Almost all palindromes are composite*, Math. Res. Lett. **11** (2004), 853–868.
2. S. Col, *Palindromes dans les progressions arithmétiques*, Acta Arith. **137** (2009), no. 1, 1–41 (French).
3. C. Dartyge, B. Martin, J. Rivat, I. E. Shparlinski, and C. Swaenepoel, *Reversible primes*, arXiv preprint (2023), `arXiv:2309.11380`.
4. G. Harman, *Prime-Detecting Sieves*, London Math. Soc. Monographs, vol. 33, Princeton University Press, New Jersey, 2007.
5. C. Mauduit and J. Rivat, *La somme des chiffres des carrés*, Acta Math. **203** (2009), 107–148.
6. ———, *Sur un problème de Gelfond : la somme des chiffres des nombres premiers*, Ann. of Math. **171** (2010), 1591–1646.
7. J. Maynard, *Primes with restricted digits*, Invent. Math. **217** (2019), 127–218.
8. ———, *Primes and polynomials with restricted digits*, Int. Math. Res. Not. **2022** (2022), no. 14, 10626–10648.
9. H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathamatics, vol. 227, Springer-Verlag, 1971.
10. H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory: I. Classical Theory*, Cambridge studies in advanced mathematics, vol. 97, Cambridge University Press, 2006.
11. A. Tuxanidy and D. Panario, *Infinitude of palindromic almost-prime numbers*, arXiv preprint (2023), `arXiv:2307.16637`.

Gautami Bhowmik

Laboratoire Paul Painlevé, Labex-CEMPI, Université de Lille
59655 Villeneuve d'Ascq Cedex, France.
Email address: `gautami.bhowmik@univ-lille.fr`

Yuta Suzuki

Department of Mathematics, Rikkyo University,
3-34-1 Nishi-Ikebukuro, Toshima-ku, Tokyo 171-8501, Japan.
Email address: `suzuyu@rikkyo.ac.jp`