Reversible primes

Cécile Dartyge, Bruno Martin, Joël Rivat, Igor E. Shparlinski, Cathy Swaenepoel

REVERSIBLE PRIMES

CÉCILE DARTYGE, BRUNO MARTIN, JOËL RIVAT,
IGOR E. SHPARLINSKI, AND CATHY SWAENEPOEL

ABSTRACT. For an n-bit positive integer a written in binary as

$$a = \sum_{j=0}^{n-1} \varepsilon_j(a)\, 2^j,$$

where $\varepsilon_j(a) \in \{0,1\}$, $j \in \{0,\dots,n-1\}$, $\varepsilon_{n-1}(a) = 1$, let us define

$$\overleftarrow{a} = \sum_{j=0}^{n-1} \varepsilon_j(a)\, 2^{n-1-j},$$

the digital reversal of a. Also let $\mathcal{B}_n = \{2^{n-1} \leqslant a < 2^n : \ a \text{ odd}\}$. With a sieve argument, we obtain an upper bound of the expected order of magnitude for the number of $p \in \mathcal{B}_n$ such that p and $\overleftarrow{p}$ are prime. We also prove that for sufficiently large n,

$$|\{a \in \mathcal{B}_n : \ \max\{\Omega(a), \Omega(\overleftarrow{a})\} \leqslant 8\}| \geqslant c\,\frac{2^n}{n^2},$$

where $\Omega(n)$ denotes the number of prime factors counted with multiplicity of n and $c > 0$ is an absolute constant. Finally, we provide an asymptotic formula for the number of n-bit integers a such that a and $\overleftarrow{a}$ are both squarefree. Our method leads us to provide various estimates for the exponential sum

$$\sum_{a \in \mathcal{B}_n} \exp\left(2\pi i(\alpha a + \vartheta \overleftarrow{a})\right) \quad (\alpha, \vartheta \in \mathbb{R}).$$

CONTENTS

2020 *Mathematics Subject Classification.* 11A63, 11N05, 11N36.

Key words and phrases. prime numbers, squarefree numbers, reversed binary expansions, digits.

Notation

Throughout the paper, the notations $U = O(V)$, $U \ll V$ and $V \gg U$ all mean that there is an absolute constant $C > 0$ such that $|U| \leqslant CV$. If the implicit constant C is allowed to depend on a parameter α then this dependence is indicated by writing $U = O_\alpha(V)$, $U \ll_\alpha V$ or $V \gg_\alpha U$. We also write $U \asymp V$ if $U \ll V \ll U$ and similarly for $U \asymp_\alpha V$.

For a real number $A > 0$, we write $a \sim A$ to denote $a \in [A, 2A)$.

For a finite set $\mathcal{S}$ we use $|\mathcal{S}|$ to denote its cardinality.

We use $\mu(d)$, $\tau(d)$, $\omega(d)$ and $\Omega(d)$ to denote the Möbius function, number of positive divisors, number of distinct prime factors and the number of prime factors counted with multiplicity of an integer $d \geqslant 1$. We denote by $P^-(d)$ and $P^+(d)$ the smallest and the largest prime factors of an integer $d \geqslant 2$, respectively.

For a real number x we also set

$$\mathrm{e}(x) = \exp(2\pi i x) \qquad \text{and} \qquad \|x\| = \min\{|x - k| : \ k \in \mathbb{Z}\}.$$

For a certain property P, we define $\mathbf{1}_{\mathsf{P}}$ by $\mathbf{1}_{\mathsf{P}} = 1$ if P is satisfied and $\mathbf{1}_{\mathsf{P}} = 0$ otherwise.

The letter p, with or without indices, always denotes a prime number.

1. Introduction

1.1. **Motivation and set-up.** Since recently, a large body of research has appeared on arithmetic properties of integers with various digits restrictions in a given integer base. For example, this includes the work of Mauduit and Rivat [21] on the sum of digits of primes, the work of Bourgain [4, 5] and Swaenepoel [31] on primes with prescribed digits on a positive proportion of positions in their digital expansion, and the results of Maynard [22,23] on primes with missing digits, see also [6–11, 13,16,19,26,28] and references therein for a series of other results about primes and other interesting integers with various digit restrictions. In this direction, polynomial values with digital restrictions have been studied by Mauduit and Rivat [20], Maynard [23] and very recently by Spiegelhofer [29], see also [12, 15, 30].

In the present paper, we are interested in a question, which apparently has never been studied theoretically. Let $b \geqslant 2$ an integer. For a positive integer k written in a base b as

$$k = \sum_{j=0}^{n-1} \varepsilon_j(k)\, b^j,$$

where $\varepsilon_j(k) \in \{0, \dots, b-1\}$ for $j \in \{0, \dots, n-1\}$ and $\varepsilon_{n-1}(k) \neq 0$, we define

$$\overleftarrow{k} = \sum_{j=0}^{n-1} \varepsilon_j(k)\, b^{n-1-j}$$

as the "reverse" of k in base b (throughout the paper, we make sure that there is no ambiguity on the base b). It is certainly interesting to understand whether there is any correlation between arithmetic properties of k and $\overleftarrow{k}$. For instance, a natural question would be to evaluate the number of n-digits integers a such that a and $\overleftarrow{a}$ belong to a given set $\mathcal{S}$ defined by a multiplicative property.

We are especially interested in primality of both k and $\overleftarrow{k}$. The prime numbers p such that $\overleftarrow{p}$ is also a prime number are called *reversible primes*. Sometimes they are also referred as "emirps", "reversal primes" or "mirror primes". The first reversible primes in bases 2 and 10 can be found in [27, A074832] and [27, A007500], respectively.

Remarkable examples of reversible primes are of course palindromic primes, that is, primes p such that $p = \overleftarrow{p}$. Unlike reversible primes, the distribution of palindromic primes has already been deeply investigated. Let us denote by $\mathcal{P}_b(x)$ the set of palindromes less than x in

base b. Improving on results by Banks, Hart and Sakata [1], Col [9] has obtained an upper bound of the right order of magnitude for the number of palindromic primes in every base $b \geqslant 2$: for $x \geqslant 2$, we have

$$|\{p \in \mathcal{P}_b(x)\}| \ll_b \frac{|\mathcal{P}_b(x)|}{\log x}.$$

Col [9] has also proved that for all $b \geqslant 2$, there exists $\kappa_b \geqslant 1$ such that for a sufficiently large x (depending only on b)

$$|\{k \in \mathcal{P}_b(x) : \ \Omega(k) \leqslant \kappa_b\}| \gg_b \frac{|\mathcal{P}_b(x)|}{\log x}$$

and he computed some admissible values of κ_b. In particular, he showed that there are infinitely many binary palindromes k such that $\Omega(k) \leqslant 60$. We also mention that Irving [18] has proved that, for sufficiently large b, there exists a 3-digits palindrome in base b with exactly 2 prime factors and Banks and Shparlinski [3] showed that in any base $b \geqslant 2$, for sufficiently large n, there exists a n-digit palindrome k such that $\omega(k) \geqslant (\log\log k)^{1+o(1)}$ and a n-digit palindrome m such that $P^+(m) \geqslant (\log m)^{2+o(1)}$.

In this paper, in order to emphasize our main ideas to handle reversible primes, we choose to concentrate on the emblematic case of binary expansions. So from now on, we consider n-bit integers k such that

$$k = \sum_{j=0}^{n-1} \varepsilon_j(k)\, 2^j, \quad \overleftarrow{k} = \sum_{j=0}^{n-1} \varepsilon_j(k)\, 2^{n-1-j}$$

with $\varepsilon_j(k) \in \{0,1\}$, $j \in \{0,\dots,n-1\}$, $\varepsilon_{n-1}(k) = 1$. The sieve method developed by Col in [9] is not suitable to study reversible primes. Instead, we develop a two-dimensional sieve approach that enables us to obtain an upper bound of the expected order of magnitude for the number of reversible primes and to prove that there are infinitely many reversible almost primes. Furthermore, we are able to get an asymptotic formula for the number of reversible squarefree integers.

1.2. **Main results.**

1.2.1. *Reversible primes.* The n-bit prime numbers p such that $\overleftarrow{p}$ is also prime must satisfy $\varepsilon_0(p) = \varepsilon_{n-1}(p) = 1$, which implies that $p \in \mathcal{B}_n$, where

$$\mathcal{B}_n = \{2^{n-1} \leqslant a < 2^n : \ a \text{ odd}\}$$

is the set of n-bit odd integers. Clearly

$$|\mathcal{B}_n| = 2^{n-2}.$$

We also note that if $a \in \mathcal{B}_n$, then

$$\overleftarrow{a} \equiv (-1)^{n-1} a \bmod 3, \tag{1.1}$$

so that $3 \mid a$ if and only if $3 \mid \overleftarrow{a}$.

We denote by $\Theta(n)$ the number of n-bit reversible primes:

$$\Theta(n) = \left|\{2^{n-1} \leqslant p < 2^n : \ p \text{ and } \overleftarrow{p} \text{ are prime}\}\right|.$$

It is certainly natural to expect that

$$\Theta(n) = (c + o(1)) \frac{2^n}{n^2} \qquad (n \to \infty), \tag{1.2}$$

for some absolute constant $c > 0$. In Section 8, we present numerical investigations and a heuristic argument that permit us to formulate a conjecture regarding the value of c in (1.2). We are not able to obtain such an asymptotic formula but we obtain an upper bound on $\Theta(n)$ of the expected order of magnitude. To achieve this, we use a sieve method based on the following trivial inequality. For any real number $z \leqslant 2^{n-1}$ we have

$$\Theta(n) \leqslant \Theta(n, z), \tag{1.3}$$

where

$$\Theta(n, z) = |\{a \in \mathcal{B}_n : \ p \mid a\overleftarrow{a} \Rightarrow p \geqslant z\}|.$$

We use the two-dimensional combinatorial sieve described in [14, p. 308-310], with the associated constant

$$\beta_2 = 4.2664\ldots$$

from [14, Appendix III], to establish the following matching upper and lower bounds on $\Theta(n, z)$.

Theorem 1.1. *Let $0 < \gamma < 1/(2\beta_2)$. There exists $n_0 \geqslant 1$, which depends only on γ, such that for $n \geqslant n_0$, we have*

$$\Theta\left(n, 2^{\gamma n}\right) \asymp_\gamma \frac{2^n}{n^2}.$$

Hence, we immediately derive from (1.3) and Theorem 1.1 an upper bound on $\Theta(n)$ of the expected order of magnitude.

Corollary 1.2. *For any integer $n \geqslant 1$, we have*

$$\Theta(n) \ll \frac{2^n}{n^2}.$$

Another direct consequence of Theorem 1.1 is the existence of infinitely many almost prime numbers whose reverse is also almost prime. If a n-bit integer a is such that all prime factors of $a\overleftarrow{a}$ are bigger than $2^{\gamma n}$ then $\max\{\Omega(a), \Omega(\overleftarrow{a})\} \leqslant \lfloor 1/\gamma \rfloor$. Our limit for the choice of $1/\gamma$ is $2\beta_2 = 8.53\ldots$.

Corollary 1.3. *There exists $n_0 \geqslant 1$ such that for any integer $n \geqslant n_0$, we have*

$$|\{a \in \mathcal{B}_n : \max\{\Omega(a), \Omega(\overleftarrow{a})\} \leqslant 8\}| \gg \frac{2^n}{n^2}.$$

The lower bound in Corollary 1.3 is not of the expected order of magnitude. A power of $\log n$ is missing. This is due to the fact that the almost primes a and $\overleftarrow{a}$ detected in Corollary 1.3 are without small prime factors.

1.2.2. *Reversible squarefree integers.* It is also interesting to consider simultaneously squarefree values of a and $\overleftarrow{a}$. Thus, we define

$$Q(n) = \left|\{a \in \mathcal{B}_n : \ \mu^2(a) = \mu^2(\overleftarrow{a}) = 1\}\right|$$

as the cardinality of the set of the $a \in \mathcal{B}_n$ such that a and its reverse $\overleftarrow{a}$ are both squarefree. This is related to the sequence [27, A077337] (in base $b = 10$). In this case, we are able to obtain an asymptotic formula for $Q(n)$ which matches the following heuristic.

If we choose $a \in \mathcal{B}_n$ at random then the probability that $9 \nmid a$ and $9 \nmid \overleftarrow{a}$ is

$$\begin{aligned}\mathbb{P}(9 \nmid a \text{ and } 9 \nmid \overleftarrow{a}) &= 1 - \mathbb{P}(9 \mid a \text{ or } 9 \mid \overleftarrow{a}) \\ &= 1 - \mathbb{P}(9 \mid a) - \mathbb{P}(9 \mid \overleftarrow{a}) + \mathbb{P}(9 \mid a \text{ and } 9 \mid \overleftarrow{a}).\end{aligned}$$

If $3 \mid a$ then $3 \mid \overleftarrow{a}$. Therefore, if $9 \mid a$ then $\overleftarrow{a} \equiv 0, 3$ or $6 \bmod 9$. Hence we may expect that

$$\mathbb{P}(9 \mid a \text{ and } 9 \mid \overleftarrow{a}) \approx \frac{1}{9} \cdot \frac{1}{3} = \frac{1}{27}$$

and

$$\mathbb{P}(9 \nmid a \text{ and } 9 \nmid \overleftarrow{a}) \approx 1 - \frac{1}{9} - \frac{1}{9} + \frac{1}{27} = \frac{22}{27}.$$

Moreover, if $a \in \mathcal{B}_n$ then a and $\overleftarrow{a}$ are both odd. Thus we may expect that

$$\begin{aligned}\frac{1}{|\mathcal{B}_n|} Q(n) &\approx \mathbb{P}(9 \nmid a \text{ and } 9 \nmid \overleftarrow{a}) \prod_{p \geqslant 5} \mathbb{P}(p^2 \nmid a \text{ and } p^2 \nmid \overleftarrow{a}) \\ &\approx \frac{22}{27} \prod_{p \geqslant 5} \left(1 - \frac{1}{p^2}\right)^2 = \frac{22}{27} \left(\frac{4}{3}\right)^2 \left(\frac{9}{8}\right)^2 \frac{1}{\zeta(2)^2} \\ &= \frac{11}{6} \frac{1}{\zeta(2)^2} = \frac{66}{\pi^4}.\end{aligned}$$

Therefore we expect that

$$Q(n) = |\mathcal{B}_n| \left(\frac{66}{\pi^4} + o(1) \right),$$

which we prove in a quantitative way.

We also define

$$\widetilde{Q}(n) = \left| \{ 2^{n-1} \leqslant a < 2^n : \ \mu^2(a) = \mu^2(\overleftarrow{a}) = 1 \} \right|.$$

Theorem 1.4. *There exists an absolute constant $c > 0$ such that for any $n \geqslant 1$, we have*

$$Q(n) = |\mathcal{B}_n| \left(\frac{66}{\pi^4} + O(\exp(-c\sqrt{n})) \right) \tag{1.4}$$

and

$$\widetilde{Q}(n) = 2^{n-1} \left(\frac{99}{2\pi^4} + O(\exp(-c\sqrt{n})) \right). \tag{1.5}$$

Examining the proof of Theorem 1.4 one can easily see that the value $c = 0.0439$ is admissible.

To conclude this section, we point to the reader that so far, it is not known whether there exists infinitely many squarefree palindromes.

1.3. Our approach to estimate $\Theta(n, z)$.

1.3.1. *Overview.* Our proof follows the following sequence of steps and ideas.

- We rely on sieving, which means we have to establish a reasonable level of distribution of the products $a\overleftarrow{a}$ in arithmetic progressions, see (1.6). This naturally leads to two problems: evaluating the main term which is given by some explicit multiplicative function, see (1.7) and (1.8), and estimating the error term (on average over moduli in the sieving with some weights), which is done in Lemma 1.5.
- We handle the error term and prove Lemma 1.5 by establishing a connection with some exponential sums, see Section 5, and estimating these sums, see Sections 2 and 3.
- In particular, we study in Section 2 exponential sums with linear combinations of a and $\overleftarrow{a}$. As for many other exponential sums involving digital functions, they can be decomposed in a product of elementary trigonometric sums, see Section 2.2. This product representation permits us to develop iterative arguments, see for instance the proof of Lemma 2.6, and obtain pointwise bounds, see Section 2.3, as well as bounds on average, see Sections 2.4 and 2.5.

1.3.2. *Detailed description.* As already mentioned, we rely on a classical sieve method. For $d \geqslant 1$, we put

$$T_n(d) = |\{a \in \mathcal{B}_n : \ d \mid a\overleftarrow{a}\}|. \tag{1.6}$$

Clearly $T_n(2) = 0$. For $a \in \mathcal{B}_n$ randomly chosen, since $3 \mid \overleftarrow{a}$ is equivalent to $3 \mid a$ (by (1.1)), the probability that $3 \mid a\overleftarrow{a}$ is close to $1/3$ and for any prime $p \geqslant 5$, the events "$p \mid a$" and "$p \mid \overleftarrow{a}$" should be independent so that the probability that $p \mid a\overleftarrow{a}$ is expected to be $\frac{1}{p} + \frac{1}{p} - \frac{1}{p^2} = \frac{2p-1}{p^2}$. Moreover for distinct prime numbers p_1 and p_2, the events "$p_1 \mid a\overleftarrow{a}$" and "$p_2 \mid a\overleftarrow{a}$" are expected to be independent. These heuristics lead us to define $R_n(d)$ for d squarefree by

$$T_n(d) = \frac{f(d)}{d}\,|\mathcal{B}_n| + R_n(d), \tag{1.7}$$

where f is the multiplicative function defined for any prime number p by

$$f(p) = \begin{cases} 0 & \text{if } p = 2, \\ 1 & \text{if } p = 3, \\ \frac{2p-1}{p} & \text{if } p \geqslant 5, \end{cases} \tag{1.8}$$

and $f(p^\nu) = 0$ for any $\nu \geqslant 2$ (it follows that $f(d) \neq 0$ if and only if d is odd and squarefree).

Let

$$V(w) = \prod_{2 \leqslant p < w} \left(1 - \frac{f(p)}{p}\right).$$

If $w \leqslant 3$ then

$$V(w) = 1$$

and if $w > 3$ then

$$V(w) = \frac{2}{3} \prod_{3 < p < w} \left(1 - \frac{2p-1}{p^2}\right) = \frac{2}{3} \prod_{3 < p < w} \left(1 - \frac{1}{p}\right)^2.$$

The *Mertens formula*, see, for example, [32, Part I, Theorem 1.12], implies that

$$V(w) \asymp \frac{1}{(\log w)^2}$$

and that there exists an absolute constant $C > 0$ such that for any $2 \leqslant w_1 \leqslant w$, we have

$$\frac{V(w_1)}{V(w)} \leqslant \left(\frac{\log w}{\log w_1}\right)^2 \left(1 + \frac{C}{\log w_1}\right).$$

We are now ready to apply the sieve theorem stated in a more precise form in [14, Equations (1.17) and (1.18)] with

$$\mathscr{A} = (a^{\overleftarrow{a}})_{a\in\mathcal{B}_n}, \qquad \mathscr{P} = \{p \geqslant 3 : \ p \text{ prime}\}, \qquad \kappa = 2.$$

For any $y \geqslant z \geqslant 3$, we have

$$\begin{aligned}\Theta(n,z) \leqslant |\mathcal{B}_n|V(z)\left(h^+\left(\frac{\log y}{\log z}\right) + O\left(\frac{\log\log y}{(\log y)^{1/6}}\right)\right)\\ +O\left(\sum_{\substack{d|P(z)\\ d<y}} 4^{\omega(d)}|R_n(d)|\right),\end{aligned} \tag{1.9}$$

where

$$P(z) = \prod_{3\leqslant p<z} p,$$

and $h^+(u)$ is some continuous function, which decreases monotonically towards 1 as $u \to +\infty$. Moreover, for any $y \geqslant z \geqslant 3$, we have a similar lower bound

$$\begin{aligned}\Theta(n,z) \geqslant |\mathcal{B}_n|V(z)\left(h^-\left(\frac{\log y}{\log z}\right) + O\left(\frac{\log\log y}{(\log y)^{1/6}}\right)\right)\\ +O\left(\sum_{\substack{d|P(z)\\ d<y}} 4^{\omega(d)}|R_n(d)|\right),\end{aligned} \tag{1.10}$$

where $h^-(u)$ is some continuous function, which increases monotonically towards 1 as $u \to +\infty$ and $h^-(u) > 0$ for $u > \beta_2 = 4.2664\ldots$.

Our main technical result, which we establish in Section 6, is the following.

Lemma 1.5. *Let $0 < \xi < 1/2$. There exists $c > 0$, which depends only on ξ, such that for any $n \geqslant 1$, we have*

$$\sum_{\substack{d<2^{\xi n}\\ d \text{ odd}}} \mu^2(d)4^{\omega(d)}|R_n(d)| \ll_\xi 2^n \exp(-c\sqrt{n}).$$

In order to prove Lemma 1.5, we define for any real numbers α and ϑ, the exponential sum

$$F_n(\alpha,\vartheta) = \frac{1}{|\mathcal{B}_n|}\sum_{a\in\mathcal{B}_n} \mathrm{e}\left(\alpha^{\overleftarrow{a}} - \vartheta a\right) \tag{1.11}$$

and for any integer $d \geqslant 1$ and $(h_1, h_2) \in \mathbb{Z}^2$,

$$H(d, h_1, h_2) = \sum_{\substack{0 \leqslant u,v < d \\ d \mid uv}} \mathrm{e}\left(\frac{h_1 u + h_2 v}{d}\right). \tag{1.12}$$

We show in Section 5 that to prove Lemma 1.5, it is enough to evaluate the sum

$$E = \sum_{\substack{d \leqslant D \\ \mu^2(d)=1 \\ \gcd(d,6)=1}} \frac{4^{\omega(d)}}{d^2} \sum_{0 < h_1, h_2 < d} |H(d, h_1, h_2)| \left| F_n\left(\frac{h_2}{d}, -\left(\frac{h_1}{d} + \frac{\ell}{3^j}\right)\right)\right|,$$

with $D = 2^{\xi n}$, $0 < \xi < 1/2$, $j \in \{0, 1\}$, $\ell \in \{0, \dots, 3^j - 1\}$.

We study $F_n(\alpha, \vartheta)$ in detail in Section 2. We strongly make use of the fact that $|F_n(\alpha, \vartheta)|$ can be written as a product of cosines (which is very common for exponential sums involving digital functions in base 2). Also, we combine the large sieve inequality and an extension of the Sobolev-Gallagher inequality to evaluate some discrete averages of F_n. Here we make the trivial observations that

$$\overline{F_n(\alpha, \vartheta)} = F_n(-\alpha, -\vartheta) = F_n(\vartheta, \alpha) \tag{1.13}$$

and

$$|F_n(\alpha, \vartheta)| \leqslant 1. \tag{1.14}$$

We note that for rational α and ϑ, the exponential sums $F_n(\alpha, \vartheta)$ have also been estimated in [2] via a different approach. However the bounds of [2] are not sufficient for our purpose.

The quantity $H(d, h_1, h_2)$ is studied in Section 3.

In Section 6, we use our estimates on $F_n(\vartheta, \alpha)$ and $H(d, h_1, h_2)$ to obtain the bound $E \ll_\xi \exp(-c_\xi \sqrt{n})$ for some constant $c_\xi > 0$ which depends only on ξ. We complete the proof of the main results in Section 7.

2. Study of $F_n(\alpha, \vartheta)$

2.1. Generalized Sobolev–Gallagher inequality.

We recall the following:

Definition 2.1. *We say that a sequence $(x_1, \dots, x_N) \in \mathbb{R}^N$ is δ-spaced modulo 1 if $\|x_i - x_j\| \geqslant \delta$ for $1 \leqslant i < j \leqslant N$.*

The Sobolev–Gallagher inequality (see [24, Section 3] for relevant references) is known for continuously differentiable functions. We extend it to functions of bounded variation (see for instance [33, p. 355]).

Lemma 2.2. *Let $f : \mathbb{R} \to \mathbb{R}$ be a 1-periodic continuous function of bounded variation, with total variation V_f on $[0,1]$. For $\delta > 0$ and any δ-spaced sequence $(x_1, \dots, x_N) \in \mathbb{R}^N$, we have*

$$\sum_{n=1}^{N} |f(x_n)| \leqslant \frac{1}{\delta} \int_0^1 |f(u)|\, du + \frac{1}{2}\mathsf{V}_f\,.$$

Proof. We adapt the proof in [24] with Stieltjes integrals. If $\widetilde{x}_n$ is the fractional part of $x_n - x_1 + \frac{\delta}{2}$ and $g(x) = f(x + x_1 - \frac{\delta}{2})$ then $\widetilde{x}_n \in [\frac{\delta}{2}, 1 - \frac{\delta}{2}]$, $g(\widetilde{x}_n) = f(x_n)$, and g is also a 1-periodic continuous function, with a bounded variation V_g on $[0,1]$, and $\mathsf{V}_g = \mathsf{V}_f$. It is sufficient to prove the result for $g(\widetilde{x}_n)$. Hence we may assume from now that $x_n \in [\frac{\delta}{2}, 1 - \frac{\delta}{2}]$. For $x \in [0,1]$ we denote by $\mathsf{V}_f(x)$ the total variation of f on $[0,x]$ (thus $\mathsf{V}_f(1) = \mathsf{V}_f$). Since f is continuous, by partial summation, for $n \in \{1, \dots, N\}$ we have

$$f(x_n) = \frac{1}{\delta}\int_{x_n - \frac{\delta}{2}}^{x_n + \frac{\delta}{2}} f(u)du + \int_{x_n - \frac{\delta}{2}}^{x_n} \left(\frac{u - x_n}{\delta} + \frac{1}{2}\right) df(u) + \int_{x_n}^{x_n + \frac{\delta}{2}} \left(\frac{u - x_n}{\delta} - \frac{1}{2}\right) df(u).$$

For $x_n - \frac{\delta}{2} \leqslant u \leqslant x_n$ we have

$$0 \leqslant \frac{u - x_n}{\delta} + \frac{1}{2} \leqslant \frac{1}{2}$$

and for $x_n \leqslant u \leqslant x_n + \frac{\delta}{2}$ we have

$$-\frac{1}{2} \leqslant \frac{u - x_n}{\delta} - \frac{1}{2} \leqslant 0.$$

Hence

$$|f(x_n)| \leqslant \frac{1}{\delta}\int_{x_n - \frac{\delta}{2}}^{x_n + \frac{\delta}{2}} |f(u)|\, du + \frac{1}{2}\int_{x_n - \frac{\delta}{2}}^{x_n} d\mathsf{V}_f(u) + \frac{1}{2}\int_{x_n}^{x_n + \frac{\delta}{2}} d\mathsf{V}_f(u).$$

Since the intervals $(x_n - \frac{\delta}{2}, x_n + \frac{\delta}{2})$ are non-overlapping modulo 1, it follows that

$$\begin{aligned}\sum_{n=1}^{N} |f(x_n)| &\leqslant \frac{1}{\delta}\int_0^1 |f(u)|\, du + \frac{1}{2}\int_0^1 d\mathsf{V}_f(u) \\ &= \frac{1}{\delta}\int_0^1 |f(u)|\, du + \frac{1}{2}\mathsf{V}_f,\end{aligned}$$

as desired. □

2.2. **Product formula.** We need the following useful identities for $F_n(\alpha, \vartheta)$ defined by (1.11).

Lemma 2.3. *For $(\alpha, \vartheta) \in \mathbb{R}^2$ and $n \geqslant 3$, we have*

$$|F_n(\alpha, \vartheta)| = |F_n(\vartheta, \alpha)| = \prod_{j=1}^{n-2} \left|U\left(\alpha 2^{n-1-j} - \vartheta 2^j\right)\right|,$$

where

$$U(x) = \frac{1 + \mathrm{e}\,(x)}{2}.$$

Proof. By writing

$$\begin{aligned} a &= 2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_1 2 + 1, \\ \overleftarrow{a} &= 1 + a_{n-2}2 + \cdots + a_1 2^{n-2} + 2^{n-1}, \end{aligned}$$

we obtain

$$F_n(\alpha, \vartheta) = \mathrm{e}\left((\alpha - \vartheta)(2^{n-1} + 1)\right) \prod_{j=1}^{n-2} U\left(\alpha 2^{n-1-j} - \vartheta 2^j\right).$$

It is also obvious that $F_n(\alpha, \vartheta) = \overline{F_n(\vartheta, \alpha)}$. □

Lemma 2.4. *For $(\alpha, \vartheta) \in \mathbb{R}^2$ and $3 \leqslant m \leqslant n-1$, we have*

$$|F_n(\alpha, \vartheta)| = |F_m(\alpha 2^{n-m}, \vartheta)| \cdot |F_{n-m+2}(\alpha, \vartheta 2^{m-2})|.$$

Proof. For $3 \leqslant m \leqslant n$, by Lemma 2.3, with the help of $k = n - 1 - j$ we can write

$$|F_n(\alpha, \vartheta)| = \left(\prod_{j=1}^{m-2} \left|U\left(\alpha 2^{n-1-j} - \vartheta 2^j\right)\right|\right) \left(\prod_{k=1}^{n-m} \left|U\left(\alpha 2^k - \vartheta 2^{n-1-k}\right)\right|\right),$$

while

$$\begin{aligned} |F_m(\alpha 2^{n-m}, \vartheta)| &= \prod_{j=1}^{m-2} \left|U\left(\alpha 2^{n-m} 2^{m-1-j} - \vartheta 2^j\right)\right| \\ &= \prod_{j=1}^{m-2} \left|U\left(\alpha 2^{n-1-j} - \vartheta 2^j\right)\right| \end{aligned}$$

and

$$|F_{n-m+2}(\vartheta 2^{m-2},\alpha)| = \prod_{k=1}^{n-m+2-2} \left|U\left(\vartheta 2^{m-2}2^{n-m+2-1-k}-\alpha 2^k\right)\right|$$
$$= \prod_{k=1}^{n-m} \left|U\left(\vartheta 2^{n-1-k}-\alpha 2^k\right)\right|.$$

Since

$$|F_{n-m+2}(\alpha,\vartheta 2^{m-2})| = |F_{n-m+2}(\vartheta 2^{m-2},\alpha)|$$

and $|U(\cdot)|$ is even, the result follows. □

2.3. **Pointwise bounds for F_n.** We use an idea of Col [9, Proof of Lemme 2] and sharpen the arguments of [9, Section 4.2] to get an upper bound for $|F_n(\alpha,\vartheta)|$.

Lemma 2.5. *For $(x,y,z)\in\mathbb{R}^3$ we have*

$$|U(x)U(y)U(z)| \leqslant \frac{1}{4}|U(x+y+z)| + \frac{3}{4}.$$

Proof. For $(x,y,z)\in\mathbb{R}^3$ we have

$$|U(x)U(y)U(z)| = \frac{1}{8}\big|1+\mathrm{e}(x)+\mathrm{e}(y)+\mathrm{e}(z)+\mathrm{e}(x+y)$$
$$+\mathrm{e}(x+z)+\mathrm{e}(y+z)+\mathrm{e}(x+y+z)\big|$$
$$\leqslant \frac{|1+\mathrm{e}(x+y+z)|+6}{8} = \frac{1}{4}|U(x+y+z)|+\frac{3}{4},$$

which concludes the proof. □

For any integer $N\geqslant 1$ and any $\vartheta\in\mathbb{R}$, we define

$$G_N(\vartheta) = \prod_{j=0}^{N-1}\left(\frac{1}{4}\left|U\left(\vartheta 2^j\right)\right|+\frac{3}{4}\right). \tag{2.1}$$

Lemma 2.6. *For any integer $n\geqslant 4$ and any $(\alpha,\vartheta)\in\mathbb{R}^2$, we have*

$$|F_n(\alpha,\vartheta)| \leqslant \prod_{j=1}^{n-3}\left(\frac{1}{4}\left|U\left(3\vartheta 2^j\right)\right|+\frac{3}{4}\right)^{1/3} = G_{n-3}^{1/3}(6\vartheta). \tag{2.2}$$

Proof. Applying Lemma 2.3 and writing

$$|F_n(\alpha,\vartheta)| = \prod_{j=1}^{n-2}\left|U\left(\alpha 2^{n-1-j}-\vartheta 2^j\right)\right|$$
$$\leqslant \prod_{j=1}^{n-3}\left|U\left(\alpha 2^{n-1-j}-\vartheta 2^j\right)\right|^{1/3}\prod_{j=2}^{n-2}\left|\overline{U\left(\alpha 2^{n-1-j}-\vartheta 2^j\right)}\right|^{2/3},$$

we get

$$|F_n(\alpha,\vartheta)| \leqslant \prod_{j=1}^{n-3} \left|U\left(\alpha 2^{n-1-j} - \vartheta 2^j\right) U^2\left(-\alpha 2^{n-2-j} + \vartheta 2^{j+1}\right)\right|^{1/3}.$$

Taking

$$x = \alpha 2^{n-1-j} - \vartheta 2^j \qquad \text{and} \qquad y = z = -\alpha 2^{n-2-j} + \vartheta 2^{j+1}$$

in Lemma 2.5 we obtain the desired estimate. □

Lemma 2.7. *For $q \in \mathbb{Z}$, $q \geqslant 2$ and $\vartheta \in \mathbb{R} \setminus \mathbb{Z}$, the integer*

$$j = \left\lfloor \frac{\log \frac{q}{(q+1)\|\vartheta\|}}{\log q} \right\rfloor$$

satisfies

$$\left\|q^j \vartheta\right\| \geqslant \frac{1}{q+1}.$$

Proof. Since $\|\vartheta\| \leqslant 1/2$, we have $j \geqslant 0$. Therefore $q^j \in \mathbb{Z}$ and we have $\|q^j\vartheta\| = \|q^j \|\vartheta\|\|$ by parity and periodicity. By definition of j, we have

$$\frac{1}{q+1} < q^j \|\vartheta\| \leqslant \frac{q}{q+1} = 1 - \frac{1}{q+1},$$

which gives the result. □

We are now ready to establish one of our main technical tools.

Lemma 2.8. *For $\alpha \in \mathbb{R}$ and $n, \ell, h, d \in \mathbb{Z}$ such that $n \geqslant 4$, $d \geqslant 5$, d is odd and $d \nmid 3h$, we have*

$$\left|F_n\left(\alpha, \frac{h}{d} + \frac{\ell}{3}\right)\right| \ll \exp\left(\frac{-c_0\, n}{\log\left(\frac{4d}{3}\right)}\right),$$

where

$$c_0 = \frac{1}{3}\log\left(\frac{8}{7}\right)\log 2 = 0.0308\ldots.$$

Proof. Since $|U(x)| = \cos\pi\|x\|$ for any $x \in \mathbb{R}$, we have by Lemma 2.6,

$$\begin{aligned}\left|F_n\left(\alpha, \frac{h}{d} + \frac{\ell}{3}\right)\right| &\leqslant \prod_{j=1}^{n-3}\left(\frac{1}{4}\cos\pi\left\|3\left(\frac{h}{d}+\frac{\ell}{3}\right)2^j\right\| + \frac{3}{4}\right)^{1/3} \\ &= \prod_{j=1}^{n-3}\left(\frac{1}{4}\cos\pi\left\|\frac{3h2^j}{d}\right\| + \frac{3}{4}\right)^{1/3}.\end{aligned}$$

Thus, defining

$$J = 1 + \left\lfloor \frac{\log\left(\frac{2d}{3}\right)}{\log 2} \right\rfloor \geqslant 1, \qquad K = \left\lfloor \frac{n-3}{J} \right\rfloor, \qquad \vartheta_k = \frac{3h2^{kJ+1}}{d}$$

for any integer k, we may write

$$\left| F_n\left(\alpha, \frac{h}{d} + \frac{\ell}{3}\right)\right| \leqslant \prod_{0\leqslant k<K} \prod_{0\leqslant j<J} \left(\frac{1}{4}\cos \pi \left\|2^j \vartheta_k\right\| + \frac{3}{4}\right)^{1/3}.$$

We fix $k \in \{0, \dots, K-1\}$. Since d is odd and $d \nmid 3h$, we have $\|\vartheta_k\| \geqslant \frac{1}{d}$. Thus, denoting

$$j_k = \left\lfloor \frac{\log \frac{2}{3\|\vartheta_k\|}}{\log 2} \right\rfloor,$$

we have

$$0 \leqslant j_k \leqslant J-1$$

and by Lemma 2.7,

$$\left\|2^{j_k}\vartheta_k\right\| \geqslant \frac{1}{3}.$$

It follows that

$$\left| F_n\left(\alpha, \frac{h}{d} + \frac{\ell}{3}\right)\right| \leqslant \prod_{0\leqslant k<K} \left(\frac{1}{4}\cos \pi \left\|2^{j_k} \vartheta_k\right\| + \frac{3}{4}\right)^{1/3} \leqslant \left(\frac{7}{8}\right)^{K/3}.$$

Since $J \leqslant \frac{\log\left(\frac{4d}{3}\right)}{\log 2}$, we have

$$K > \frac{n-3}{J} - 1 \geqslant \frac{(n-3)\log 2}{\log\left(\frac{4d}{3}\right)} - 1 = \frac{n \log 2}{\log\left(\frac{4d}{3}\right)} + O(1),$$

we get

$$\left| F_n\left(\alpha, \frac{h}{d} + \frac{\ell}{3}\right)\right| \leqslant \left(\frac{7}{8}\right)^{\frac{K}{3}} \ll \exp\left(\frac{-n \log\left(\frac{8}{7}\right)\log 2}{3\log\left(\frac{4d}{3}\right)}\right),$$

which completes the proof. □

2.4. **Bounds on some continuous averages.** To fix the ideas, it is interesting to note that by orthogonality we have

$$\int_0^1 |F_n(\alpha, \vartheta)|^2 \, d\vartheta = \frac{1}{|\mathcal{B}_n|^2} \int_0^1 \left| \sum_{a\in\mathcal{B}_n} \mathrm{e}\left(\alpha \overleftarrow{a} - \vartheta a\right)\right|^2 d\vartheta$$

$$= \frac{1}{|\mathcal{B}_n|^2} \sum_{a_1\in\mathcal{B}_n} \sum_{a_2\in\mathcal{B}_n} \mathrm{e}\left(\alpha(\overleftarrow{a_1} - \overleftarrow{a_2})\right) \int_0^1 \mathrm{e}\left(\vartheta(a_2 - a_1)\right) d\vartheta = \frac{1}{|\mathcal{B}_n|},$$

and by the Cauchy–Schwarz inequality this gives the trivial upper bound

$$\int_0^1 |F_n(\alpha,\vartheta)|\,d\vartheta \leqslant \left(\int_0^1 |F_n(\alpha,\vartheta)|^2\,d\vartheta\right)^{1/2} = \frac{1}{|\mathcal{B}_n|^{1/2}}.$$

The following estimate of G_N (defined by (2.1)) is a key argument in the sequel.

Lemma 2.9. *For any integer $N \geqslant 1$ and any real number $\kappa \in [0,1]$, we have*

$$\int_0^1 G_N^\kappa(\vartheta)d\vartheta \leqslant C(\kappa)^N,$$

where

$$C(\kappa) = \left(\frac{\sqrt{2}}{8} + \frac{3}{4}\right)^\kappa.$$

Proof. For any $N \geqslant 1$, we have

$$\begin{aligned}
\int_0^1 G_N^\kappa(\vartheta)d\vartheta &= \int_0^1 \left(\frac{1}{4}\left|U\left(\vartheta\right)\right| + \frac{3}{4}\right)^\kappa G_{N-1}^\kappa(2\vartheta)d\vartheta \\
&= \int_0^{1/2} \left(\frac{1}{4}\left|U\left(\vartheta\right)\right| + \frac{3}{4}\right)^\kappa G_{N-1}^\kappa(2\vartheta)d\vartheta \\
&\qquad + \int_0^{1/2} \left(\frac{1}{4}\left|U\left(\vartheta+\frac{1}{2}\right)\right| + \frac{3}{4}\right)^\kappa G_{N-1}^\kappa(2\vartheta)d\vartheta \\
&= \int_0^1 \left(\frac{1}{4}\left|U\left(\frac{\vartheta}{2}\right)\right| + \frac{3}{4}\right)^\kappa G_{N-1}^\kappa(\vartheta)\frac{d\vartheta}{2} \\
&\qquad + \int_0^1 \left(\frac{1}{4}\left|U\left(\frac{\vartheta+1}{2}\right)\right| + \frac{3}{4}\right)^\kappa G_{N-1}^\kappa(\vartheta)\frac{d\vartheta}{2} \\
&= \int_0^1 \Phi_\kappa(\vartheta) G_{N-1}^\kappa(\vartheta)d\vartheta,
\end{aligned}$$

where

$$\Phi_\kappa(\vartheta) = \frac{1}{2}\left(\frac{1}{4}\left|U\left(\frac{\vartheta}{2}\right)\right| + \frac{3}{4}\right)^\kappa + \frac{1}{2}\left(\frac{1}{4}\left|U\left(\frac{\vartheta+1}{2}\right)\right| + \frac{3}{4}\right)^\kappa.$$

Since $x \mapsto x^\kappa$ is concave for $0 \leqslant \kappa \leqslant 1$ and $|\cos x| + |\sin x| \leqslant \sqrt{2}$, we have

$$\begin{aligned}\Phi_\kappa(\vartheta) &\leqslant \left(\frac{1}{2}\left(\frac{1}{4}\left|U\left(\frac{\vartheta}{2}\right)\right| + \frac{3}{4}\right) + \frac{1}{2}\left(\frac{1}{4}\left|U\left(\frac{\vartheta+1}{2}\right)\right| + \frac{3}{4}\right)\right)^\kappa \\ &= \left(\frac{1}{8}\left(\left|U\left(\frac{\vartheta}{2}\right)\right| + \left|U\left(\frac{\vartheta+1}{2}\right)\right|\right) + \frac{3}{4}\right)^\kappa \\ &= \left(\frac{1}{8}\left(\left|\cos\frac{\pi\vartheta}{2}\right| + \left|\sin\frac{\pi\vartheta}{2}\right|\right) + \frac{3}{4}\right)^\kappa \\ &\leqslant \left(\frac{\sqrt{2}}{8} + \frac{3}{4}\right)^\kappa = C(\kappa).\end{aligned}$$

We have proved that

$$\int_0^1 G_N^\kappa(\vartheta)d\vartheta \leqslant C(\kappa)\int_0^1 G_{N-1}^\kappa(\vartheta)d\vartheta.$$

By induction, it follows that

$$\int_0^1 G_N^\kappa(\vartheta)d\vartheta \leqslant C(\kappa)^N \int_0^1 G_0^\kappa(\vartheta)d\vartheta = C(\kappa)^N$$

which completes the proof. □

Lemma 2.10. *For any integer $N \geqslant 1$ and any real number $\kappa > 0$, G_N^κ admits almost everywhere a derivative $(G_N^\kappa)'$ which satisfies*

$$\left\|(G_N^\kappa)'\right\|_1 \leqslant \frac{\kappa\pi}{3}\, 2^N \left\|G_N^\kappa\right\|_1.$$

Proof. Since

$$G_N(\vartheta) = \prod_{j=0}^{N-1}\left(\frac{1}{4}\left|\cos(\pi\vartheta 2^j)\right| + \frac{3}{4}\right),$$

we have for almost all $\vartheta \in \mathbb{R}$,

$$\left|(G_N^\kappa)'(\vartheta)\right| \leqslant |G_N^\kappa(\vartheta)| \sum_{j=0}^{N-1} \frac{\kappa\frac{\pi 2^j}{4}\left|\sin(\pi\vartheta 2^j)\right|}{\frac{1}{4}\left|\cos\left(\pi\vartheta 2^j\right)\right| + \frac{3}{4}} \leqslant \frac{\kappa\pi}{3} 2^N \left|G_N^\kappa(\vartheta)\right|$$

and the result follows. □

2.5. **Bounds on some discrete averages of F_n.** For a triple $\mathcal{D} = (D_1, D_2, D_3)$ we define the set

$$\mathfrak{D}(\mathcal{D}) = \big\{(d_1,d_2,d_3) \in \mathbb{N}^3 :\ d_1 \sim D_1,\ d_2 \sim D_2,\ d_3 \sim D_3,\ \gcd(d_1d_2d_3, 6) = 1\big\},$$

and for

$$\mathbf{d} = (d_1, d_2, d_3) \in \mathfrak{D}(\mathcal{D})$$

we define

$$\mathfrak{H}(\mathbf{d}) = \big\{(h_1, h_2) \in \mathbb{N}^2 : \ 0 < h_1 < d_2 d_3, \ 0 < h_2 < d_1 d_3, \\ \gcd(h_1, d_2 d_3) = \gcd(h_2, d_1 d_3) = 1\big\}.$$

Finally, for $\mathcal{D} = (D_1, D_2, D_3)$, $\boldsymbol{\ell} = (\ell_1, \ell_2) \in \mathbb{Z}^2$ and $r \in \{1, 2\}$, we define

$$M_r(n; \mathcal{D}, \boldsymbol{\ell}) \\ = \sum_{\mathbf{d} \in \mathfrak{D}(\mathcal{D})} \sum_{(h_1, h_2) \in \mathfrak{H}(\mathbf{d})} \left| F_n\left(\frac{h_2}{d_1 d_3} + \frac{\ell_1}{3}, -\frac{h_1}{d_2 d_3} - \frac{\ell_2}{3}\right)\right|^r. \tag{2.3}$$

Let us introduce the non-decreasing function $\widetilde{\tau}$ defined by

$$\widetilde{\tau}(t) = \max_{d \leqslant t} \tau(d), \qquad t \in [1, +\infty)$$

and observe that, for any positive integer d,

$$2^{\omega(d)} \leqslant \tau(d) \leqslant \widetilde{\tau}(d). \tag{2.4}$$

Recalling the definition of $C(\kappa)$ from Lemma 2.9, we define

$$\eta_0 = -\frac{\log C(2/3)}{\log 2} \approx 0.073\ldots.$$

In order to bound $M_1(n; \mathcal{D}, \boldsymbol{\ell})$, we first establish the following bound on $M_2(n; \mathcal{D}, \boldsymbol{\ell})$.

Lemma 2.11. *For any $n \geqslant 10$, any $\mathcal{D} = (D_1, D_2, D_3) \in [1, +\infty)^3$ and any $\varepsilon \in (0, 1]$ such that*

$$D_1^2 D_2^{2\varepsilon} D_3^{1+\varepsilon} \leqslant 2^{n-10}, \tag{2.5}$$

we have for any $\boldsymbol{\ell} = (\ell_1, \ell_2) \in \mathbb{Z}^2$,

$$\frac{M_2(n; \mathcal{D}, \boldsymbol{\ell})}{D_1 D_2 D_3^2} \ll \widetilde{\tau}(4 D_2 D_3) \frac{D_2}{D_1} \left(D_2^2 D_3\right)^{-\varepsilon \eta_0},$$

where the implicit constant is absolute.

Proof. We introduce two integer parameters $n_1, n_2 \geqslant 4$ such that $n_1 + n_2 \leqslant n$. Applying Lemma 2.4 twice and recalling (1.14), we derive that there exists $(u, v) \in \mathbb{N}^2$ such that for any $(\alpha, \vartheta) \in \mathbb{R}^2$,

$$|F_n(\alpha, \vartheta)| \leqslant |F_{n_1}(\alpha 2^u, \vartheta)| \cdot |F_{n_2}(\alpha, \vartheta 2^v)|. \tag{2.6}$$

Furthermore, by (2.2), we have

$$|F_n(\alpha, \vartheta)| \leqslant G_{n_1-3}^{1/3}(6\vartheta) \cdot |F_{n_2}(\alpha, \vartheta 2^v)|.$$

Moreover, since G_{n_1-3} is 1-periodic and even, we have

$$G_{n_1-3}\left(6\left(-\frac{h_1}{d_2d_3}-\frac{\ell_2}{3}\right)\right)=G_{n_1-3}\left(\frac{6h_1}{d_2d_3}\right).$$

Hence,

$$M_2(n;\mathcal{D},\boldsymbol{\ell})\leqslant \sum_{\mathbf{d}\in\mathfrak{D}(\mathcal{D})}\sum_{(h_1,h_2)\in\mathfrak{H}(\mathbf{d})} G_{n_1-3}^{2/3}\left(\frac{6h_1}{d_2d_3}\right)\times \left|F_{n_2}\left(\frac{h_2}{d_1d_3}+\frac{\ell_1}{3},-\frac{h_12^v}{d_2d_3}-\frac{\ell_22^v}{3}\right)\right|^2.$$

For given d_3 and ℓ_1, the points

$$\frac{h_2}{d_1d_3}+\frac{\ell_1}{3},\qquad d_1\sim D_1,\ 0<h_2<d_1d_3,\ \gcd(h_2,d_1d_3)=1,$$

are $(8D_1^2D_3)^{-1}$-spaced modulo 1. By summing over d_1 and h_2, we obtain by the large sieve inequality (see for instance [24]),

$$M_2(n;\mathcal{D},\boldsymbol{\ell})\ll \sum_{\substack{d_2\sim D_2\\ d_3\sim D_3\\ \gcd(d_2d_3,6)=1}}\sum_{\substack{0<h_1<d_2d_3\\ \gcd(h_1,d_2d_3)=1}} G_{n_1-3}^{2/3}\left(\frac{6h_1}{d_2d_3}\right)(D_1^2D_32^{-n_2}+1).$$

Since $\gcd(d_2d_3,6)=1$, we have by a change of variable,

$$M_2(n;\mathcal{D},\boldsymbol{\ell})\ll (D_1^2D_32^{-n_2}+1)\sum_{\substack{d_2\sim D_2\\ d_3\sim D_3\\ \gcd(d_2d_3,6)=1}}\sum_{\substack{0<h_1<d_2d_3\\ \gcd(h_1,d_2d_3)=1}} G_{n_1-3}^{2/3}\left(\frac{h_1}{d_2d_3}\right).$$

Writing

$$\tau(d;D_2,D_3)=\left|\{(d_2,d_3):d_2\sim D_2,d_3\sim D_3,d=d_2d_3\}\right|,$$

we have

$$\begin{aligned}M_2(n;\mathcal{D},\boldsymbol{\ell})&\\ &\ll \left(D_1^2D_32^{-n_2}+1\right)\sum_{d\in[D_2D_3,4D_2D_3)}\tau(d;D_2,D_3)\\ &\qquad\qquad\sum_{\substack{0<h_1<d\\ \gcd(h_1,d)=1}} G_{n_1-3}^{2/3}\left(\frac{h_1}{d}\right),\end{aligned}$$

and observing that by (2.4) we have

$$\tau(d;D_2,D_3)\leqslant\tau(d)\leqslant\widetilde{\tau}(d)\leqslant\widetilde{\tau}(4D_2D_3),$$

we immediately derive

$$M_2(n;\mathcal{D},\boldsymbol{\ell}) \ll \widetilde{\tau}(4D_2D_3)\left(D_1^2D_3 2^{-n_2}+1\right)\sum_{d\in[D_2D_3,4D_2D_3)}\sum_{\substack{0<h_1<d\\ \gcd(h_1,d)=1}} G_{n_1-3}^{2/3}\left(\frac{h_1}{d}\right).$$

By Lemma 2.9, we have

$$\left\|G_{n_1-3}^{2/3}\right\|_1 \ll C(2/3)^{n_1} = 2^{-n_1\eta_0}$$

and by Lemma 2.10, the variation of $G_{n_1-3}^{2/3}$ on $[0,1]$ is

$$\mathsf{V}_{G_{n_1-3}^{2/3}} \ll 2^{n_1}\left\|G_{n_1-3}^{2/3}\right\|_1.$$

Since the points h_1/d are $(16D_2^2D_3^2)^{-1}$-spaced modulo 1, it follows from Lemma 2.2 that

$$M_2(n;\mathcal{D},\boldsymbol{\ell}) \ll \widetilde{\tau}(4D_2D_3)\left(D_1^2D_3 2^{-n_2}+1\right)\left(D_2^2D_3^2+2^{n_1}\right)2^{-n_1\eta_0}.$$

We choose for n_1 and n_2 the unique integers such that

$$2^{n_1-5} < (D_2^2D_3)^{\varepsilon} \leqslant 2^{n_1-4}, \quad 2^{n_2-5} < D_1^2D_3 \leqslant 2^{n_2-4}.$$

Since $D_1, D_2, D_3 \geqslant 1$ we have $n_1 \geqslant 4$, $n_2 \geqslant 4$ and by (2.5) we have $n_1+n_2 \leqslant n$. Since $\varepsilon \in (0,1]$, this leads to

$$M_2(n;\mathcal{D},\boldsymbol{\ell}) \ll \widetilde{\tau}(4D_2D_3)D_2^2D_3^2\left(D_2^2D_3\right)^{-\varepsilon\eta_0}$$

and completes the proof. □

We are now able to bound $M_1(n;\mathcal{D},\boldsymbol{\ell})$.

Lemma 2.12. *For any $n \geqslant 22$, any $\mathcal{D} = (D_1,D_2,D_3) \in [1,+\infty)^3$ and any $\varepsilon \in (0,1]$ such that*

$$(D_1D_2D_3)^{2(1+\varepsilon)} \leqslant 2^{n-22}, \tag{2.7}$$

we have for any $\boldsymbol{\ell} = (\ell_1,\ell_2) \in \mathbb{Z}^2$,

$$\frac{M_1(n;\mathcal{D},\boldsymbol{\ell})}{D_1D_2D_3^2} \ll \widetilde{\tau}(4D_1D_3)^{1/2}\widetilde{\tau}(4D_2D_3)^{1/2}\left(D_1D_2D_3\right)^{-\varepsilon\eta_0},$$

where the implicit constant is absolute.

Proof. Let $n_1, n_2 \geqslant 10$ such that $n_1+n_2 \leqslant n$. Similarly to (2.6), we see that there exists $(u,v) \in \mathbb{N}^2$ such that for any $(\alpha,\vartheta) \in \mathbb{R}^2$,

$$|F_n(\alpha,\vartheta)| \leqslant |F_{n_1}(\alpha 2^u,\vartheta)| \cdot |F_{n_2}(\alpha,\vartheta 2^v)|.$$

It is convenient to define

$$(u_1,v_1) = (u,0) \qquad \text{and} \qquad (u_2,v_2) = (0,v).$$

Applying the Cauchy–Schwarz inequality, we get

$$M_1(n;\mathcal{D},\boldsymbol{\ell})^2 \leqslant \prod_{k=1}^{2} \sum_{\mathbf{d}\in\mathfrak{D}(\mathcal{D})} \sum_{(h_1,h_2)\in\mathfrak{H}(\mathbf{d})} \left| F_{n_k}\left(\frac{h_2 2^{u_k}}{d_1d_3}+\frac{\ell_1 2^{u_k}}{3}, -\frac{h_1 2^{v_k}}{d_2d_3}-\frac{\ell_2 2^{v_k}}{3}\right)\right|^2.$$

The maps $\alpha \mapsto F_{n_k}(\alpha,\vartheta)$ and $\vartheta \mapsto F_{n_k}(\alpha,\vartheta)$ are 1-periodic, and since

$$\gcd(2^{u_k}, d_1d_3) = \gcd(2^{v_k}, d_2d_3) = 1,$$

the integer $h_1 2^{v_k}$ runs over all residue classes modulo d_2d_3 coprime with d_2d_3 and $h_2 2^{u_k}$ runs over all residue classes modulo d_1d_3 coprime with d_1d_3. Therefore, by a change of variables we obtain

$$\begin{aligned} M_1(n;\mathcal{D},\boldsymbol{\ell})^2 &\leqslant \prod_{k=1}^{2} \sum_{\mathbf{d}\in\mathfrak{D}(\mathcal{D})} \sum_{(h_1,h_2)\in\mathfrak{H}(\mathbf{d})} \left| F_{n_k}\left(\frac{h_2}{d_1d_3}+\frac{\ell_1 2^{u_k}}{3}, -\frac{h_1}{d_2d_3}-\frac{\ell_2 2^{v_k}}{3}\right)\right|^2 \\ &= \prod_{k=1}^{2} M_2(n_k;\mathcal{D},\boldsymbol{\ell}_k), \end{aligned}$$

where $\boldsymbol{\ell}_k = (\ell_1 2^{u_k}, \ell_2 2^{v_k})$. We choose for n_1 and n_2 the unique integers such that

$$2^{n_1-11} < D_1^2 D_2^{2\varepsilon} D_3^{1+\varepsilon} \leqslant 2^{n_1-10}, \quad 2^{n_2-10} < D_1^{2\varepsilon} D_2^2 D_3^{1+\varepsilon} \leqslant 2^{n_2-10}.$$

Since $D_1, D_2, D_3 \geqslant 1$ we have $n_1 \geqslant 10$, $n_2 \geqslant 10$ and by (2.7) we have $n_1+n_2 \leqslant n$. By applying Lemma 2.11 with n replaced by n_1, we obtain

$$\frac{M_2(n_1;\mathcal{D},\boldsymbol{\ell}_1)}{D_1D_2D_3^2} \ll \widetilde{\tau}(4D_2D_3)\frac{D_2}{D_1}\left(D_2^2D_3\right)^{-\varepsilon\eta_0}.$$

To bound $M_2(n_2;\mathcal{D},\boldsymbol{\ell}_2)$, we first note that by (1.13), we have

$$M_2(n_2;\mathcal{D},\boldsymbol{\ell}_2) = M_2(n_2;\widetilde{\mathcal{D}},\widetilde{\boldsymbol{\ell}}_2),$$

where $\widetilde{\mathcal{D}} = (D_2, D_1, D_3)$ and $\widetilde{\boldsymbol{\ell}}_2 = (\ell_2 2^{v_2}, \ell_1 2^{u_2})$. Next, by applying Lemma 2.11 with n, $\mathcal{D}$ and $\boldsymbol{\ell}$ replaced by n_2, $\widetilde{\mathcal{D}}$ and $\widetilde{\boldsymbol{\ell}}_2$, we get

$$\frac{M_2(n_2;\mathcal{D},\boldsymbol{\ell}_2)}{D_1D_2D_3^2} \ll \widetilde{\tau}(4D_1D_3)\frac{D_1}{D_2}\left(D_1^2D_3\right)^{-\varepsilon\eta_0}.$$

It follows that

$$\frac{M_1(n;\mathcal{D},\boldsymbol{\ell})^2}{(D_1D_2D_3^2)^2} \ll \widetilde{\tau}(4D_1D_3)\widetilde{\tau}(4D_2D_3)\left(D_1D_2D_3\right)^{-2\varepsilon\eta_0},$$

as desired. □

3. Study of $H(d, h_1, h_2)$

We recall that, by (1.12), for any integer $d \geqslant 1$ and $(h_1, h_2) \in \mathbb{Z}^2$,

$$H(d, h_1, h_2) = \sum_{\substack{0 \leqslant u,v < d \\ d \mid uv}} \mathrm{e}\left(\frac{h_1 u + h_2 v}{d}\right).$$

Lemma 3.1. *For any $(h_1, h_2) \in \mathbb{Z}^2$ the function $d \mapsto H(d, h_1, h_2)$ is multiplicative and for any prime number p, we have*

$$H(p, h_1, h_2) = p\mathbf{1}_{p \mid h_1} + p\mathbf{1}_{p \mid h_2} - 1.$$

Proof. For $d_1 \geqslant 1$ and $d_2 \geqslant 1$ with $\gcd(d_1, d_2) = 1$ the summation over u with $0 \leqslant u < d = d_1 d_2$ may be replaced by $d_2 u_1 + d_1 u_2$ with $0 \leqslant u_1 < d_1$, $0 \leqslant u_2 < d_2$ and similarly for v. We have

$$\begin{aligned}
\frac{h_1 u}{d} &\equiv \frac{h_1(d_2 u_1 + d_1 u_2)}{d_1 d_2} \equiv \frac{h_1 u_1}{d_1} + \frac{h_1 u_2}{d_2} \bmod 1,\\
\frac{h_2 v}{d} &\equiv \frac{h_2(d_2 v_1 + d_1 v_2)}{d_1 d_2} \equiv \frac{h_2 v_1}{d_1} + \frac{h_2 v_2}{d_2} \bmod 1,
\end{aligned}$$

and also

$$\begin{aligned}
uv &\equiv (d_2 u_1 + d_1 u_2)(d_2 v_1 + d_1 v_2) \equiv d_2^2 u_1 v_1 \bmod d_1,\\
uv &\equiv (d_2 u_1 + d_1 u_2)(d_2 v_1 + d_1 v_2) \equiv d_1^2 u_2 v_2 \bmod d_2.
\end{aligned}$$

Since $\gcd(d_1, d_2) = 1$, the condition $d_1 d_2 \mid uv$, may be replaced by $d_1 \mid u_1 v_1$ and $d_2 \mid u_2 v_2$. This leads to

$$\begin{aligned}
&H(d_1 d_2, h_1, h_2)\\
&\quad= \sum_{\substack{0 \leqslant u_1, v_1 < d_1 \\ d_1 \mid u_1 v_1}} \mathrm{e}\left(\frac{h_1 u_1 + h_2 v_1}{d_1}\right) \sum_{\substack{0 \leqslant u_2, v_2 < d_2 \\ d_2 \mid u_2 v_2}} \mathrm{e}\left(\frac{h_1 u_2 + h_2 v_2}{d_2}\right),\\
&\quad= H(d_1, h_1, h_2)\, H(d_2, h_1, h_2),
\end{aligned}$$

which shows that $d \mapsto H(d, h_1, h_2)$ is multiplicative.

If $d = p$ is a prime number then $p \mid uv$ means $p \mid u$ or $p \mid v$, namely $u = 0$ or $v = 0$, hence

$$\begin{aligned}
H(p, h_1, h_2) &= \sum_{0 \leqslant v < p} \mathrm{e}\left(\frac{h_2 v}{p}\right) + \sum_{0 \leqslant u < p} \mathrm{e}\left(\frac{h_1 u}{p}\right) - 1\\
&= p\mathbf{1}_{p \mid h_1} + p\mathbf{1}_{p \mid h_2} - 1,
\end{aligned}$$

as claimed. □

We now recall the definition (1.8) of the multiplicative function $f(d)$.

Lemma 3.2. *For any squarefree integer $d \geqslant 1$ such that $\gcd(d,6)=1$, we have*

$$H(d,0,0) = df(d).$$

Proof. For any prime number $p \geqslant 5$, we have

$$H(p,0,0) = 2p-1 = pf(p),$$

and the result now follows from the multiplicativity of the functions $H(d,0,0)$ and $f(d)$. □

4. Average order of useful multiplicative functions

We use the following upper bounds in the proof of Lemma 1.5.

Lemma 4.1. *For any real numbers $z>0$ and $x \geqslant 2$, we have*

$$\sum_{n\leqslant x} \frac{\mu^2(n) z^{\omega(n)}}{n} \ll_z (\log x)^z \tag{4.1}$$

and

$$\sum_{n\leqslant x} \mu^2(n) z^{\omega(n)} \ll_z x(\log x)^{z-1}. \tag{4.2}$$

Stronger results may be obtained by [25, Corollary 2.15] and [32, Chapter II, Theorem 6.1].

Proof. Since $n \mapsto \mu^2(n) z^{\omega(n)}$ is multiplicative with non negative values, we have

$$\sum_{n\leqslant x} \frac{\mu^2(n) z^{\omega(n)}}{n} \leqslant \prod_{p\leqslant x} \left(1 + \frac{\mu^2(p) z^{\omega(p)}}{p}\right) = \prod_{p\leqslant x} \left(1+\frac{z}{p}\right)$$

and by Mertens formula,

$$\sum_{p\leqslant x} \log\left(1+\frac{z}{p}\right) \leqslant z \sum_{p\leqslant x} \frac{1}{p} = z\left(\log\log x + O(1)\right).$$

This shows (4.1). In order to prove (4.2), we first write

$$(\log x) \sum_{n\leqslant x} \mu^2(n) z^{\omega(n)} = S_1(x) + S_2(x),$$

where

$$S_1(x) = \sum_{n\leqslant x} \mu^2(n) z^{\omega(n)} \log n \quad \text{and} \quad S_2(x) = \sum_{n\leqslant x} \mu^2(n) z^{\omega(n)} \log \frac{x}{n}.$$

Since $\mu^2(n)\log n = \mu^2(n)\sum_{p\mid n}\log p$ and $\sum_{p\leqslant X}\log p \ll X$, we obtain

$$S_1(x) = \sum_{p\leqslant x}\log p \sum_{m\leqslant x/p}\mu^2(mp)z^{\omega(mp)} = \sum_{p\leqslant x}\log p \sum_{\substack{m\leqslant x/p\\ p\nmid m}}\mu^2(m)z^{1+\omega(m)}$$

$$\leqslant \sum_{m\leqslant x}\mu^2(m)z^{1+\omega(m)}\sum_{p\leqslant x/m}\log p \ll_z x\sum_{m\leqslant x}\frac{\mu^2(m)z^{\omega(m)}}{m}.$$

Moreover since $\log\frac{x}{n}\leqslant\frac{x}{n}$, the same bound also holds for $S_2(x)$. By (4.1), it follows that

$$\sum_{n\leqslant x}\mu^2(n)z^{\omega(n)} \ll_z \frac{x}{\log x}\sum_{n\leqslant x}\frac{\mu^2(n)z^{\omega(n)}}{n} \ll_z x(\log x)^{z-1}$$

which establishes (4.2). □

5. Preliminary study of $R_n(d)$

We recall that $R_n(d)$ is defined by (1.7) together with (1.6). It is convenient to define for $j\in\{0,1\}$ and $d\geqslant 1$:

$$\widetilde{R}_n(d,j) = \frac{|\mathcal{B}_n|}{3^j d^2}\sum_{0<h_1,h_2<d}\overline{H(d,h_1,h_2)} \sum_{0\leqslant\ell<3^j} F_n\left(\frac{h_2}{d}, -\left(\frac{h_1}{d}+\frac{\ell}{3^j}\right)\right). \tag{5.1}$$

We note that for $j\in\{0,1\}$, $\widetilde{R}_n(1,j)=0$.

Lemma 5.1. *For any squarefree integer $d\geqslant 1$ such that $\gcd(d,6)=1$ and any $j\in\{0,1\}$, we have*

$$R_n(3^j d) = \widetilde{R}_n(d,j) + O\left(f(d)\right).$$

Proof. Let $j\in\{0,1\}$. By multiplicativity, we have

$$\frac{f(3^j d)}{3^j d} = \frac{f(3^j)f(d)}{3^j d} = \frac{f(d)}{3^j d},$$

hence, recalling (1.7), we obtain

$$R_n(3^j d) = T_n(3^j d) - \frac{f(3^j d)}{3^j d}\,|\mathcal{B}_n| = T_n(3^j d) - \frac{f(d)}{3^j d}\,|\mathcal{B}_n|.$$

Since $\overleftarrow{a}\equiv(-1)^{n-1}a \bmod 3$, recalling the definition (1.6) we may also write

$$T_n(3^j d) = \left|\{a\in\mathcal{B}_n:\ d\mid a\overleftarrow{a} \text{ and } 3^j\mid a\}\right|.$$

We now filter the integers $a \in \mathcal{B}_n$ according to the residue classes of a and $\overleftarrow{a}$ modulo d:

$$T_n(3^j d) = \sum_{\substack{0 \leqslant u,v<d \\ uv \equiv 0 \bmod d}} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \mathbf{1}_{a \equiv u \bmod d} \mathbf{1}_{\overleftarrow{a} \equiv v \bmod d},$$

and using the orthogonality of exponential functions to control the conditions $a \equiv u \bmod d$ and $\overleftarrow{a} \equiv v \bmod d$, we obtain

$$\begin{aligned} T_n(3^j d) &= \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \frac{1}{d^2} \sum_{0 \leqslant h_1,h_2<d} \mathrm{e}\left(\frac{h_1(a-u) + h_2(\overleftarrow{a} - v)}{d}\right) \\ &= T_{n,0}(3^j d) + T_{n,1}(3^j d) + T_{n,2}(3^j d) - T_{n,3}(3^j d) \end{aligned}$$

with

$$T_{n,0}(3^j d) = \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \frac{1}{d^2} \sum_{0 < h_1,h_2<d} \mathrm{e}\left(\frac{h_1(a-u) + h_2(\overleftarrow{a} - v)}{d}\right),$$

$$T_{n,1}(3^j d) = \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \frac{1}{d^2} \sum_{0 \leqslant h_2<d} \mathrm{e}\left(\frac{h_2(\overleftarrow{a} - v)}{d}\right),$$

$$T_{n,2}(3^j d) = \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \frac{1}{d^2} \sum_{0 \leqslant h_1<d} \mathrm{e}\left(\frac{h_1(a-u)}{d}\right),$$

$$T_{n,3}(3^j d) = \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \frac{1}{d^2}.$$

Note that $T_{n,3}(3^j d)$ compensates for double counting of the term corresponding to $h_1 = h_2 = 0$, which is counted in both $T_{n,1}(3^j d)$ and $T_{n,2}(3^j d)$. By Lemma 3.2, we have

$$\sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} 1 = H(d,0,0) = d f(d).$$

It follows that

$$T_{n,3}(3^j d) = \frac{f(d)}{d} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} 1 = \frac{f(d)}{d} \frac{|\mathcal{B}_n|}{3^j} + O\left(\frac{f(d)}{d}\right).$$

Moreover, since $a \equiv 0 \bmod 3^j$ is equivalent to $\overleftarrow{a} \equiv 0 \bmod 3^j$, we have

$$T_{n,1}(3^j d) = \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \frac{1}{d} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \mathbf{1}_{\overleftarrow{a} \equiv v \bmod d} = \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \frac{1}{d} \left(\frac{|\mathcal{B}_n|}{3^j d} + O(1) \right)$$
$$= \frac{f(d)}{d} \frac{|\mathcal{B}_n|}{3^j} + O\left(f(d)\right).$$

Similarly, we obtain

$$T_{n,2}(3^j d) = \frac{f(d)}{d} \frac{|\mathcal{B}_n|}{3^j} + O\left(f(d)\right).$$

For $T_{n,0}(3^j d)$, we write

$$T_{n,0}(3^j d)$$
$$= \frac{1}{d^2} \sum_{0<h_1,h_2<d} \sum_{\substack{0 \leqslant u,v<d \\ d \mid uv}} \mathrm{e}\left(\frac{-h_1 u - h_2 v}{d}\right) \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \mathrm{e}\left(\frac{h_1 a + h_2 \overleftarrow{a}}{d}\right)$$
$$= \frac{1}{d^2} \sum_{0<h_1,h_2<d} \overline{H(d,h_1,h_2)} \sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \mathrm{e}\left(\frac{h_1 a + h_2 \overleftarrow{a}}{d}\right),$$

where for any h_1, h_2,

$$\sum_{\substack{a \in \mathcal{B}_n \\ a \equiv 0 \bmod 3^j}} \mathrm{e}\left(\frac{h_1 a + h_2 \overleftarrow{a}}{d}\right) = \frac{1}{3^j} \sum_{0 \leqslant \ell < 3^j} \sum_{a \in \mathcal{B}_n} \mathrm{e}\left(\frac{h_1 a + h_2 \overleftarrow{a}}{d} + \frac{\ell a}{3^j}\right)$$
$$= \frac{|\mathcal{B}_n|}{3^j} \sum_{0 \leqslant \ell < 3^j} F_n\left(\frac{h_2}{d}, -\left(\frac{h_1}{d} + \frac{\ell}{3^j}\right)\right)$$

so that

$$T_{n,0}(3^j d) = \widetilde{R}_n(d,j).$$

This completes the proof. □

Lemma 5.2. *For any real number $D \geqslant 2$, we have*

$$\sum_{\substack{d<D \\ d \text{ odd}}} \mu^2(d) 4^{\omega(d)} |R_n(d)|$$
$$\ll D(\log D)^7 + \max_{j \in \{0,1\}} \sum_{\substack{d<D \\ \gcd(d,6)=1}} \mu^2(d) 4^{\omega(d)} |\widetilde{R}_n(d,j)|.$$

Proof. By splitting the sum over d according to $\gcd(d,3)$, we obtain

$$\sum_{\substack{d<D\\ \mu^2(d)=1\\ d \text{ odd}}} 4^{\omega(d)}|R_n(d)| = \sum_{\substack{d<D\\ \mu^2(d)=1\\ \gcd(d,6)=1}} 4^{\omega(d)}|R_n(d)| + \sum_{\substack{d<D/3\\ \mu^2(d)=1\\ \gcd(d,6)=1}} 4^{\omega(3d)}|R_n(3d)|$$
$$\leqslant 5 \max_{j\in\{0,1\}} \sum_{\substack{d<D\\ \mu^2(d)=1\\ \gcd(d,6)=1}} 4^{\omega(d)}|R_n(3^j d)|.$$

It follows from Lemma 5.1 that for $j \in \{0,1\}$,

$$\sum_{\substack{d<D\\ \mu^2(d)=1\\ \gcd(d,6)=1}} 4^{\omega(d)}|R_n(3^j d)| \ll \sum_{\substack{d<D\\ \mu^2(d)=1\\ \gcd(d,6)=1}} 4^{\omega(d)}|\widetilde{R}_n(d,j)| + \sum_{\substack{d<D\\ \mu^2(d)=1}} 4^{\omega(d)} f(d).$$

Since $f(d) < 2^{\omega(d)}$ for any squarefree integer d (this follows from the multiplicativity of f and $f(p) < 2$), we have by (4.2),

$$\sum_{\substack{d<D\\ \mu^2(d)=1}} 4^{\omega(d)} f(d) \leqslant \sum_{\substack{d<D\\ \mu^2(d)=1}} 8^{\omega(d)} \ll D(\log D)^7.$$

Combining the previous estimates, we get

$$\sum_{\substack{d<D\\ \mu^2(d)=1\\ d \text{ odd}}} 4^{\omega(d)}|R_n(d)| \ll D(\log D)^7 + \max_{j\in\{0,1\}} \sum_{\substack{d<D\\ \mu^2(d)=1\\ \gcd(d,6)=1}} 4^{\omega(d)}|\widetilde{R}_n(d,j)|,$$

as desired. □

6. Proof of Lemma 1.5

Let $0 < \xi < 1/2$ and $D = 2^{\xi n}$. Let $j \in \{0,1\}$ and $0 \leqslant \ell < 3^j$. By Lemma 5.2 and (5.1), it suffices to show that there exists $c > 0$, which depends only on ξ, such that

$$E(n, D, j, \ell) \ll_\xi \exp(-c\sqrt{n}),$$

where

$$E(n,D,j,\ell) = \sum_{\substack{d\leqslant D\\ \mu^2(d)=1\\ \gcd(d,6)=1}} \frac{4^{\omega(d)}}{d^2} \sum_{0<h_1,h_2<d} |H(d,h_1,h_2)| \left| F_n\left(\frac{h_2}{d}, -\left(\frac{h_1}{d}+\frac{\ell}{3^j}\right)\right)\right|.$$

In order to handle the common factors of d, h_1 and h_2, we write $d = d_0d_1d_2d_3$ with suitable d_i. More precisely, we show that the set of summation $\mathcal{E}(D)$ of all $(d, h_1, h_2) \in \mathbb{N}^3$ satisfying

$$1 \leqslant d \leqslant D,\ \mu^2(d) = 1,\ \gcd(d, 6) = 1,$$
$$0 < h_1 < d,\ 0 < h_2 < d$$

may be replaced by the set $\mathcal{F}(D)$ of all $(d_0, d_1, d_2, d_3, h_1^*, h_2^*) \in \mathbb{N}^6$ satisfying

$$1 \leqslant d_0d_1d_2d_3 \leqslant D,\ \mu^2(d_0d_1d_2d_3) = 1,\ \gcd(d_0d_1d_2d_3, 6) = 1,$$
$$0 < h_1^* < d_2d_3,\ 0 < h_2^* < d_1d_3,\ \gcd(h_1^*, d_2d_3) = 1,\ \gcd(h_2^*, d_1d_3) = 1.$$

We easily check that the map

$$\begin{array}{ccc} \mathcal{E}(D) & \to & \mathcal{F}(D) \\ (d, h_1, h_2) & \mapsto & (d_0, d_1, d_2, d_3, h_1^*, h_2^*) \end{array},$$

where $d_0, d_1, d_2, d_3, h_1^*, h_2^*$ are defined by

$$d_0 = \gcd(d, h_1, h_2),\ d_0d_1 = \gcd(d, h_1),\ d_0d_2 = \gcd(d, h_2),$$
$$d_0d_1d_2d_3 = d,\ h_1^*d_0d_1 = h_1,\ h_2^*d_0d_2 = h_2,$$

is well defined and bijective with inverse

$$\begin{array}{ccc} \mathcal{F}(D) & \to & \mathcal{E}(D) \\ (d_0, d_1, d_2, d_3, h_1^*, h_2^*) & \mapsto & (d_0d_1d_2d_3, h_1^*d_0d_1, h_2^*d_0d_2). \end{array}$$

It follows that

$$E(n, D, j, \ell) = \sum_{(d_0,d_1,d_2,d_3,h_1^*,h_2^*)\in\mathcal{F}(D)} \frac{4^{\omega(d_0d_1d_2d_3)}}{(d_0d_1d_2d_3)^2} \times |H(d_0d_1d_2d_3, h_1^*d_0d_1, h_2^*d_0d_2)| \times \left|F_n\left(\frac{h_2^*}{d_1d_3}, -\left(\frac{h_1^*}{d_2d_3} + \frac{\ell}{3^j}\right)\right)\right|.$$

Moreover, Lemma 3.1 implies that for $(d_0, d_1, d_2, d_3, h_1^*, h_2^*) \in \mathcal{F}(D)$,

$$|H\left(d_0d_1d_2d_3, h_1^*d_0d_1, h_2^*d_0d_2\right)| \leqslant 2^{\omega(d_0)}d_0d_1d_2.$$

Hence

$$E(n, D, j, \ell) \leqslant E_1(n, D, j, \ell),$$

where

$$E_1(n, D, j, \ell) = \sum_{(d_0,d_1,d_2,d_3,h_1^*,h_2^*)\in\mathcal{F}(D)} \frac{8^{\omega(d_0)}4^{\omega(d_1d_2d_3)}}{d_0d_1d_2d_3^2} \left|F_n\left(\frac{h_2^*}{d_1d_3}, -\left(\frac{h_1^*}{d_2d_3} + \frac{\ell}{3^j}\right)\right)\right|.$$

We now write $E_1(n,D,j,\ell) = E_2(n,D,j,\ell)+E_3(n,D,j,\ell)$, where in the sum $E_2(n,D,j,\ell)$ we have $d_1d_2d_3 \leqslant W$ and in the sum $E_3(n,D,j,\ell)$, we have $d_1d_2d_3 > W$, where W is a parameter to be precised such that

$$2 \leqslant W \leqslant D.$$

For $(d_0,d_1,d_2,d_3,h_1^*,h_2^*) \in \mathcal{F}(D)$ with $d_1d_2d_3 \leqslant W$, by Lemma 2.8, we have

$$\left|F_n\left(\frac{h_2^*}{d_1d_3}, -\left(\frac{h_1^*}{d_2d_3}+\frac{\ell}{3^j}\right)\right)\right| \ll \exp\left(\frac{-c_0\,n}{\log\left(\frac{4W}{3}\right)}\right).$$

It follows that

$$E_2(n,D,j,\ell) \ll \exp\left(\frac{-c_0\,n}{\log\left(\frac{4W}{3}\right)}\right) \sum_{\substack{1\leqslant d_0d_1d_2d_3\leqslant D\\ d_1d_2d_3\leqslant W\\ \mu^2(d_0d_1d_2d_3)=1}} \frac{8^{\omega(d_0)}4^{\omega(d_1d_2d_3)}}{d_0},$$

where, by Lemma 4.1, the sum in the right-hand side is at most

$$\begin{aligned}
&\sum_{\substack{d_1\leqslant W\\ \mu^2(d_1)=1}} 4^{\omega(d_1)} \sum_{\substack{d_2\leqslant W/d_1\\ \mu^2(d_2)=1}} 4^{\omega(d_2)} \sum_{\substack{d_3\leqslant W/(d_1d_2)\\ \mu^2(d_3)=1}} 4^{\omega(d_3)} \sum_{\substack{d_0\leqslant D\\ \mu^2(d_0)=1}} \frac{8^{\omega(d_0)}}{d_0}\\
&\qquad \ll W(\log W)^3(\log D)^8 \sum_{\substack{d_1\leqslant W\\ \mu^2(d_1)=1}} \frac{4^{\omega(d_1)}}{d_1} \sum_{\substack{d_2\leqslant W\\ \mu^2(d_2)=1}} \frac{4^{\omega(d_2)}}{d_2}\\
&\qquad \ll W(\log W)^{11}(\log D)^8 \ll W(\log D)^{19}.
\end{aligned}$$

Therefore,

$$E_2(n,D,j,\ell) \ll W(\log D)^{19} \exp\left(\frac{-c_0\,n}{\log\left(\frac{4W}{3}\right)}\right).$$

In order to bound $E_3(n,D,j,\ell)$, we first proceed to some dyadic splitting in d_1,d_2,d_3 so that $d_i \in [D_i,2D_i)$ for $i=1,2,3$ with

$$W/8 < D_1D_2D_3 \leqslant D$$

and we relax the conditions $\mu^2(d_0d_1d_2d_3)=1$ and $\gcd(d_0d_1d_2d_3,6)=1$ to keep only $\mu^2(d_0)=1$ and $\gcd(d_1d_2d_3,6)=1$:

$$\begin{aligned}E_3(n,D,j,\ell)&\\ &\ll (\log D)^3 \sum_{\substack{d_0\leqslant D\\ \mu^2(d_0)=1}} \frac{8^{\omega(d_0)}}{d_0} \max_{\substack{(D_1,D_2,D_3)\in\mathbb{N}^3\\ W/8<D_1D_2D_3\leqslant D}} \sum_{\substack{d_1,d_2,d_3\\ d_i\sim D_i,\, i=1,2,3\\ \gcd(d_1d_2d_3,6)=1}} \frac{4^{\omega(d_1d_2d_3)}}{d_1d_2d_3^2}\\ &\qquad\times \sum_{\substack{0<h_1^*<d_2d_3\\ \gcd(h_1^*,d_2d_3)=1}} \sum_{\substack{0<h_2^*<d_1d_3\\ \gcd(h_2^*,d_1d_3)=1}} \left|F_n\left(\frac{h_2^*}{d_1d_3},-\left(\frac{h_1^*}{d_2d_3}+\frac{\ell}{3^j}\right)\right)\right|.\end{aligned}$$

It follows from (4.1) and (2.4) that

$$\begin{aligned}E_3(n,D,j,\ell)&\\ &\ll (\log D)^{11} \max_{\substack{\mathcal{D}=(D_1,D_2,D_3)\in\mathbb{N}^3\\ W/8<D_1D_2D_3\leqslant D}} \widetilde{\tau}(8D_1D_2D_3)^2\, \frac{M_1(n;\mathcal{D},(0,3^{1-j}\ell))}{D_1D_2D_3^2},\end{aligned}$$

where $M_1(n;\mathcal{D},(0,3^{1-j}\ell))$ is defined by (2.3). If $D_1D_2D_3\leqslant D$ then, since $D=2^{\xi n}$, the condition (2.7) is satisfied for $n\geqslant n_0(\xi)$ with the choice

$$\varepsilon=\varepsilon(\xi)=\frac{1}{2}\min\left\{2,\frac{1}{2\xi}-1\right\}\in(0,1].$$

Thus by Lemma 2.12,

$$\frac{M_1(n;\mathcal{D},(0,3^{1-j}\ell))}{D_1D_2D_3^2}\ll \widetilde{\tau}(4D_1D_3)^{1/2}\,\widetilde{\tau}(4D_2D_3)^{1/2}\,(D_1D_2D_3)^{-\varepsilon\eta_0}.$$

Since $\widetilde{\tau}(d)\ll_\xi d^{\varepsilon\eta_0/6}$ for any positive integer d (see for instance [17, Theorem 315]) and recalling that $D_1D_2D_3>W/8$, we obtain

$$E_3(n,D,j,\ell)\ll_\xi (\log D)^{11}W^{-\varepsilon\eta_0/2}.$$

Combining the previous estimates, we get

$$E(n,D,j,\ell)\ll_\xi W(\log D)^{19}\exp\left(\frac{-c_0\,n}{\log\left(\frac{4W}{3}\right)}\right)+(\log D)^{11}W^{-\varepsilon\eta_0/2}.$$

By choosing

$$W=\exp\left(\delta n^{1/2}\right)\qquad\text{with}\qquad\delta=\delta(\xi)=c_0^{1/2}\left(\frac{\varepsilon(\xi)\eta_0}{2}+1\right)^{-1/2}>0,$$

we obtain

$$E(n,D,j,\ell) \ll_\xi n^{19}\exp\left(-\left(\frac{c_0}{\delta}-\delta\right)n^{1/2}\right)+n^{11}\exp\left(-\frac{\delta\varepsilon\eta_0}{2}n^{1/2}\right)$$
$$=\left(n^{19}+n^{11}\right)\exp\left(-\widetilde{\delta}\,n^{1/2}\right),$$

where $\widetilde{\delta}=\delta\varepsilon\eta_0/2>0$ depends only on ξ. It follows that

$$E(n,D,j,\ell) \ll_\xi \exp\left(-\frac{\widetilde{\delta}}{2}n^{1/2}\right),$$

which completes the proof of Lemma 1.5.

7. Proofs of main results

7.1. **Proof of Theorem 1.1.** We recall the notations introduced in Section 1.3.

Let $0<\gamma<1/(2\beta_2)$. We define $\xi=\frac{1}{2}(\beta_2\gamma+\frac{1}{2})$ so that $\beta_2\gamma<\xi<1/2$ and let $z=2^{\gamma n}$ and $y=2^{\xi n}\geqslant z$.

By Lemma 1.5, there exists $c>0$, which depends only on γ, such that

$$\sum_{\substack{d\mid P(z)\\ d<y}} 4^{\omega(d)}|R_n(d)| \leqslant \sum_{\substack{d<y\\ d \text{ odd}}} \mu^2(d)4^{\omega(d)}|R_n(d)| \ll_\gamma 2^n\exp(-c\sqrt{n}).$$

Since $h^+\left(\frac{\log y}{\log z}\right)=h^+\left(\frac{\xi}{\gamma}\right)>0$, it follows from (1.9) that

$$\Theta\left(n,z\right) \ll_\gamma \frac{2^n}{n^2}.$$

Moreover, since $\beta_2\gamma<\xi$, we have $h^-\left(\frac{\log y}{\log z}\right)=h^-\left(\frac{\xi}{\gamma}\right)>0$ and it follows from (1.10) that there exists $n_0=n_0(\gamma)$ such that for $n\geqslant n_0$, we have

$$\Theta\left(n,z\right) \gg_\gamma \frac{2^n}{n^2}.$$

This completes the proof of Theorem 1.1.

7.2. **Proof of Theorem 1.4.** We first detect the condition that $\overleftarrow{a}$ is squarefree:

$$Q(n)=\sum_{a\in\mathcal{B}_n}\mu^2(a)\sum_{d_1^2\mid\overleftarrow{a}}\mu(d_1).$$

Let $D_1\leqslant 2^{n/2}$ be a parameter to be precised. We split the sum in $Q(n)=S_{11}+S_{12}$, where $d_1\leqslant D_1$ in S_{11} and $d_1>D_1$ in S_{12}. For the

sum S_{12}, we forget the condition "a is squarefree", and reverse the roles between a and $\overleftarrow{a}$:

$$|S_{12}| = \left| \sum_{D_1 < d_1 < 2^{n/2}} \mu(d_1) \sum_{\substack{a \in \mathcal{B}_n \\ d_1^2 | \overleftarrow{a}}} \mu^2(a) \right| \leqslant \sum_{D_1 < d_1 < 2^{n/2}} \sum_{\substack{a \in \mathcal{B}_n \\ d_1^2 | a}} 1 \ll \sum_{d_1 > D_1} \frac{|\mathcal{B}_n|}{d_1^2} \ll \frac{|\mathcal{B}_n|}{D_1}.$$

We now detect in S_{11} the condition $\mu^2(a) = 1$:

$$S_{11} = \sum_{d_1 \leqslant D_1} \mu(d_1) \sum_{\substack{a \in \mathcal{B}_n \\ d_1^2 | \overleftarrow{a}}} \mu^2(a) = \sum_{d_1 \leqslant D_1} \mu(d_1) \sum_{\substack{a \in \mathcal{B}_n \\ d_1^2 | \overleftarrow{a}}} \sum_{d_2^2 | a} \mu(d_2).$$

We introduce a parameter D_2 such that $D_1 \leqslant D_2 \leqslant 2^{n/2}$ and split S_{11} in $S_{11} = S_{21} + S_{22}$, where $d_2 \leqslant D_2$ in S_{21} and $d_2 > D_2$ in S_{22}. We bound trivially S_{22}:

$$|S_{22}| \leqslant D_1 \sum_{d_2 > D_2} \sum_{\substack{a \in \mathcal{B}_n \\ d_2^2 | a}} 1 \ll |\mathcal{B}_n| \frac{D_1}{D_2}.$$

It remains to estimate

$$S_{21} = \sum_{\substack{d_1 \leqslant D_1 \\ d_2 \leqslant D_2 \\ \gcd(d_1 d_2, 2) = 1}} \mu(d_1)\mu(d_2) \sum_{\substack{a \in \mathcal{B}_n \\ d_1^2 | \overleftarrow{a} \\ d_2^2 | a}} 1.$$

Since the inner sum above is for $a \in \mathcal{B}_n$, it is licit to add the condition $\gcd(d_1 d_2, 2) = 1$. We detect the conditions $d_1^2 \mid \overleftarrow{a}$ and $d_2^2 \mid a$ via exponential sums. The sum S_{21} becomes:

$$\begin{aligned} S_{21} &= \sum_{\substack{d_1 \leqslant D_1 \\ d_2 \leqslant D_2 \\ \gcd(d_1 d_2, 2) = 1}} \frac{\mu(d_1)\mu(d_2)}{d_1^2 d_2^2} \sum_{a \in \mathcal{B}_n} \sum_{0 \leqslant h_1 < d_1^2} \sum_{0 \leqslant h_2 < d_2^2} \mathrm{e}\left(\frac{h_1 \overleftarrow{a}}{d_1^2} + \frac{h_2 a}{d_2^2} \right) \\ &= |\mathcal{B}_n| \sum_{\substack{d_1 \leqslant D_1 \\ d_2 \leqslant D_2 \\ \gcd(d_1 d_2, 2) = 1}} \frac{\mu(d_1)\mu(d_2)}{d_1^2 d_2^2} \sum_{0 \leqslant h_1 < d_1^2} \sum_{0 \leqslant h_2 < d_2^2} F_n\left(\frac{h_1}{d_1^2}, \frac{-h_2}{d_2^2} \right). \end{aligned}$$

We now split this sum in $S_{21} = S_{31} + S_{32}$, where, in S_{31} we have $d_1^2 \nmid 3h_1$ or $d_2^2 \nmid 3h_2$ and in S_{32}, $d_1^2 \mid 3h_1$ and $d_2^2 \mid 3h_2$. By Lemma 2.8, we have

$$|S_{31}| \leqslant |\mathcal{B}_n| D_1 D_2 \max_{\substack{(d_1,d_2,h_1,h_2)\\ d_i \leqslant D_i, 0 \leqslant h_i < d_i^2, i=1,2\\ \gcd(d_1 d_2, 2)=1\\ d_1^2 \nmid 3h_1 \text{ or } d_2^2 \nmid 3h_2}} \left| F_n\left(\frac{h_1}{d_1^2}, \frac{-h_2}{d_2^2}\right)\right|$$
$$\ll |\mathcal{B}_n| D_1 D_2 \exp\left(\frac{-c_0 n}{\log(\frac{4D_2^2}{3})}\right).$$

It remains to estimate S_{32}. We split the sum according to the value of $\left(\frac{3h_1}{d_1^2}, \frac{3h_2}{d_2^2}\right) \in \{0,1,2\}^2$:

$$S_{32} = |\mathcal{B}_n| \sum_{0 \leqslant u_1, u_2 \leqslant 2} F_n\left(\frac{u_1}{3}, \frac{-u_2}{3}\right) \prod_{i=1}^{2} \left(\sum_{\substack{d_i \leqslant D_i\\ \gcd(d_i,2)=1,\ 3 \mid u_i d_i^2}} \frac{\mu(d_i)}{d_i^2} \right).$$

For $i \in \{1,2\}$ and $u_i \in \{0,1,2\}$, we easily check that

$$\sum_{\substack{d_i \leqslant D_i\\ \gcd(d_i,2)=1,\ 3 \mid u_i d_i^2}} \frac{\mu(d_i)}{d_i^2} = \frac{c(u_i)}{\zeta(2)} + O\left(\frac{1}{D_i}\right),$$

where $c(u_i)$ is defined by $c(0) = 4/3$ and $c(1) = c(2) = -1/6$. It follows that

$$S_{32} = |\mathcal{B}_n| \sum_{0 \leqslant u_1, u_2 \leqslant 2} F_n\left(\frac{u_1}{3}, \frac{-u_2}{3}\right) \left(\frac{c(u_1)c(u_2)}{\zeta(2)^2} + O\left(\frac{1}{D_1}\right)\right)$$
$$= \frac{S_{41}}{\zeta(2)^2} + O\left(\frac{|\mathcal{B}_n|}{D_1}\right),$$

where S_{41} is defined by

$$S_{41} = |\mathcal{B}_n| \sum_{0 \leqslant u_1, u_2 \leqslant 2} F_n\left(\frac{u_1}{3}, \frac{-u_2}{3}\right) c(u_1)c(u_2).$$

To estimate the sum over (u_1, u_2), we use again exponential sums:

$$S_{41} = \sum_{0 \leqslant u_1, u_2 \leqslant 2} c(u_1)c(u_2) \sum_{a \in \mathcal{B}_n} \mathrm{e}\left(\frac{u_1 \overleftarrow{a}}{3} + \frac{u_2 a}{3}\right)$$
$$= \sum_{a \in \mathcal{B}_n} \left(\sum_{0 \leqslant u_1 \leqslant 2} c(u_1)\, \mathrm{e}\left(\frac{u_1 \overleftarrow{a}}{3}\right)\right) \left(\sum_{0 \leqslant u_2 \leqslant 2} c(u_2)\, \mathrm{e}\left(\frac{u_2 a}{3}\right)\right).$$

For the inner sum over u_1, we write

$$\begin{aligned}\sum_{0\leqslant u_1\leqslant 2} c(u_1)\,\mathrm{e}\left(\frac{u_1\overleftarrow{a}}{3}\right) &= c(0)+c(1)\left(\mathrm{e}\left(\frac{\overleftarrow{a}}{3}\right)+\mathrm{e}\left(\frac{2\overleftarrow{a}}{3}\right)\right)\\ &= c(0)+c(1)\left(3\cdot\mathbf{1}_{3|\overleftarrow{a}}-1\right)\\ &= \frac{1}{2}\left(3-\mathbf{1}_{3|\overleftarrow{a}}\right)\end{aligned}$$

and similarly for the sum over u_2. Since

$$\overleftarrow{a}\equiv(-1)^{n-1}a \bmod 3,$$

it follows that

$$S_{41}=\frac{1}{4}\sum_{a\in\mathcal{B}_n}\left(3-\mathbf{1}_{3|a}\right)^2=\frac{1}{4}\left(9|\mathcal{B}_n|-5\sum_{\substack{a\in\mathcal{B}_n\\3|a}}1\right)=\frac{11}{6}\,|\mathcal{B}_n|+O(1).$$

Combining the previous estimates, we finally obtain

$$Q(n)=|\mathcal{B}_n|\left(\frac{11}{6\zeta(2)^2}+O\left(\frac{D_1}{D_2}+\frac{1}{D_1}+D_1D_2\exp\left(\frac{-c_0n}{\log(\frac{4D_2^2}{3})}\right)\right)\right).$$

By choosing $D_2=D_1^2=\exp\left(\frac{1}{2}c_0^{1/2}n^{1/2}\right)$, we get

$$Q(n)=|\mathcal{B}_n|\left(\frac{11}{6\zeta(2)^2}+O\left(\exp\left(-cn^{1/2}\right)\right)\right)$$

with $c=\frac{1}{4}c_0^{1/2}=0.0439\ldots$, which proves (1.4).

If b is an $(n-1)$-bit integer then $2b$ is an n-bit integer and $\overleftarrow{2b}=\overleftarrow{b}$. It follows that the number of even integers a such that $2^{n-1}\leqslant a<2^n$ and $\mu^2(a)=\mu^2(\overleftarrow{a})=1$ is

$$\left|\{2^{n-2}\leqslant b<2^{n-1}:\ \mu^2(2b)=\mu^2(\overleftarrow{b})=1\}\right|=Q(n-1).$$

Since $|\mathcal{B}_n|=2^{n-2}$, this implies that

$$\widetilde{Q}(n)=Q(n)+Q(n-1)=2^{n-1}\left(\frac{11}{8\zeta(2)^2}+O(\exp(-cn^{1/2}))\right),$$

which proves (1.5).

8. Numerical investigations on the number of reversible primes

8.1. **Preambule.** In this section, we provide numerical investigations on reversible primes. In fact, we do not restrict ourselves to base 2 and provide also some numerical data in base 10.

8.2. **Base 2.** We recall that [27, A074831] provides a table of the number of binary reversible primes less than 10^m for $m \leqslant 12$. We think more useful to provide a table of the number $\Theta(n)$ of binary reversible primes with exactly n binary digits and we do so for $n \leqslant 50$ in Table 1, see also [27, A366910].

We have written a program that combines a classical Eratosthenes sieve (optimized using the library `primesieve`) with a variant of Eratosthenes sieve in residue classes. This permits to organize the computations by blocks so that the tables fit into the computer memory and produce a considerable speedup due to a strong use of the `L1` memory cache.

n	$\Theta(n)$	n	$\Theta(n)$	n	$\Theta(n)$	n	$\Theta(n)$	n	$\Theta(n)$
1	0	11	69	21	16732	31	7377931	41	4222570054
2	1	12	94	22	29392	32	13878622	42	8056984176
3	2	13	178	23	55109	33	25958590	43	15315267089
4	2	14	308	24	101120	34	48421044	44	29274821854
5	4	15	589	25	179654	35	92163237	45	55976669028
6	6	16	908	26	332130	36	173672988	46	106505783902
7	9	17	1540	27	625928	37	325098134	47	204628057694
8	14	18	2814	28	1136814	38	617741968	48	392422557460
9	27	19	5158	29	2120399	39	1177573074	49	749026893680
10	36	20	9210	30	3963166	40	2221353224	50	1440435348050

Table 1. Base 2: values of $\Theta(n)$ for $n \leqslant 50$.

A table of the number of binary prime palindromes with n binary digits is given in [27, A117773]. Our calculations give us the opportunity to confirm these values for all $n \leqslant 50$.

Let us describe a heuristic argument that leads us to a conjecture on the asymptotic behaviour of $\Theta(n)$.

Let a be a randomly chosen integer in $\mathcal{B}_n$. If a is prime then $3 \nmid a$, which is equivalent to $3 \nmid \overleftarrow{a}$ by (1.1). Therefore the events "a is prime" and "$\overleftarrow{a}$ is prime" are not expected to be "independent" but it is natural to expect that they are "conditionally independent" given

that $3 \nmid a$. This would imply that

$$\begin{aligned}\mathbb{P}\left(a \text{ and } \overleftarrow{a} \text{ are prime}\right) &= \mathbb{P}\left(a \text{ and } \overleftarrow{a} \text{ are prime} \,|\, 3 \nmid a\right) \mathbb{P}\left(3 \nmid a\right) \\ &\approx \mathbb{P}\left(a \text{ is prime} \,|\, 3 \nmid a\right) \mathbb{P}\left(\overleftarrow{a} \text{ is prime} \,|\, 3 \nmid a\right) \mathbb{P}\left(3 \nmid a\right) \\ &= \frac{\mathbb{P}(a \text{ is prime})\, \mathbb{P}(\overleftarrow{a} \text{ is prime})}{\mathbb{P}\left(3 \nmid a\right)}.\end{aligned}$$

Moreover $\mathbb{P}(a \text{ is prime}) = \mathbb{P}(\overleftarrow{a} \text{ is prime})$ and since $a \in \mathcal{B}_n$, by the Prime Number Theorem, we have

$$\mathbb{P}(a \text{ is prime}) = \frac{\mathrm{Li}(2^n) - \mathrm{Li}(2^{n-1})}{|\mathcal{B}_n|}(1 + o(1)) \qquad (n \to \infty),$$

where

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Thus we may expect that

$$\Theta(n) = |\mathcal{B}_n|\, \mathbb{P}\left(a \text{ and } \overleftarrow{a} \text{ are prime}\right) \approx \Theta_{\exp}(n),$$

where

$$\Theta_{\exp}(n) = \frac{3\left(\mathrm{Li}(2^n) - \mathrm{Li}(2^{n-1})\right)^2}{2^{n-1}} = (3 + o(1))\frac{2^{n-1}}{(\log 2^n)^2} \qquad (n \to \infty).$$

This agrees with the values of $\Theta(n)$ provided in Table 1, as illustrated graphically by Figure 1.

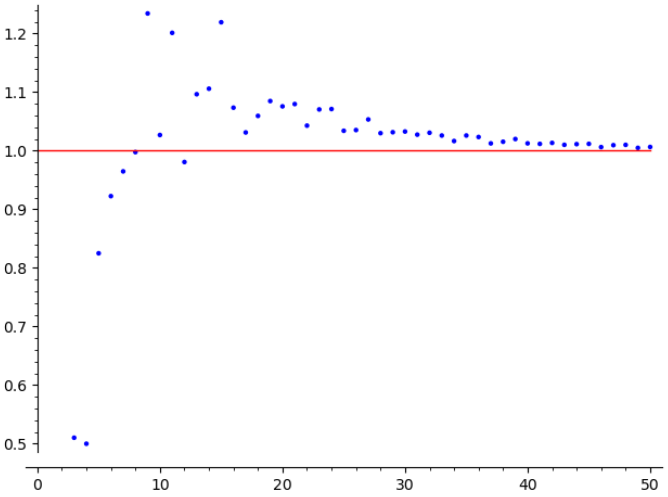

FIGURE 1. Base 2: graph of $\Theta(n)/\Theta_{\exp}(n)$ for $n \leqslant 50$.

This leads us to formulate the following.

Conjecture 8.1.

$$\Theta(n) = (3 + o(1))\frac{2^{n-1}}{(\log 2^n)^2} \qquad (n \to \infty).$$

8.3. **Base 10.** In this section, we consider n-digits integers k in base 10 such that

$$k = \sum_{j=0}^{n-1} \varepsilon_j(k)\, 10^j, \quad \overleftarrow{k} = \sum_{j=0}^{n-1} \varepsilon_j(k)\, 10^{n-1-j},$$

where $\varepsilon_j(k) \in \{0, 1, \dots, 10\}$, $j \in \{0, \dots, n-1\}$, $\varepsilon_{n-1}(k) \neq 0$. We define

$$\Theta_{10}(n) = \left|\left\{10^{n-1} \leqslant p < 10^n : \ p \text{ and } \overleftarrow{p} \text{ are prime}\right\}\right|.$$

We note that [27, A048054] provides a table of the number $\Theta_{10}(n)$ of base 10 reversible primes with exactly n digits in base 10 for $n \leqslant 13$. We extend this to $n \leqslant 15$ in Table 2.

n	$\Theta_{10}(n)$	n	$\Theta_{10}(n)$	n	$\Theta_{10}(n)$
1	4	6	9538	11	274932272
2	9	7	71142	12	2294771254
3	43	8	535578	13	19489886063
4	204	9	4197196	14	167630912672
5	1499	10	33619380	15	1456476399463

TABLE 2. Base 10: values of $\Theta_{10}(n)$ for $n \leqslant 15$.

Furthermore, [27, A016115] provides a table of the number of base 10 prime palindromes with n digits. Our calculations give us the opportunity to confirm these values for all $n \leqslant 15$.

ACKNOWLEDGEMENT

This work was motivated by conversations with Pieter Moree, who we would like to thank. The authors also express their gratitude to their late colleague and friend Christian Mauduit with who several possible approaches to this project were discussed in 2014 in Luminy.

During the preparation of this work C.D., B.M. and J.R. were supported by ANR-FWF Grant 4945-N and ANR Grant 20-CE91-0006 and I.S. by the ARC Grants DP230100530 and DP230100534.

Declarations of interest: none.

References

[1] W. D. Banks, D. Hart and M. Sakata, *Almost all palindromes are composite*, Mathematical Research Letters, 11 (2004), 853–868. 4

[2] W. D. Banks, F. Saidak and M. Sakata, *Kloosterman sums for modified van der Corput sequences*, Unif. Distrib. Theory 2 (2007), 39–52. 10

[3] W. D. Banks and I.E. Shparlinski, *Prime divisors of palindromes*, Period. Math. Hungar., 51 (2005), 1–10. 4

[4] J. Bourgain, *Prescribing the binary digits of primes*, Israel J. Math., 194 (2013), 935–955. 3

[5] J. Bourgain, *Prescribing the binary digits of primes, II*, Israel J. Math., 206 (2015), 165–182. 3

[6] Y. Bugeaud, *On the digital representation of integers with bounded prime factors*, Osaka J. Math., 55 (2018), 315–324. 3

[7] Y. Bugeaud and H. Kaneko, *On the digital representation of smooth numbers*, Math. Proc. Cambridge Philos. Soc., 165 (2018), 533–540. 3

[8] S. Col, *Diviseurs des nombres ellipséphiques*, Period. Math. Hungarica, 58 (2009), 1–23. 3

[9] S. Col, *Palindromes dans les progressions arithmétiques*, Acta Arith., 137 (2009), 1–41. 3, 4, 13

[10] C. Dartyge and C. Mauduit, *Nombres presque premiers dont l'écriture en base r ne comporte pas certains chiffres*, J. Number Theory, 81 (2000), 270–291. 3

[11] C. Dartyge and C. Mauduit, *Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers*, J. Number Theory, 91 (2001), 230–255. 3

[12] C. Dartyge and G. Tenenbaum *Congruences de sommes de chiffres de valeurs polynomiales*, Bull. London Math. Soc. 38 (2006), 61-69. 3

[13] R. Dietmann, C. Elsholtz and I. E. Shparlinski, *Prescribing the binary digits of squarefree numbers and quadratic residues*, Trans. Amer. Math. Soc., 369 (2017), 8369–8388. 3

[14] H. Diamond, H. Halberstam and H.-E. Richert, *Combinatorial sieves of dimension exceeding one*, J. Number Theory, 28 (1988), 306–346. 5, 9

[15] M. Drmota, C. Mauduit and J. Rivat, *The sum of digits function of polynomial sequences*, J. London Math. Soc., 84, (2011), 81–102. 3

[16] M. Drmota, C. Mauduit and J. Rivat, *Prime numbers in two bases*, Duke Math. J., 69 (2020), 1809–1876. 3

[17] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, fifth ed., 1979. 30

[18] A. J. Irving, *Diophantine Approximation with Products of Two Primes*, J. London Math. Soc., 89 (2014), 581–602. 4

[19] F. Karwatowski, *Primes with one excluded digit*, Acta Arith., 202 (2022), 105–121. 3

[20] C. Mauduit and J. Rivat, *La somme des chiffres des carrés*, Acta Math., 203 (2009), 107–148. 3

[21] C. Mauduit and J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math.,171 (2010), 1591–1646. 3

[22] J. Maynard, *Primes with restricted digits*, Invent. Math., 217 (2019), 127–218. 3

[23] J. Maynard, *Primes and polynomials with restricted digits*, Int. Math. Res. Not., 2022 (2022), 10626–10648. 3
[24] H. L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc., 84 (1978), 547–567. 10, 11, 19
[25] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Adv. Math. , Cambridge Univ. Press, Cambridge, 2007. 23
[26] E. Naslund, *The tail distribution of the sum of digits of prime numbers*, Unif. Distrib. Theor., 10 (2015), 63–68. 3
[27] OEIS, *On-line encyclopedia of integer sequences*, https://oeis.org. 3, 6, 35, 37
[28] K. Pratt, *Primes from sums of two squares and missing digits*, Proc. Lond. Math. Soc., 20 (2020), 770–830. 3
[29] L. Spiegelhofer, *Thue–Morse along the sequence of cubes*, Preprint, 2023, https://arxiv.org/abs/2308.09498. 3
[30] T. Stoll, *The sum of digits of polynomial values in arithmetic progressions*, Functiones et Approximatio 47 (2012), 233-239. 3
[31] C. Swaenepoel, *Prime numbers with a positive proportion of preassigned digits*, Proc. London Math. Soc., 121 (2020), 83–151. 3
[32] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Grad. Studies in Math., vol. 163, AMS, 2015. 8, 23
[33] E. C. Titchmarsh, *The Theory of Functions*, Oxford University Press, London, second ed., 1939. 10

Cécile Dartyge, Institut Élie Cartan, Université de Lorraine, BP 70239, 54506 Vandœuvre-lès-Nancy Cedex, France
Email address: cecile.dartyge@univ-lorraine.fr

Bruno Martin, Univ. Littoral Côte d'Opale, EA 2797 – LMPA – Laboratoire de Mathématiques pures et appliquées Joseph Liouville, F-62228 Calais, France.
Email address: Bruno.Martin@univ-littoral.fr

Joël Rivat, Université d'Aix-Marseille, Institut Universitaire de France, Institut de Mathématiques de Marseille CNRS UMR 7373, 163 avenue de Luminy, Case 907, 13288 Marseille Cedex 9, France.
Email address: joel.rivat@univ-amu.fr

Igor E. Shparlinski, School of Mathematics and Statistics, University of New South Wales, Sydney, NSW, 2052, Australia
Email address: igor.shparlinski@unsw.edu.au

Cathy Swaenepoel, Université Paris Cité and Sorbonne Université, CNRS, INRIA, IMJ-PRG, F-75013 Paris, France.
Email address: cathy.swaenepoel@u-paris.fr