Irrationality of Power Series for Various Number Theoretic Functions*

William D. Banks
Department of Mathematics, University of Missouri
Columbia, MO 65211, USA
bbanks@math.missouri.edu

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

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

October 8, 2005

Abstract

We study formal power series whose coefficients are taken to be a variety of number theoretic functions, such as the Euler, Möbius and divisor functions. We show that these power series are irrational over $\mathbb{Z}[X]$, and we obtain lower bounds on the precision of their rational approximations.

*Accepted by *Manuscripta Mathematica*, MM-No.: 744

1 Introduction

We consider formal power series whose coefficients are taken to be variety of common number theoretic functions, and we show that these series are irrational over $\mathbb{Z}[X]$. Moreover, we obtain a lower bound on the precision of their rational approximations. Our approach is based on certain properties of linear recurrence sequences over finite fields (in particular, the periodicity and distribution properties of such sequences), and on various well-known statements from analytic number theory.

The study of Diophantine properties of power series whose coefficients have number theoretic or combinatorial meaning is currently a very active area of research; see [1] and references therein. We believe that our underlying method, which requires some fine tuning to deal with each specific case, can be adapted to work with a very large class of functions.

To describe our results, we start with a list of number theoretic functions that are considered in the sequel; for an integer $n > 1$, let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be its prime factorization.

- The *Euler function*, which gives the cardinality of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, is defined by
$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1).$$
- The functions $\omega(n)$ and $\Omega(n)$ have their usual meanings: $\omega(n) = k$ is the number of distinct prime factors of n, and $\Omega(n) = \alpha_1 + \ldots + \alpha_k$ is the number of prime divisors of n, counted with multiplicity.
- The function $\tau(n)$ counts the number of positive divisors d of n; one has
$$\tau(n) = \prod_{j=1}^{k} (\alpha_j + 1).$$
- The function $\rho(n) = 2^{\omega(n)} = 2^k$ counts the number of *squarefree* positive divisors of n.
- The function $\sigma(n)$ gives the *sum* of the positive divisors d of n; we have
$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{\alpha_j + 1} - 1}{p_j - 1}.$$

- The *Liouville function* is given by $\lambda(n) = (-1)^{\omega(n)} = (-1)^k$, while $\mu(n)$ denotes the *Möbius function*; we recall that $\mu(n) = \lambda(n)$ if n is squarefree, and $\mu(n) = 0$ otherwise.

Following standard conventions, we also put

$$\omega(1) = \Omega(1) = 0 \qquad \text{and} \qquad \varphi(1) = \tau(1) = \rho(1) = \sigma(1) = \lambda(1) = \mu(1) = 1.$$

Finally:

- For every positive integer n, let $p(n)$ denote the n-th prime number; thus, $p(1) = 2$, $p(2) = 3$, $p(3) = 5$, $p(4) = 7$, $p(5) = 11$, etc.

Our goal in this paper is to study the irrationality of the corresponding formal power series:

$$\mathcal{F}(X) = \sum_{n=1}^{\infty} \varphi(n) X^n, \quad \mathcal{W}_1(X) = \sum_{n=1}^{\infty} \omega(n) X^n, \quad \mathcal{W}_2(X) = \sum_{n=1}^{\infty} \Omega(n) X^n,$$

$$\mathcal{T}(X) = \sum_{n=1}^{\infty} \tau(n) X^n, \qquad \mathcal{P}(X) = \sum_{n=1}^{\infty} p(n) X^n, \qquad \mathcal{R}(X) = \sum_{n=1}^{\infty} \rho(n) X^n,$$

$$\mathcal{S}(X) = \sum_{n=1}^{\infty} \sigma(n) X^n, \qquad \mathcal{L}(X) = \sum_{n=1}^{\infty} \lambda(n) X^n, \quad \mathcal{M}(X) = \sum_{n=1}^{\infty} \mu(n) X^n.$$

Let $\mathbb{Z}[[X]]$ denote the ring of formal power series over the integers, and let $\mathbb{Q}((X))$ denote the field of fractions of $\mathbb{Z}[[X]]$; then $\mathbb{Q}((X))$ is the field of formal Laurent series of the form:

$$\mathcal{U}(X) = \sum_{n \geq N}^{\infty} u(n) X^n, \tag{1}$$

where $u(n) \in \mathbb{Q}$ for all $n \geq N$ and $u(N) \neq 0$, together with the zero element $\mathcal{U} = 0$. For a Laurent series given by (1), we define the *X-adic order of $\mathcal{U}$* by $\operatorname{ord}(\mathcal{U}) = N$; we also put $\operatorname{ord}(0) = \infty$. We note that an element $\mathcal{U} \in \mathbb{Q}((X))$ lies in $\mathbb{Z}[[X]]$ if and only if $\operatorname{ord}(\mathcal{U}) \geq 0$ and $u(n) \in \mathbb{Z}$ for all $n \geq 0$.

For any positive integer d and any formal power series $\mathcal{U} \in \mathbb{Z}[[X]]$, we define

$$\Delta_d(\mathcal{U}) = \max_{\substack{f,g \in \mathbb{Z}[X] \\ \deg f, \deg g \leq d \\ g \neq 0}} \operatorname{ord}\left(\mathcal{U}(X) - \frac{f(X)}{g(X)}\right),$$

where $\mathbb{Z}[X]$ is the ring of polynomials over $\mathbb{Z}$. Clearly, $\Delta_d(\mathcal{U})$ is finite for every d if and only if $\mathcal{U}$ is *irrational*; in other words, $\mathcal{U} \neq f/g$ (when both sides are viewed as Laurent series) for all polynomials $f, g \in \mathbb{Z}[x]$ with $g \neq 0$.

Throughout the paper, all constants implied by the symbols 'O', '$\ll$' and '$\gg$' are absolute. We recall that the notations $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent.

Our main result is the following:

Theorem 1. *For a positive integer d, the following bounds hold:*

$$\Delta_d(\mathcal{F}) = \exp\left(O(d^{2/3}\log^{2/3} d)\right), \qquad \Delta_d(\mathcal{W}_i) = O\left(d \cdot 3^{1.965d}\right),\ i = 1, 2,$$

$$\Delta_d(\mathcal{T}) = O\left(d^2\right), \qquad \Delta_d(\mathcal{P}) = O\left(\frac{d^2 9^d}{\log^2 d}\right),$$

$$\Delta_d(\mathcal{R}) = O\left(d \cdot 3^{11d/4}\right), \qquad \Delta_d(\mathcal{S}) = \exp\left(O(d^{2/3}\log^{2/3} d)\right),$$

$$\Delta_d(\mathcal{L}) = O\left(d \cdot 3^{11d/4}\right), \qquad \Delta_d(\mathcal{M}) = O\left(d \cdot 3^{11d/4}\right).$$

2 A Guide to the Proofs

Although the details vary from case to case, utilizing very different number theoretic tools, proofs of all of the bounds of Theorem 1 have the following basic structure:

- We assume that the power series $\mathcal{U}(X)$ in question can be very well approximated by a ratio of two polynomials of degree at most d.
- We choose an appropriate "small" prime q (for example, $q = 2$ and $q = 3$ are our common choices) and reduce the power series $\mathcal{U}(X)$ modulo q. The resulting power series still has a very good rational approximation by a ratio of two polynomials of degree at most d. Thus, a long initial segment of coefficients of $\mathcal{U}(X)$ necessarily satisfies a linear recurrence relation modulo q of order at most d.
- Finally, we show that known results about the period length or the distribution of values of linear recurrence sequences contradict certain number theoretic properties of the coefficients of $\mathcal{U}(X)$, such as multiplicativity, additivity, divisibility, or distribution in arithmetic progressions.

For each of the series we consider, we use a specific (and rather unusual) combination of two kinds of tools: one coming from the theory of linear recurrence sequences, and another coming from analytic number theory.

3 Preparations

3.1 Power Series and Linear Recurrence Sequences

Given a nonzero polynomial $f \in \mathbb{Z}[X]$, we define its *content* $\mathrm{cont}(f)$ as the greatest common divisor of its coefficients. More generally, for a nonzero formal power series in $\mathbb{Z}[[X]]$,

$$f(X) = \sum_{j=0}^{\infty} f_j X^j,$$

we define $\mathrm{cont}_j(f) = \gcd(f_0, f_1, \ldots, f_j)$ for each $j \geq 0$. Since the sequence of positive integers $(\mathrm{cont}_j(f))_{j\geq 0}$ is nonincreasing, it follows that there exists j_0 such that $\mathrm{cont}_j(f) = \mathrm{cont}_{j_0}(f)$ for all $j \geq j_0$. We write $\mathrm{cont}(f)$ for $\mathrm{cont}_{j_0}(f)$. Note that the above definition coincides with the usual definition of the *content* when f happens to be a polynomial with integer coefficients.

We need the following technical result.

Lemma 2. *If $\mathcal{U}$ is a formal power series in $\mathbb{Z}[[X]]$, f and g are polynomials in $\mathbb{Z}[X]$ of degree at most $d \geq 0$, and*

$$\mathrm{ord}\left(\mathcal{U}(X) - \frac{f(X)}{g(X)}\right) > d,$$

then $\mathrm{cont}_j(g) \,|\, \mathrm{cont}_j(f)$ for $j = 0, 1, \ldots, d$. In particular, $\mathrm{cont}(f) \,|\, \mathrm{cont}(g)$.

Proof. We have

$$\mathcal{U}(X) - \frac{f(X)}{g(X)} = \sum_{n\geq d+1} v(n) X^n,$$

where $v(n) \in \mathbb{Q}$ for $n \geq d+1$; that is,

$$\mathcal{U}(X)\, g(X) = f(X) + g(X) \sum_{n\geq d+1} v(n) X^n.$$

Comparing the coefficients on either side of this identity for each $j = 0, \dots, d$ we see that $\mathrm{cont}_j(g)$ divides the j-th coefficient of f (since the coefficients of $\mathcal{U}$ all lie in $\mathbb{Z}$); then $\mathrm{cont}_j(g) \,|\, \mathrm{cont}_i(g) \,|\, f_i$ for all $i = 0, \dots, j$, and the result follows. $\square$

For an arbitrary integral domain $\mathcal{K}$ with field of fractions $\mathbb{F}$, the natural map $\psi_{\mathcal{K}} : \mathbb{Z} \to \mathcal{K}$, $n \mapsto n \cdot 1_{\mathcal{K}}$, extends to a ring homomorphism

$$\psi_{\mathcal{K}} : \mathbb{Z}[[X]] \to \mathcal{K}[[X]]$$

in the obvious way. If $\mathcal{U}$ is a formal Laurent series in $\mathbb{F}((X))$ given by (1) with $u(n) \in \mathbb{F}$ for all $n \geq N$ and $u(N) \neq 0$, we define the X-adic order of $\mathcal{U}$ in $\mathbb{F}((X))$ by $\mathrm{ord}_{\mathcal{K}}(\mathcal{U}) = N$; as before, we also put $\mathrm{ord}_{\mathcal{K}}(0) = \infty$.

For any positive integer d and any formal power series $\mathcal{U} \in \mathcal{K}[[X]]$, we define

$$\Delta_{d,\mathcal{K}}(\mathcal{U}) = \max_{\substack{f,g \in \mathcal{K}[X] \\ \deg f, \deg g \leq d \\ g \neq 0}} \mathrm{ord}_{\mathcal{K}} \left(\mathcal{U}(X) - \frac{f(X)}{g(X)} \right),$$

where $\mathcal{K}[X]$ is the ring of polynomials over $\mathcal{K}$.

Lemma 3. *Let p be a prime, and let $\mathcal{K} = \mathbb{F}_p$ be the finite field with p elements. For every formal power series $\mathcal{U} \in \mathbb{Z}[[X]]$ with $\Delta_d(\mathcal{U}) \geq D$, there exist polynomials $\widetilde{f}, \widetilde{g} \in \mathcal{K}[X]$ of degree at most d, such that the constant term of $\widetilde{g}$ is nonzero, and*

$$\mathrm{ord}_{\mathcal{K}} \left(\widetilde{\mathcal{U}}(X) - \frac{\widetilde{f}(X)}{\widetilde{g}(X)} \right) \geq D - d,$$

where $\widetilde{\mathcal{U}} = \psi_{\mathcal{K}}(\mathcal{U})$.

Proof. We may clearly assume that $D > d$, since the result is trivial otherwise. In this situation, $\psi_{\mathcal{K}} : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is the *reduction map* which sends each integer n to its congruence class n modulo p. Since $\Delta_d(\mathcal{U}) \geq D$, for some polynomials $f, g \in \mathbb{Z}[X]$ of degree at most d, with $g \neq 0$, we have

$$\mathrm{ord} \left(\mathcal{U}(X) - \frac{f(X)}{g(X)} \right) \geq D. \tag{2}$$

By Lemma 2, we have $\mathrm{cont}(g) \,|\, \mathrm{cont}(f)$; without loss of generality, we may therefore assume that $\mathrm{cont}(g) = 1$. Let j be the smallest such index for

which $p \nmid \mathrm{cont}_j(g)$; then clearly $j \leq d$. By the same lemma, we have $\mathrm{cont}_j(g) \,|\, \mathrm{cont}_j(f)$; hence, it follows that

$$f(X) = f_1(X)X^j + pf_2(X) \qquad \text{and} \qquad g(X) = g_1(X)X^j + pg_2(X)$$

hold for some uniquely defined polynomials $f_1, f_2, g_1, g_2 \in \mathbb{Z}[X]$ such that p does not divide the constant term of g_1. Applying the reduction map $\psi_{\mathcal{K}}$, it follows that $\widetilde{g} = \psi_{\mathcal{K}}(g_1)$ has a *nonzero* constant term. Since $\mathbb{F}_p$ is a field, this implies that $\widetilde{g}$ is an *invertible* element of the ring $\mathcal{K}[[X]]$. Now from (2), we see that

$$\mathcal{U}(X)\, g(X) - f(X) = \sum_{n \geq D} v(n) X^n,$$

where the coefficients $v(n)$ lie in $\mathbb{Z}$; applying the reduction map, we get the identity

$$\widetilde{\mathcal{U}}(X)\, \widetilde{g}(X) X^j - \widetilde{f}(X) X^j = \sum_{n \geq D} \widetilde{v}(n) X^n$$

in $\mathbb{F}_p[[X]]$, where $\widetilde{f} = \psi_{\mathcal{K}}(f_1)$, and $\widetilde{v}(n) = \psi_{\mathcal{K}}(v(n))$ for all $n \geq D$. By the above remarks, we have

$$\left(\widetilde{\mathcal{U}}(X) - \frac{\widetilde{f}(X)}{\widetilde{g}(X)} \right) X^j = \frac{1}{\widetilde{g}(X)} \sum_{n \geq D} \widetilde{v}(n) X^n,$$

and therefore,

$$\mathrm{ord}_{\mathcal{K}} \left(\widetilde{\mathcal{U}}(X) - \frac{\widetilde{f}(X)}{\widetilde{g}(X)} \right) \geq D - j \geq D - d.$$

This completes the proof. □

Lemma 4. *Let $\mathcal{U}$ be a formal power series in $\mathcal{K}[[X]]$,*

$$\mathcal{U}(X) = \sum_{n \geq 0} u(n) X^n,$$

where $\mathcal{K}$ is an integral domain. Given that

$$\mathrm{ord}_{\mathcal{K}} \left(\mathcal{U}(X) - \frac{f(X)}{g(X)} \right) \geq D$$

holds for some polynomials $f, g \in \mathcal{K}[x]$,

$$f(X) = \sum_{j=0}^{k} f_j X^j \qquad \textit{and} \qquad g(X) = \sum_{j=0}^{m} g_j X^j,$$

the identity

$$u(n+m)g_0 = -\sum_{j=0}^{m-1} u(n+j)g_{m-j}$$

holds in $\mathcal{K}$ *for* $\max\{k-m, 0\} < n < D-m$.

Proof. We regard f and g as elements of $\mathcal{K}[[X]]$,

$$f(X) = \sum_{j=0}^{\infty} f_j X^j \qquad \text{and} \qquad g(X) = \sum_{j=0}^{\infty} g_j X^j,$$

with $f_j = 0$ for all $j > k$ and $g_j = 0$ for all $j > m$. As in the proof of Lemma 2, we have

$$\mathcal{U}(X)\, g(X) = f(X) + g(X) \sum_{n \ge D} v(n) X^n,$$

where $v(n)$ lies in the field of fractions $\mathbb{F}$ of $\mathcal{K}$ for all $n \ge D$.

If $\max\{k, m\} < n < D$, then $f_n = 0$, and this is also equal to the n-th coefficient of $\mathcal{U}(X)\, g(X)$, namely,

$$\sum_{\substack{i,j \ge 0 \\ i+j=n}} u(i) g_j = \sum_{j=0}^{m} u(n-j) g_j = \sum_{j=0}^{m} u(n-m+j) g_{m-j}.$$

This completes the proof. □

We also recall the following well-known statement about the periodicity of linear recurrence sequences over finite fields; see Chapter 8 of [7].

Lemma 5. *Suppose that* $(U_n)_{n \ge 0}$ *is a sequence in the finite field with* q *elements* $\mathbb{F}_q$ *which satisfies the linear recurrence relation of order* k

$$U_{n+k} = \sum_{j=0}^{k-1} U_{n+j} G_j$$

for all $K \le n \le L-k$, *where* $G_0, \ldots, G_{k-1}$ *are fixed elements of* $\mathbb{F}_q$. *Then there exists an integer* $0 < t < q^k$ *such that* $U_n = U_{n+t}$ *holds for all integers* n *in the interval* $K \le n < n+t \le L$.

The following (and more general) bound on the number of zeros of a linear recurrence sequence over a finite field can be found in Section 7.1 of [3], in Chapter 8 of [7], and in Section 7.1 of [9].

Lemma 6. *Suppose that $(U_n)_{n\geq 0}$ is a nonzero sequence in the finite field $\mathbb{F}_q$ with q elements which satisfies a linear recurrence relation of order k*

$$U_{n+k} = \sum_{j=0}^{k-1} U_{n+j} G_j$$

for all $K \leq n \leq L-k$, where $G_0, \ldots, G_{k-1}$ are fixed elements of $\mathbb{F}_q$ (not all zero). Then

$$\#\{K \leq n < K+t \mid U_n = 0\} = \frac{t}{q} + O(q^{k/2} \log q).$$

We also need a lower bound for the number of nonzero values of a linear recurrence sequence over a finite field, which can be proved in similar way to the proof of Theorem 14.7 of [3]; see also Theorem 7.4 of [9].

Lemma 7. *Suppose that $(U_n)_{n\geq 0}$ is a nonzero sequence in the finite field with q elements $\mathbb{F}_q$ which satisfies a linear recurrence relation of order k:*

$$U_{n+k} = \sum_{j=0}^{k-1} U_{n+j} G_j$$

for all $K \leq n \leq L-k$, where $G_0, \ldots, G_{k-1}$ are fixed elements of $\mathbb{F}_q$ (not all zero). Let t be the smallest integer such that $U_n = U_{n+t}$ for every integer n such that $K \leq n \leq n+t \leq L$. Then for all positive integers $T \leq t$ and $r \leq k$, the following inequality holds:

$$\#\{K \leq n < K+T \mid U_n \neq 0\} \geq \frac{r(T-k)}{k} - \frac{1}{k} \sum_{w=1}^{r-1} \binom{k}{w} (q-1)^w (r-w).$$

Proof. Because t is the smallest period, the k-tuples $(U_n, \ldots, U_{n+k-1})$ are pairwise distinct for $K \leq n < K+T-k$. Let $N(w)$ denote the number of such k-tuples with precisely w nonzero entries. Since each element U_n with $K \leq n < K+T$ appears in at most k distinct k-tuples, we obtain

$$\#\{K \leq n < K+T \mid U_n \neq 0\} \geq \frac{1}{k} \sum_{w=1}^{k} N(w) w.$$

Trivially, we have

$$N(w) \le \binom{k}{w}(q-1)^w$$

and

$$\sum_{w=1}^{k} N(w) = T - k.$$

Therefore,

$$\begin{aligned}
\sum_{w=1}^{k} N(w)w &\ge \sum_{w=1}^{r-1} N(w)w + r\sum_{w=r}^{k} N(w) \\
&= \sum_{w=1}^{r-1} N(w)w + r\left(T - k - \sum_{w=1}^{r-1} N(w)\right) \\
&= r(T-k) - \sum_{w=1}^{r-1} N(w)(r-w) \\
&\ge r(T-k) - \sum_{w=1}^{r-1} \binom{k}{w}(q-1)^w(r-w),
\end{aligned}$$

which finishes the proof. □

3.2 Analytic Number Theory Background

Let us denote by $S(T)$ the number of positive integers $n \le T$ which are *squarefree* (that is, n is not divisible by the square of any prime number). We recall the following well-known statement.

Lemma 8. *The following asymptotic formula holds:*

$$S(T) = \frac{6}{\pi^2}\,T + O(T^{1/2}).$$

We next denote by $Q(T)$ the number of positive integers $n \le T$ which are *squarefull* (that is, $p^2 \mid n$ for every prime p dividing n). The following statement (see [10]) shows that the squarefull integers form a rather sparse set.

Lemma 9. *The following bound holds:*

$$Q(T) = \frac{\zeta(3/2)}{\zeta(2)}\, T^{1/2} + O(T^{1/3}),$$

where $\zeta(s)$ is the Riemann zeta function.

For positive integers a and t with $\gcd(t, a) = 1$, we denote by $p_r(t, a)$ the smallest integer $\ell \equiv a \pmod{t}$ with $\Omega(\ell) \leq r$. In particular, $p_1(t, a)$ is the smallest prime in the above arithmetic progression. Accordingly, we use the form of Linnik's theorem given by Heath-Brown [4].

Lemma 10. *For positive integers a and t with $\gcd(t, a) = 1$, the estimate*

$$p_1(t, a) = O(t^{11/2})$$

holds.

In some cases, using another result of Heath-Brown [5] leads to a stronger bound:

Lemma 11. *For positive integers a and t with $\gcd(t, a) = 1$, the estimate*

$$p_2(t, a) = O(t^{1.965})$$

holds.

As usual, we denote by $\pi(T, t, a)$ the number of primes $\ell \leq T$ with $\ell \equiv a \pmod{t}$. We also let $\pi(T)$ denote the total number of primes $\ell \leq T$.

The classical work of Littlewood [6] on the "prime number race in arithmetic progressions" contains the following result.

Lemma 12. *For any sufficiently large positive real number T the estimate*

$$\max_{x \leq T} |\pi(x, 3, 1) - \pi(x, 3, 2)| \gg \frac{\log\log\log T}{\log T} T^{1/2}$$

holds.

Let us denote by $N_\phi(T)$ ($N_\sigma(T)$) the number of positive integers $n \leq T$ such that $3 \nmid \varphi(n)$ ($3 \nmid \sigma(n)$, respectively).

Lemma 13. *There exists a constant $C > 0$ such that*

$$N_\phi(T) < CT \log^{-1/2} T$$

holds. A similar upper bound holds with ϕ replaced by σ.

Proof. It follows from a much more general statement about divisibility of the values of the Euler function, obtained in the proof of Theorem 4.1 of [2], that the number of positive integers $n \le T$ with $3 \nmid \varphi(n)$ is $O(T \log^{-1/2} T)$ (see also [8]). The same method also extends to integers with $3 \nmid \sigma(n)$ without any modifications. □

4 Proof of Theorem 1

4.1 The Series $\mathcal{W}_1(X)$ and $\mathcal{W}_2(X)$

Suppose that

$$\operatorname{ord}\left(\mathcal{W}_1(X) - \frac{f(X)}{g(X)}\right) = D$$

holds for some polynomials $f, g \in \mathbb{Z}[X]$ of degree at most d. Reducing this relation modulo 3 and applying Lemma 3, we deduce that

$$\operatorname{ord}_{\mathbb{F}_3}\left(\widetilde{\mathcal{W}}_1(X) - \frac{\widetilde{f}(X)}{\widetilde{g}(X)}\right) \ge D - d$$

holds for some polynomials $\widetilde{f}, \widetilde{g} \in \mathbb{F}_3[X]$ of degree at most d, where the constant term of $\widetilde{g}$ equals 1.

By Lemmas 4 and 5, it follows that there exists a positive integer $t < 3^d$ such that $\omega(n) \equiv \omega(n+t) \pmod 3$ for $d+1 \le n < n+t \le D-d-1$.

Let $\ell = p_2(t,1)$ be the smallest product of two primes such that $\ell \equiv 1 \pmod t$. Let m be one of the numbers $2d, 2d+1, 2d+2, 2d+3$ which is relatively prime to ℓ. Assuming that the inequality $D \ge (2d+3)(\ell+1)$ holds, and taking into account that $m \equiv m\ell \pmod t$ and $d+1 \le m < m\ell \le D-d-1$, we obtain that

$$\omega(m) \equiv \omega(m\ell) \pmod 3.$$

However, this is impossible as $1 \le \omega(m\ell) - \omega(m) \le 2$ (since $\gcd(m,\ell) = 1$). This contradiction shows that, in fact, $D < (2d+3)(\ell+1)$. Using Lemma 11,

we derive the bound $D = O\left(d \cdot 3^{1.965d}\right)$, which finishes the proof of our stated bound for $\Delta_d(\mathcal{W}_1)$.

The bound on $\Delta_d(\mathcal{W}_2)$ is obtained in the exactly the same way, except that m can simply be taken as $m = 2d$.

4.2 The Series $\mathcal{L}(X)$, $\mathcal{M}(X)$ and $\mathcal{R}(X)$

As before, we assume that

$$\operatorname{ord}\left(\mathcal{L}(X) - \frac{f(X)}{g(X)}\right) = D$$

holds for some polynomials $f, g \in \mathbb{Z}[X]$ of degree at most d. Reducing this relation modulo 3 and applying Lemma 3, we deduce that

$$\operatorname{ord}_{\mathbb{F}_3}\left(\widetilde{\mathcal{W}_1}(X) - \frac{\widetilde{f}(X)}{\widetilde{g}(X)}\right) \geq D - d$$

holds for some polynomials $\widetilde{f}, \widetilde{g} \in \mathbb{F}_3[X]$ of degree at most d, where the constant term of $\widetilde{g}$ is nonzero in $\mathbb{F}_3$.

By Lemmas 4 and 5, we see that there exists a positive integer $t < 3^d$ such that $\lambda(n) \equiv \lambda(n+t) \pmod 3$ for $d+1 \leq n < n+t \leq D-d-1$ (note that if $D \leq 2(d+1)$, there is nothing to prove).

Since $\lambda(n) \not\equiv 0 \pmod 3$, by Lemma 6, we see that in fact $t = O(3^{d/2})$. Let $\ell = p_1(t,1)$ be the smallest prime with $\ell \equiv 1 \pmod t$. Let $m = 2d$ if $\gcd(2d, \ell) = 1$ and $m = 2d+1$ otherwise. Assuming that the inequality $D \geq (2d+1)(\ell+1)$ holds, and taking into account that $m \equiv m\ell \pmod t$ and $d+1 \leq m < m\ell \leq D-d-1$, we obtain that

$$\lambda(m) \equiv \lambda(m\ell) \pmod 3.$$

However, $\lambda(m\ell) = -\lambda(m)$, since $\gcd(m, \ell) = 1$. This contradiction shows that $D < (2d+1)(\ell+1)$. Using Lemma 10, we have $D = O\left(d \cdot 3^{11d/4}\right)$ which finishes the proof of our bound for $\Delta_d(\mathcal{L})$.

Because $2 \equiv -1 \pmod 3$ the reductions modulo 3 of $\mathcal{L}(X)$ and $\mathcal{R}(X)$ coincide. We therefore immediately obtain the stated upper bound for $\Delta_d(\mathcal{R})$ as well.

To derive the upper bound on $\Delta_d(\mathcal{M})$, we remark that, by Lemma 8, $\mu(n) \neq 0$ for $(6/\pi^2)t + o(t)$ values of n in the interval $1 \leq n < t$. Hence,

Lemma 6 again applies and we deduce that $t = O(3^{d/2})$. The rest of the proof of the bound for $\Delta_d(\mathcal{M})$ is the same as before (with m chosen as the smallest prime with $m \geq 2d$, $m \neq \ell$).

4.3 The Series $\mathcal{T}(X)$

We assume that

$$\operatorname{ord}\left(\mathcal{T}(X) - \frac{f(X)}{g(X)}\right) = D$$

holds for some polynomials $f, g \in \mathbb{Z}[X]$ of degree at most d and such that $\operatorname{cont}(g) = 1$, and reduce this relation modulo 2.

Recalling that

$$\frac{\zeta(3/2)}{\zeta(2)} = 1.588\ldots < 2,$$

we see that from Lemma 9 that for sufficiently large d there are $d+1$ consecutive non-squarefull integers n in the interval $[d, 2d^2]$. It follows from the explicit formula for $\tau(n)$, that $\tau(n) \equiv 0 \pmod 2$ for every nonsquarefull positive integer n. Thus, by Lemma 4, we see that $\tau(n) \equiv 0 \pmod 2$ for every integer n with $2d^2 \leq n \leq D$. Therefore, if ℓ is the smallest prime with $\ell > \sqrt{2}d$ then $D < \ell^2$, because $\tau(\ell^2) \equiv 1 \pmod 2$. Now the Prime Number Theorem implies the desired bound on $\Delta_d(\mathcal{T})$.

4.4 The Series $\mathcal{P}(X)$

Suppose that $\mathcal{P} = f/g$, that is,

$$\operatorname{ord}\left(\mathcal{P}(X) - \frac{f(X)}{g(X)}\right) = D$$

holds for some polynomials $f, g \in \mathbb{Z}[X]$ of degree at most d, where $d \geq 2$. Reducing this relation modulo 3 and applying Lemma 3, we deduce that

$$\operatorname{ord}_{\mathbb{F}_3}\left(\widetilde{\mathcal{P}}(X) - \frac{\widetilde{f}(X)}{\widetilde{g}(X)}\right) \geq D - d$$

for some polynomials $\widetilde{f}, \widetilde{g} \in \mathbb{F}_3[X]$ of degree at most d, where the constant term of $\widetilde{g}$ is nonzero in $\mathbb{F}_3$.

By Lemmas 4 and 5, it follows that there exists an positive integer $t < 3^d$ such that $p(n) \equiv p(n+t) \pmod 3$ for all $d < n \le n + t < D - d$.

We put $T = D - d$. Clearly, we can assume that T is sufficiently large, because otherwise the bound is trivial.

Since $d \ge 2$, $3 \nmid p(n)$ if $n > d$. Let $a_1, \dots, a_r$ be the distinct congruence classes modulo t such that the conditions $n \ge d + 1$ and $n \equiv a_j \pmod t$ for some $j = 1, \dots, r$ imply that $p(n) \equiv 1 \pmod 3$. Similarly, let $b_1, \dots, b_s$ be the distinct congruence classes modulo t such that the conditions $n \ge d + 1$ and $n \equiv b_j \pmod t$ for some $j = 1, \dots, s$ imply that $p(n) \equiv 2 \pmod 3$. Clearly, $r + s = t$. Now, for $0 \le x \le t$, we have

$$\begin{aligned} \pi(x; 3, 1) &= \#\{n \le \pi(x) : p(n) \equiv 1 \pmod 3\} \\ &= \#\{n \le \pi(x) : n \equiv a_j \pmod t \text{ for some } j = 1, \dots, r\} + O(d) \\ &= \frac{r\,\pi(x)}{t} + O(d + t). \end{aligned}$$

Similarly,

$$\pi(x; 3, 2) = \frac{s\,\pi(x)}{t} + O(d + t).$$

Therefore,

$$|\pi(x; 3, 1) - \pi(x; 3, 2)| = \frac{|r - s|\pi(x)}{t} + O(d + t).$$

Thus, by Lemma 12, and by the Prime Number Theorem if $r \ne s$, we obtain

$$\frac{\log\log\log T}{\log T} T^{1/2} \ll d + t \ll 3^d,$$

which implies the desired bound on $\Delta_d(\mathcal{P})$.

4.5 The Series $\mathcal{F}(X)$ and $\mathcal{S}(X)$

We assume that

$$\operatorname{ord}\left(\mathcal{F}(X) - \frac{f(X)}{g(X)}\right) = D$$

holds for some polynomials $f, g \in \mathbb{Z}[X]$ of degree at most d and such that $\operatorname{cont}(g) = 1$. Reducing this relation modulo 3, for the corresponding reductions defined over $\mathbb{F}_3$, we obtain that

$$\operatorname{ord}_{\mathbb{F}_3}\left(\widetilde{\mathcal{F}}(X) - \frac{\widetilde{f}(X)}{\widetilde{g}(X)}\right) \ge D$$

holds with $\widetilde{f}, \widetilde{g} \in \mathbb{F}_3[X]$. Let $k = \deg \widetilde{g} \le d$.

Let m be the smallest prime with $m \ge d$ and $m \equiv 2 \pmod 3$ and let $\ell = p(3t, 1)$. The congruences

$$\varphi(m) \equiv 1 \pmod 3, \qquad \varphi(\ell) \equiv 0 \pmod 3, \qquad m \equiv m\ell \pmod t,$$

together with Lemmas 4 and 5, show that $D \le m\ell + d$. Thus, by Lemma 10, we obtain

$$D = O(dt^{11/2}). \tag{3}$$

We put $r = \left\lceil k^{2/3} \log^{-1/3} k \right\rceil$ and denote

$$R = r + \frac{1}{k} \sum_{w=1}^{r-1} \binom{k}{w} 2^w (r - w).$$

Using Stirling's formula, one easily derives that

$$\binom{k}{w} \le \frac{k^w}{w!} = O\left(w^{1/2} \left(\frac{ek}{w} \right)^w \right).$$

Therefore,

$$R = O\left(r^{1/2} \sum_{w=1}^{r-1} \left(\frac{2ek}{w} \right)^w \right).$$

It is easy to verify that the function $f(w) = w \log(2ek/w)$ has a positive derivative

$$f'(w) = \log(2ek/w) - 1$$

and thus is decreasing for $1 \le w < 2k$. Hence, because of our choice of r,

$$\sum_{w=1}^{r-1} \left(\frac{2ek}{w} \right)^w \le r \left(\frac{2ek}{r} \right)^r,$$

therefore

$$R = \exp\left(O(k^{2/3} \log^{2/3} k) \right) = \exp\left(O(d^{2/3} \log^{2/3} d) \right).$$

We put

$$T = \left\lceil \exp\left(c d^{2/3} \log^{2/3} d \right) \right\rceil$$

for a sufficiently large constant $c > 0$ such that both inequalities

$$T \geq R^2 \qquad \text{and} \qquad c \geq 4C^2$$

hold, where C is the constant appearing in Lemma 13.

If $t \leq T$, then the desired result follows from (3). Otherwise, Lemma 7 implies that

$$\begin{aligned} \#\left\{d \leq n < d+T \mid \varphi(n) \not\equiv 0 \pmod 3\right\} &\geq \frac{rT}{k} - R \\ &\geq \frac{T}{k^{1/3}\log^{1/3} k} - R \geq 2C\frac{T}{\log^{1/2} T} - T^{1/2} > C\frac{T}{\log^{1/2} T} \end{aligned}$$

provided that d is sufficiently large, which contradicts the upper bound of Lemma 13. The case of the series $\mathcal{S}$ can be handled analogously.

5 Remarks

There are, of course, many other number theoretic series for which similar results can be obtained. For example, one can study

$$\sum_{n=1}^{\infty} P(n)X^n \qquad \text{and} \qquad \sum_{n=1}^{\infty} r(n)X^n,$$

where $P(n)$ is the largest prime divisor of n (and $P(1) = 1$), and $r(n)$ is the number of representations of n as a sum of two square numbers. Generating functions, such as

$$\sum_{n=1}^{\infty} X^{\varphi(n)} \qquad \text{and} \qquad \sum_{n=1}^{\infty} X^{p(n)},$$

can be studied as well. One can also consider power series whose coefficients are powers (or more general polynomial expressions) of the number theoretic functions. Here, we have restricted ourselves to a limited selection of such power series which, nevertheless, allow us to demonstrate various techniques that can be used for questions of this kind.

Finally, one can ask whether the above series are, or can be approximated by, powers series corresponding to algebraic functions or functions satisfying certain functional or differential equations. We hope that our approach may give some insight into these questions too.

References

[1] J.-P. Allouche, 'Transcendence of formal power series with rational coefficients', *Theoret. Comput. Sci..*, **218** (1999), 143–160.

[2] P. Erdős, A. Granville, C. Pomerance and C. Spiro, 'On the normal behaviour of the iterates of some arithmetic functions', *Analytic Number Theory*, Birkhäuser, Boston, 1990, 165–204.

[3] G. Everest, A. J. van der Poorten, I. E. Shparlinski and T. B. Ward, *Recurrence sequences*, Amer. Math. Soc., 2003.

[4] R. Heath-Brown, 'Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression', *Proc. Lond. Math. Soc.*, **64** (1991), 265–338.

[5] R. Heath-Brown, 'Almost-primes in arithmetic progressions and short intervals', *Math. Proc. Cambridge Philos. Soc.*, **83** (1978), 357–375.

[6] J. E. Littlewood, 'Sur la distribution des nombres premiers', *C. R. Acad. Sci. Paris*, **158** (1914), 1869–1872.

[7] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[8] F. Luca and C. Pomerance, 'On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ', *Colloq. Math.*, **92** (2002), 111–130.

[9] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Acad. Publ., Dordrecht, 1999.

[10] D. Suryanarayana and R. Sitaramachandra Rao, 'The distribution of square-full integers', *Arkiv för Matematik*, **11** (1973), 195–201.