Values of the Euler Function in Various Sequences

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

Kevin Ford
Department of Mathematics, 1409 West Green Street
University of Illinois at Urbana-Champaign
Urbana, IL 61801, USA
ford@math.uiuc.edu

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

Francesco Pappalardi
Dipartimento di Matematica, Università Roma Tre
Largo S. L. Murialdo, 1, Roma, 00146, Italy
pappa@mat.uniroma3.it

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

Abstract

Let $\varphi(n)$ and $\lambda(n)$ denote the Euler and Carmichael functions, respectively. In this paper, we investigate the equation $\varphi(n)^r = \lambda(n)^s$, where $r \geq s \geq 1$ are fixed positive integers. We also study those positive integers n, not equal to a prime or twice a prime, such that $\varphi(n) = p-1$ holds with some prime p, as well as those positive integers n such that the equation $\varphi(n) = f(m)$ holds with some integer m, where f is a fixed polynomial with integer coefficients and degree $\deg f > 1$.

1 Introduction

Let $\varphi(n)$ and $\lambda(n)$ denote the *Euler* and *Carmichael* functions, respectively. We recall that, for any positive integer n, $\varphi(n)$ is the cardinality of the multiplicative group $U_n = (\mathbb{Z}/n\mathbb{Z})^\times$, while $\lambda(n)$ is the maximal order of any element in U_n. There exists an extensive literature in which the distributional and arithmetical properties of $\varphi(n)$ and $\lambda(n)$ have been studied (for example, see [1, 3, 4, 5, 6, 8, 9, 12, 13, 14, 15, 16, 17, 24, 26, 28, 29]). Here, we list a few examples of properties and interrelations between $\varphi(n)$, $\lambda(n)$ and n that have been investigated in those works:

- The problem that has attracted perhaps the most attention, which directly relates the arithmetic properties of $\lambda(n)$ and n, is the question about the existence of infinitely many *Carmichael numbers*, that is, composite numbers n for which $\lambda(n) \mid n-1$ (see [1], as well as the recent improvement given in [2]).

- It is shown in [13] that a "typical" value $\varphi(n)$ has about $0.5(\log\log n)^2$ distinct prime divisors (it is useful to recall that a "typical" positive integer n has only about $\log\log n$ distinct prime divisors).

- The set of positive integers n for which the relation

$$\varphi(n) = \left(\prod_{\substack{p \mid n \\ p \text{ prime}}} p \right)^k$$

holds, where k is a fixed positive integer, has been investigated in [8].

- Positive integers n such that $\varphi(n)$ is smooth, and those for which $\varphi(n)$ is a perfect square, have been studied in [3].
- Bounds for exponential sums and the number of solutions of several congruences with $\varphi(n)$ and $\lambda(n)$ are given in [5].

In this paper, we consider several more problems with a similar flavor. In particular, we study the set of positive integers n such that

$$\varphi(n)^{k-1} = \lambda(n)^k,$$

where $k \geq 2$ is an integer; for example,

$$\varphi(1729) = \lambda(1729)^2, \quad \varphi(666)^2 = \lambda(666)^3, \quad \varphi(768)^3 = \lambda(768)^4, \quad \ldots$$

More precisely, for a fixed integer $k \geq 2$ and a real number $x \geq 1$, we define:

$$\mathcal{A}_k(x) = \{n \leq x : \varphi(n)^{k-1} = \lambda(n)^k\}.$$

In Section 2, we establish a lower bound for the cardinality $\#\mathcal{A}_k(x)$. Our bound is constructive, and it allows us to generate elements of $\mathcal{A}_k(x)$ in a regular fashion. In Section 3, we present conditional proofs, under various widely believed conjectures about the distribution of prime numbers (such as Dickson's *Prime k-tuplets Conjecture* and *Schinzel's Hypothesis H*) of the fact that for fixed positive integers $r \geq s \geq 1$ the set $\mathcal{A}_{r,s} = \{n : \varphi(n)^s = \lambda(n)^r\}$ is infinite. We also give an unconditional proof of the fact that the set $\{\log \varphi(n)/\log \lambda(n)\}_{n \geq 3}$ is dense in the interval $[1, \infty)$.

In the special case $k = 2$, an alternative (and more explicit) construction of elements from $\mathcal{A}_2(x)$ arises from solutions to the equation

$$\varphi(n) = p - 1, \qquad n \neq p \text{ or } 2p,$$

where p is prime. Indeed, for any such n, one has $\gcd(n, p) = 1$, and therefore $\varphi(np) = (p-1)^2 = \lambda(np)^2$. Another motivation to consider such equations comes from a very old problem due to Carmichael concerning the study of the equation $\varphi(n) = \varphi(m)$ with distinct positive integers n and m (see [34]). It is certainly interesting to study the equation $\varphi(n) = \varphi(m)$ under various additional hypotheses, as in this case where we insist that $m = p$ be a prime number. Accordingly, we define

$$\mathcal{L}(x) = \{p \leq x : p \text{ prime and } \varphi(n) = p - 1 \text{ for some integer } n \neq p \text{ or } 2p\},$$

and in Section 4, we establish the upper bound

$$\#\mathcal{L}(x) \le \frac{x}{\log^{2+o(1)} x}. \tag{1}$$

We also present heuristic arguments which suggest that this bound is tight, and the term $o(1)$ cannot be removed from the power of $\log x$.

The estimate (1) has an interesting consequence. For each $m \ge 1$, let $A(m)$ be the number of preimages of m under the map $\varphi : \mathbb{N} \to \mathbb{N}$; that is,

$$A(m) = \#\left(\varphi^{-1}(\{m\})\right) = \#\{n : \varphi(n) = m\}.$$

In view of Corollary 3 of [16], we know that for every fixed integer $k \ge 2$, the equation $A(m) = k$ holds for a positive proportion of those integers $m \ge 1$ for which $A(m) \ne 0$. Our result (1) shows that the function A behaves quite differently when restricted to the sequence of shifted primes; in fact, by the prime number theorem, we see that the equation $A(p-1) = 2$ holds for almost all primes p (note that $A(p-1) \ge 2$ for all primes p).

Also in Section 4, we use a similar method to study the cardinality of the related set

$$\mathcal{N}(x) = \{n \le x : \varphi(n) = p - 1 \text{ for some prime } p \nmid n\},$$

and we present heuristic arguments which suggest that our upper bound is rather tight.

Finally, in Section 5 we show that similar arguments can be used to study the values of the Euler function attained by polynomials and other sequences. More precisely, for a polynomial $f(X) \in \mathbb{Z}[X]$, we define

$$\mathcal{N}_f(x) = \{n \le x : \varphi(n) = f(m) \text{ for some integer } m\}.$$

As we have remarked, in the special case $f(X) = X^2$, this problem (and other similar ones) has been studied in [3]. However, the underlying method of that paper cannot be extended to work for general polynomials f. Here, we propose an alternative approach that works for all polynomials of degree $\deg f > 1$.

Throughout this paper, we use the symbols 'O', '$\ll$', '$\gg$', '$\asymp$' and 'o' with their usual meaning (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$ and that $A \asymp B$ means that both $A \gg B$ and $B \gg A$ hold).

We also use $\Omega(n)$, $\omega(n)$ and $\tau(n)$ with their usual meanings: $\Omega(n)$ denotes the number of prime divisors of $n > 1$ counted with multiplicity, $\omega(n)$ is the

number of distinct prime factors of a positive integer $n > 1$, and $\tau(n)$ is the number of divisors of n. We also use $P(n)$ to denote the largest prime factor of $n > 1$, and we adopt the convention that $P(1) = 1$.

Finally, for any real number $x > 0$ and any integer $\ell \geq 1$, we write $\log_\ell x$ for the function defined inductively by $\log_1 x = \max\{\log x, 1\}$ (where $\log x$ is the natural logarithm of x) and $\log_\ell x = \log_1(\log_{\ell-1} x)$ for $\ell > 1$. When $\ell = 1$, we omit the subscript in order to simplify the notation; however, we continue to assume that $\log x \geq 1$ for any $x > 0$.

Acknowledgements. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, K. F. was supported by NSF grant DMS-0301083, F. L. and F. P. were supported in part by a joint Project Italy-Mexico, and I. S. was supported in part by ARC grant DP0211459.

2 Collisions Between Powers of the Euler and Carmichael Functions

In this section, we establish a lower bound on the cardinality of the set $\mathcal{A}_k(x)$.

Theorem 2.1. *For any fixed integer $k \geq 2$, the bound*

$$\#\mathcal{A}_k(x) \geq x^{19/27k}.$$

holds if x is sufficiently large.

Proof. It is known [11] (more recent results can be found in [2] and [18]), that there exists a positive constant $\delta < 1$ such that for all sufficiently large y, the set

$$\mathcal{P} = \{p \leq y : p \text{ prime and } P(p-1) < y^{1-\delta}\} \tag{2}$$

has cardinality

$$\#\mathcal{P} \geq y \exp\left(-\log^{1/2} y\right). \tag{3}$$

Let

$$\mathcal{Q} = \{q \leq y^{1-\delta} : q \text{ prime}\} \tag{4}$$

and observe that $\mathcal{Q} \subset \mathcal{P}$. Taking $\mathcal{R} = \mathcal{P} \setminus \mathcal{Q}$, we have

$$\#\mathcal{R} = \#\mathcal{P} - \#\mathcal{Q} \geq y \exp\left(-\log^{1/2} y\right) - \pi(y^{1-\delta}) \geq y \exp\left(-\log^{2/3} y\right) \tag{5}$$

if y is sufficiently large. For any subset $\mathcal{S}$ of $\mathcal{P}$, let $m_{\mathcal{S}}$ be the positive squarefree integer whose prime factors are precisely the elements of $\mathcal{S}$, and for every $q \in \mathcal{Q}$, let the nonnegative integers $\{\alpha_q(\mathcal{S}) : q \in \mathcal{Q}\}$ be defined by the relation

$$\varphi(m_{\mathcal{S}}) = \prod_{p \in \mathcal{S}} (p-1) = \prod_{q \in \mathcal{Q}} q^{\alpha_q(\mathcal{S})}.$$

From now on, $\mathcal{T}$ denotes an arbitrary subset of $\mathcal{R}$. For any such subset $\mathcal{T}$, let $\mathcal{S} = \mathcal{S}(\mathcal{T}) = \mathcal{Q} \cup \mathcal{T}$, and let $n_{\mathcal{T}}$ be the positive integer given by

$$n_{\mathcal{T}} = 2^{k+1} m_{\mathcal{S}} \varphi(m_{\mathcal{S}})^{k-1} = 2^{(k-1)\alpha_2(\mathcal{S})+k+1} \prod_{\substack{q \in \mathcal{Q} \\ q \neq 2}} q^{(k-1)\alpha_q(\mathcal{S})+1} \prod_{p \in \mathcal{T}} p.$$

Note that, by unique factorization, different subsets $\mathcal{T} \subset \mathcal{R}$ lead to distinct values of the positive integer $n_{\mathcal{T}}$.

Let us first verify that every number $n = n_{\mathcal{T}}$ with $\mathcal{T} \subset \mathcal{R}$ satisfies the relation $\varphi(n)^{k-1} = \lambda(n)^k$ whenever y is sufficiently large. Since

$$\varphi(n_{\mathcal{T}}) = \varphi(m_{\mathcal{S}}) \cdot 2^{(k-1)\alpha_2(\mathcal{S})+k} \prod_{\substack{q \in \mathcal{Q} \\ q \neq 2}} q^{(k-1)\alpha_q(\mathcal{S})} = \left(2^{\alpha_2(\mathcal{S})+1} \prod_{\substack{q \in \mathcal{Q} \\ q \neq 2}} q^{\alpha_q(\mathcal{S})} \right)^k, \quad (6)$$

it suffices to show that

$$\lambda(n_{\mathcal{T}}) = \left(2^{\alpha_2(\mathcal{S})+1} \prod_{\substack{q \in \mathcal{Q} \\ q \neq 2}} q^{\alpha_q(\mathcal{S})} \right)^{k-1}.$$

Now $\lambda(n_{\mathcal{T}})$ is the least common multiple of the numbers:

- $\lambda\left(2^{(k-1)\alpha_2(\mathcal{S})+k+1}\right) = 2^{(k-1)(\alpha_2(\mathcal{S})+1)}$,
- $\lambda\left(q^{(k-1)\alpha_q(\mathcal{S})+1}\right) = q^{(k-1)\alpha_q(\mathcal{S})}(q-1)$ with $q \in \mathcal{Q}$,
- $\lambda(p) = p-1$ with $p \in \mathcal{T}$.

Moreover, it is clear that the only primes q dividing $\lambda(n_{\mathcal{T}})$ are those that lie in $\mathcal{Q}$.

For a prime q and integers $a \geq 0$ and $s \geq 1$, we write, as usual, $q^a \parallel s$ if $q^a \mid s$ but $q^{a+1} \nmid s$.

Fix an odd prime $q \in \mathcal{Q}$. Since

$$q^{(k-1)\alpha_q(\mathcal{S})} \parallel \lambda\big(q^{(k-1)\alpha_q(\mathcal{S})+1}\big),$$

it follows that $q^{(k-1)\alpha_q(\mathcal{S})} \mid \lambda(n_{\mathcal{T}})$. To see that $q^{(k-1)\alpha_q(\mathcal{S})} \parallel \lambda(n_{\mathcal{T}})$, let us assume that this is not so. Then there exists $\gamma > (k-1)\alpha_q(\mathcal{S}) \geq \alpha_q(\mathcal{S})$ and a prime $p \in \mathcal{S}$ such that $q^\gamma \mid p-1$. But then q^γ must also divide

$$\varphi(m_{\mathcal{S}}) = \prod_{p \in \mathcal{S}} (p-1) = \prod_{r \in \mathcal{Q}} r^{\alpha_r(\mathcal{S})},$$

which is clearly impossible. Now suppose that $q = 2$. Since

$$2^{(k-1)(\alpha_2(\mathcal{S})+1)} \parallel \lambda\big(2^{(k-1)\alpha_2(\mathcal{S})+k+1}\big),$$

it follows that $q^{(k-1)(\alpha_2(\mathcal{S})+1)} \parallel \lambda(n_{\mathcal{T}})$. To show that $q^{(k-1)(\alpha_2(\mathcal{S})+1)} \parallel \lambda(n_{\mathcal{T}})$, we assume that this is not the case and argue as before.

Thus, we have shown that

$$\lambda(n) = 2^{(k-1)(\alpha_2(\mathcal{S})+1)} \prod_{\substack{q \in \mathcal{Q} \\ q \neq 2}} q^{(k-1)\alpha_q(\mathcal{S})} = \left(2^{\alpha_2(\mathcal{S})+1} \prod_{\substack{q \in \mathcal{Q} \\ q \neq 2}} q^{\alpha_q(\mathcal{S})} \right)^{k-1},$$

and using (6), we derive the relation $\varphi(n_{\mathcal{T}})^{k-1} = \lambda(n_{\mathcal{T}})^k$.

It now remains to count numbers of the form $n_{\mathcal{T}}$. Let $N = \lfloor \delta y^{1-\delta} \rfloor$. Then, by (5), the number of subsets $\mathcal{T} \subset \mathcal{R}$ of cardinality N is

$$\begin{aligned} \binom{\#\mathcal{R}}{N} \geq \left(\frac{\#\mathcal{R}}{N}\right)^N &\geq \left(\frac{y \exp\left(-\log^{2/3} y\right)}{\delta y^{1-\delta}} \right)^{\delta y^{1-\delta} + o(1)} \\ &= \exp\big((1+o(1))\delta^2 y^{1-\delta} \log y\big) \end{aligned}$$

as $y \to \infty$. On the other hand, each integer $n_{\mathcal{T}}$ satisfies the bound

$$\begin{aligned} n_{\mathcal{T}} &= 2^{k+1} m_{\mathcal{S}} \varphi(m_{\mathcal{S}})^{k-1} < 2^{k+1} m_{\mathcal{S}}^k < 2^{k+1} \Big(\prod_{q \in \mathcal{Q}} q \Big)^k y^{kN} \\ &= \exp\big((1+o(1))k\delta y^{1-\delta} \log y\big) \end{aligned}$$

as $y \to \infty$; here, we have used the estimate

$$\prod_{q \in \mathcal{Q}} q \sim \exp(y^{1-\delta})$$

as y tends to infinity, which follows from the Prime Number Theorem.

Now let $\varepsilon > 0$ be small and fixed, and put $\vartheta = k\varepsilon/(2\delta - k\varepsilon) > 0$. For all sufficiently large x, define y by the relation

$$x = \exp\left((1+\vartheta)k\delta y^{1-\delta} \log y\right).$$

Then if x is large enough, we see that $n_{\mathcal{T}} \le x$ for every subset $\mathcal{T} \subset \mathcal{R}$ of cardinality N, and the number of such subsets is at least

$$\exp\left((1-\vartheta)\delta^2 y^{1-\delta} \log y\right) = x^{\delta/k-\varepsilon}.$$

According to Theorem 1 from [2], one can take $\delta = 0.7039$. Choosing ε sufficiently small for any given value of k, we obtain the stated result. □

3 Further Collisions

We recall the statement of the *Prime k-tuples Conjecture* (see [10, 20, 32]), which is due to Dickson.

Conjecture 3.1. *For any $k \ge 2$, let $a_1, \dots, a_k$ and $b_1, \dots, b_k$ be integers with $a_i > 0$ and $\gcd(a_i, b_i) = 1$ for each $i = 1, \dots, k$. Suppose that for every prime number $p \le k$ there exists an integer n such that $\prod_{i=1}^{k}(a_i n + b_i)$ is not a multiple of p. Then there exist infinitely many positive integers n such that $p_i = a_i n + b_i$ is prime for all $i = 1, \dots, k$.*

Theorem 3.2. *Assume that Conjecture 3.1 holds. Then for every positive integer r there exist infinitely many n such that $\varphi(n) = \lambda(n)^r$.*

Proof. The case $r = 1$ is trivial since $\varphi(n) = \lambda(n)$ for every prime n, so we may assume that $r \ge 2$. Let $c_1 > \ldots > c_r > 1$ be positive integers such that $D = \prod_{i=1}^{r} c_i$ has the following properties:

- $D + 1$ is a prime number,
- D/c_i is a multiple of $M_r = \mathrm{lcm}[1, \dots, r]$ for $i = 1, \dots, r$.

To construct such a D, we can choose $c_i = (r+1-i)M_r$ for $i = 2, \ldots, r$ and then let $c_1 = M_r\lambda$, where $\lambda \equiv 1 \pmod{M_r}$ is sufficiently large and $D+1 = M_r c_2 c_3 \ldots c_r \lambda + 1$ is prime. Let us write $a_i = D^2/c_i$ and $b_i = D/c_i + 1$ for $i = 1, \ldots, r$. Then it is easy to see that $\gcd(a_i, b_i) = 1$ for $i = 1, \ldots, r$. Moreover, if n is an arbitrary positive integer and $p \le r$ is a prime, then p divides D/c_i for all $i = 1, \ldots, r$, and thus $a_i n + b_i = (D^2/c_i)n + (D/c_i + 1)$ is coprime to p; in particular, $\prod_{i=1}^{r}(a_i n + b_i)$ is coprime to all primes $p \le r$. By Conjecture 3.1, there exist infinitely many n such that $p_i = a_i n + b_i$ is prime for all $i = 1, \ldots, r$. Let n be one such number. Write $\ell = Dn + 1$, so that $p_i = (D/c_i)\ell + 1$ for $i = 1, \ldots, r$. Put also $p_0 = D+1$. Since $c_1 > \ldots > c_r > 1$ it follows that $p_0 < p_1 < \ldots < p_r$. Let $m = \prod_{i=0}^{r} p_i$. Then

$$\varphi(m) = \prod_{i=0}^{r}(p_i - 1) = D\prod_{i=1}^{r}(D/c_i)\ell = (D\ell)^r$$

We also have

$$\lambda(m) = \operatorname{lcm}[p_i - 1 : i = 0, \ldots, r] = D\ell,$$

since, on the one hand, $\lambda(n) \mid D\ell$, while on the other hand, D and ℓ are coprime, $D \mid (p_0 - 1) \mid \lambda(n)$ and $\ell \mid (p_1 - 1) \mid \lambda(n)$; thus $D\ell \mid \lambda(m)$. This shows that the number m satisfies $\varphi(m) = \lambda(m)^r$, and the result follows. □

Remark 3.3. *A more precise version of Conjecture 3.1 (see [20, 32]) is that under the given assumptions there exists a constant c, depending only on k, $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$, such that the number of positive integers $n \le x$ such that $a_i n + b_i$ is prime for all $i = 1, \ldots, k$ is asymptotic to $(c + o(1))x/\log^k x$. Under this stronger conjecture, the construction in the proof of Theorem 3.2 implies the number of positive integers $n \le x$ for which $\varphi(n) = \lambda(n)^r$ is of order at least $x^{1/r}/\log^r x$ as $x \to \infty$.*

We now recall the statement of *Schinzel's Hypothesis H* (see [32]).

Conjecture 3.4. *Suppose that $f_1(n), \ldots, f_r(n)$ are irreducible, and integer valued polynomials (for integral n) with positive leading coefficients. Also, suppose that for every prime q there exists a positive integer n such that $q \nmid f_1(n) \ldots f_r(n)$. Then the numbers $f_1(n), \ldots, f_r(n)$ are simultaneously prime for infinitely many positive integers n.*

Theorem 3.5. *Assume that Conjecture 3.4 holds. Then for all positive integers $r \ge s$ there exist infinitely many n such that $\varphi(n)^s = \lambda(n)^r$.*

Proof. We may clearly assume that $r > s$ and that r and s are coprime. Put $t = 2(r-s)+1 \geq 3$. Let $a_1, \ldots, a_{t-1} >$ be squarefree positive integers that are pairwise coprime and such that the product $a_1 \ldots a_{t-1}$ is a multiple of $M = \prod_{p \leq rt} p$. Let $\alpha_i = i$ for $i = 1, \ldots, t-1$, and let $\alpha_t = ts$. We define a collection of polynomials as follows. First, let

$$f_1(n) = a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_{t-1}^{\alpha_{t-1}} n^{\alpha_t} + 1.$$

Next, let $f_2(n), \ldots, f_t(n)$ be obtained from $f_1(n)$ by cyclically permuting the exponents $\alpha_1, \ldots, \alpha_t$; that is,

$$f_i(n) = a_1^{\alpha_i} a_2^{\alpha_{i+1}} \ldots a_{t-i+1}^{\alpha_t} a_{t-i+2}^{\alpha_1} \ldots a_{t-1}^{\alpha_{i-2}} n^{\alpha_{i-1}} + 1$$

for $i = 2, \ldots, t$. We claim that the polynomials $f_1(n), \ldots, f_t(n)$ satisfy the conditions of Conjecture 3.4. Indeed, note that each $f_i(n)$ is primitive (because its last coefficient is 1), and it is irreducible because $f_i(n) = A_i n^{\beta_i} + 1$ with some positive integers A_i and β_i, and such a polynomial is reducible if and only if there exists a prime number p dividing β_i such that A_i is the p-th power of a rational number. Since $a_1, \ldots, a_{t-1}$ are pairwise coprime and squarefree, it follows that if such p exists, then it must divide every α_i for $i = 1, \ldots, t-1$, which is impossible because $\alpha_1 = 1$. Finally, to see that for every prime q there exists a positive integer n such that $q \nmid f(n)$, where

$$f(n) = \prod_{i=1}^{t} f_i(n),$$

note that $f(n)$ is a polynomial of degree $t(t-1)/2 + st = rt$, which is constant (and equal to 1) modulo every prime $q \leq rt$ since

$$M \;\Big|\; \prod_{i=1}^{t-1} a_i.$$

If particular, $f(n)$ is nonzero modulo q for any n provided that $q \leq rt$. If $q > rt = \deg f$, then since f is primitive, it follows that f cannot have more than $\deg f < q$ roots n modulo q; in particular, there exists an integer n such that $f(n)$ is nonzero modulo q. This proves the claim.

By Conjecture 3.4, there exist infinitely many positive integers n such that $f_i(n)$ is prime for all $i = 1, \ldots, t$. Moreover, we can assume that for infinitely

many of these, n is coprime to $a_1 \dots a_{t-1}$; indeed, assuming Conjecture 3.4, and replacing $f_i(n)$ by

$$g_i(n) = f_i\left(\prod_{i=1}^{t-1} a_i n + 1\right)$$

for $i = 1, \dots, t$, one may check (as above) that the polynomials $g_i(n)$ satisfy the conditions of Conjecture 3.4 for $i = 1, \dots, t$ as well.

Write $p_i = f_i(n)$ for $i = 1, \dots, t$, and let $m = \prod_{i=1}^{t} p_i$. Clearly,

$$\varphi(m) = \left(n \prod_{i=1}^{t-1} a_i\right)^{\sum_{i=1}^{t} \alpha_i} = \left(n \prod_{i=1}^{t-1} a_i\right)^{t(t-1)/2+st} = \left(n \prod_{i=1}^{t-1} a_i\right)^{rt}.$$

On the other hand, since $a_1, \dots, a_{t-1}, n$ are pairwise coprime and $\alpha_t > \alpha_i$ for $i = 1, \dots, t-1$, we get that

$$\lambda(m) = \left(n \prod_{i=1}^{t-1} a_i\right)^{\alpha_t} = \left(n \prod_{i=1}^{t-1} a_i\right)^{st}.$$

From the above computations, it is seen that $\varphi(m)^s = \lambda(m)^r$, and this finishes the proof. □

As a consequence of Theorem 3.2, we see that the truth of Conjecture 3.1 implies that the function $\log \varphi(n)/\log \lambda(n)$ contains in its range all positive integers. Similarly, by Theorem 3.5 we see that if Conjecture 3.4 is true, then this function contains in its range all rational numbers greater than 1. We close this section by giving an unconditional proof of the fact that the range of the above function is dense in $[1, \infty)$.

Theorem 3.6. *The set* $\{\log \varphi(n)/\log \lambda(n)\}_{n \geq 3}$ *is dense in* $[1, \infty)$.

Proof. It suffices to show that if $\alpha > 1$ is fixed but arbitrary, then α is a limit point of the sequence $\{\log \varphi(n)/\log \lambda(n)\}_{n \geq 3}$. Let $\delta \in (0, 1/2)$ and let y be sufficiently large so that if $\mathcal{P}$ is the set defined by (2), then (3) holds. Let $\beta = \lfloor \log y/\log 2 \rfloor + 1$. Let $\mathcal{Q}$ be the set of primes defined by (4), and put

$$m = \left(\prod_{q \in \mathcal{Q}} q\right)^{\beta} \qquad \text{and} \qquad n = m \prod_{p \in \mathcal{P} \setminus \mathcal{Q}} p.$$

It is obvious that $\lambda(n) = \lambda(m)$. Moreover

$$\log \lambda(n) = (\beta - 1) \sum_{q \le y^{1-\delta}} \log q \asymp y^{1-\delta} \log y = y^{1-\delta+o(1)},$$

while

$$\log \varphi(n) = \log \lambda(n) + \sum_{p \in \mathcal{P}} \log(p-1) \asymp \#\mathcal{P} \cdot \log y = y^{1+o(1)}.$$

In particular, we see that

$$\frac{\log \varphi(n)}{\log \lambda(n)} = y^{\delta+o(1)}, \tag{7}$$

while

$$\frac{\log \varphi(n)}{\log^2 \lambda(n)} = y^{2\delta-1+o(1)} = o(1). \tag{8}$$

We now assume that $y > \alpha^{2\delta^{-1}}$ so that by (7) $\log \varphi(n)/\log \lambda(n) > \alpha$. We construct a finite sequence $n_1 < n_2 < \ldots < n_t$ as follows: Let $n_1 = n$. If n_i has been constructed, we then set $n_{i+1} = n_i p_i$, where p_i is a prime in the interval $\mathcal{J} = (y^5/2, y^5)$ which does not divide n_i, such that further $(p_i - 1)/2$ has at most two prime factors, none of which divides $\varphi(n_i)$, and each one of which exceeds $y^{5/4}$. If no such p_i exists, we stop.

Let t be the maximal index for which p_i exists. We claim that $t > y^{5/4}/\log^3 y$. Indeed, since $P(n_1) < y^{1-\delta} < y^{5/4}$, it suffices to find a lower bound on the positive integer t giving the length of the longest chain of primes $p_1, \ldots, p_t$ such that $p_i \in \mathcal{J}$, $(p_i - 1)/2$ has at most two prime factors, each one exceeding $y^{5/4}$, and such that $(p_{i+1} - 1)/2$ is coprime to $p_j - 1$ for all $j \le i$. By the Chen theorem (see [22]), the set $\mathcal{P}_0$ of primes p in $\mathcal{J}$ such that $(p-1)/2$ has at most two prime factors, each one exceeding $y^{5/4}$, is of cardinality $\#\mathcal{P}_0 \gg y^5/\log^2 y$. If t denotes the length of the longest such chain, it then follows that every such prime p in $\mathcal{P}_0$ has $p-1$ divisible by some prime $q > 2$ dividing $p_i - 1$ for some $i \le t$. The number of such primes q is at most $2t$. For each prime q, the number of primes $p \le y^5$ that are congruent to 1 modulo q does not exceed $y^5/q \le y^{15/4}$. Thus, the total number of such primes p in $\mathcal{P}_0$ cannot exceed $2ty^{15/4}$, and, by the Chen theorem, we get $t \gg y^{5/4}/\log^2 y$. Thus, the inequality $t > y^{5/4}/\log^3 y$ holds once y is large enough. Assume now that $i \le t$ is such that

$$\frac{\log \varphi(n_i)}{\log \lambda(n_i)} > \alpha. \tag{9}$$

Note that $i = 1$ is one such index. We then show that for sufficiently large y we have

$$\frac{\log \varphi(n_i)}{\log \lambda(n_i)} > \frac{\log \varphi(n_{i+1})}{\log \lambda(n_{i+1})}.$$

Indeed, the above inequality is equivalent to

$$\frac{\log \varphi(n_i)}{\log \lambda(n_i)} > \frac{\log \varphi(n_i) + \log(p_i - 1)}{\log \lambda(n_i) + \log(p_i - 1) - \log 2},$$

which in turn is equivalent to

$$\frac{\log \varphi(n_i)}{\log \lambda(n_i)} > 1 + \frac{\log 2}{\log(p_i - 1) - \log 2}$$

which is certainly true for sufficiently large y by (9) and the inequality $\alpha > 1$. Define t_0 as the largest integer $t_0 \le t$ such that $\log \varphi(n_i)/\log \lambda(n_i) > \alpha$ holds for all $i = 1, \dots, t_0$ (but not for t_0+1). By the above argument, we have that $\log \varphi(n_i)/\log \lambda(n_i)$ is decreasing for $i = 1, \dots, t_0$. The difference between two consecutive values is positive but upper bounded by

$$\begin{aligned}\frac{\log \varphi(n_i)}{\log \lambda(n_i)} - \frac{\log \varphi(n_{i+1})}{\log \lambda(n_{i+1})} &= \frac{\log \varphi(n_i)}{\log \lambda(n_i)} - \frac{\log \varphi(n_i) + \log(p_i - 1)}{\log \lambda(n_i) + \log(p_i - 1) - \log 2} \\ &\ll \frac{\log \varphi(n_i) \log p_i}{\log^2 \lambda(n_i)} \ll \frac{\log \varphi(n_1) \log y}{\log^2 \lambda(n_1)} \ll y^{1-2\delta+o(1)} = o(1),\end{aligned}$$

because of (8). Finally, notice that when $i = t$ the inequality

$$\frac{\log \varphi(n_t)}{\log \lambda(n_t)} < \frac{\log \varphi(n_1) + t \log(y^5)}{\log \lambda(n_1) + t(\log(y^5/2) - \log 2)} = 1 + o(1) < \alpha$$

holds if y is large enough. It is now clear that α is a limit point of the sequence $\{\log \varphi(n)/\log \lambda(n)\}_{n \ge 3}$, and this completes the proof. □

4 Euler Function and Shifted Primes

Let

$$\kappa = \frac{1}{2 \log \rho^{-1}} = 0.8178\dots,$$

where $\rho = 0.5425\ldots$ is the unique root of the equation

$$\sum_{i=1}^{\infty} a_i \rho^i = 1$$

with $a_i = (i+1)\log(i+1) - i\log i - 1$, $i = 1, 2, \ldots$ (see [15, 26] for more details).

Theorem 4.1. *The inequality*

$$\#\mathcal{L}(x) \ll \frac{x}{\log^2 x} \exp((\kappa + o(1))(\log_3 x)^2)$$

holds as $x \to \infty$.

Proof. Let x be a large positive real number and put

$$y = \max_{\varphi(n)+1 \in \mathcal{L}(x)} n, \qquad u = \log_2 x \qquad \text{and} \qquad z = y^{1/u}.$$

From Theorem 328 of [21], we have $\varphi(n) \gg n/\log_2 n$, therefore

$$y \ll x \log_2 x.$$

Let $\mathcal{E}_1(y) = \{n \le y : P(n) \le z\}$ be the set of positive integers $n \le y$ which are z-smooth. By the corollary to Theorem 3.1 of [7] (see also [23] and [33]), we have

$$\#\mathcal{E}_1(y) \ll \exp(-(u + o(u))\log u)y \ll \frac{x}{\log^2 x}.$$

We now denote by $\mathcal{E}_2(y)$ the set of positive integers $n \le y$ such that $q^2 \mid n$ for some prime $q > z$. Clearly,

$$\#\mathcal{E}_2(y) \ll \sum_{q>z} \frac{y}{q^2} \ll \frac{y}{z} \ll \frac{x \log_2 x}{z} \ll \frac{x}{\log^2 x}.$$

Finally, let

$$\widetilde{\mathcal{N}}(y) = \mathcal{N}(y) \setminus (\mathcal{E}_1(y) \cup \mathcal{E}_2(y)).$$

In particular, $P(n) \ge z$ and $P(n)^2 \nmid n$ for every $n \in \widetilde{\mathcal{N}}(y)$. Thus, each $n \in \widetilde{\mathcal{N}}(y)$ leads to a solution (p, ℓ) to the equation $\varphi(m)\ell - (\varphi(m) - 1) = p$,

where the primes p, ℓ satisfy $p \le x$ and $\ell \le y/m$. Note that $\varphi(m) > 1$ since $m \ge 3$, and we have $m \le y/z$.

By the Brun method (see, for example, Theorem 2.3 in [19]), we see that for any integers $a \ge 1$ and $b \ge 1$ with $\gcd(a, b) = 1$, the linear form $a\ell + b$ takes prime values for at most

$$O\left(\frac{y}{\varphi(a)\log^2(y/a)}\right) = O\left(\frac{y\log_2 a}{a\log^2(y/a)}\right) \tag{10}$$

primes $\ell \le y/a$. Let $\mathcal{V}(t)$ be the set of values of the Euler function up to t; that is,

$$\mathcal{V}(t) = \{a \le t : a = \varphi(m) \text{ for some } m \in \mathbb{Z}\}.$$

Let

$$w = \max_{m \le y/z} \varphi(m).$$

We have

$$w \le yz^{-1}.$$

Using (10) with a running through the set $\mathcal{V}(w)$ and $b = 1 - a$, and taking into account that

$$\log(y/a) \ge \log(y/w) \gg \log z = \frac{\log y}{u} \gg \frac{\log x}{\log_2 x},$$

we obtain

$$\#\mathcal{L}(y) \ll \#\mathcal{E}_1 + \#\mathcal{E}_2 + \sum_{a \in \mathcal{V}(w)} \frac{y\log_2 a}{a\log^2(y/a)} \ll \frac{x(\log_2 x)^3}{\log^2 x} \sum_{a \in \mathcal{V}(w)} \frac{1}{a}.$$

Using the inequality

$$\#\mathcal{V}(t) = \frac{t}{\log t}\exp((\kappa + o(1))(\log_3 t)^2) \tag{11}$$

given in [26] (see also [15] for a more precise statement), and partial summation, we derive that

$$\sum_{a \in \mathcal{V}(w)} \frac{1}{a} = \exp((\kappa + o(1))(\log_3 w)^2),$$

and the result follows. □

Remark 4.2. *Clearly, if $q > 3$ is a Sophie Germain prime (that is, $p = 2q+1$ is also prime), then $\varphi(3q) = 2q = \varphi(p)$, which together with the effective version of Conjecture 3.1 from [20, 32] seems to imply that $\mathcal{L}(x) \gg x/\log^2 x$. Heuristic considerations suggest that*

$$\lim_{x\to\infty} \#\mathcal{L}(x)\frac{\log^2 x}{x} = \infty.$$

This is based on considering, as in the previous proof, integers of the form $n = m\ell \le x$ with $m \le y$ and such that $p = \varphi(m)\ell + 1$ is prime, where y is some slowly growing function of x. For example, if the density of such primes p is of order $x/(\varphi(m)\log^2 x)$ uniformly for $m \le y$, then the bound (11) implies

$$\#\mathcal{L}(x) \gg \frac{\log^2 x}{x}\sum_{a\in\mathcal{V}(y)}\frac{1}{a} \gg \frac{\log^2 x}{x}\exp((\kappa + o(1))(\log_3 y)^2)$$

(it is useful to notice that $\log_3 y = (1 + o(1))\log_3 x$ even when y is very small compared to x). However, it seems that proving of the above relations is out of reach nowadays as it requires a very strong quantitative form of Conjecture 3.1.

The above method applies also to give an upper bound on $\#\mathcal{N}(x)$.

Theorem 4.3. *The inequality*

$$\#\mathcal{N}(x) \ll \frac{x\log_3 x}{\log x}$$

holds for sufficiently large values of x.

Proof. Let $y = x^{1/\log_2 x}$ and set

$$\mathcal{E}_1(x) = \{n \le x : P(n) \le y \text{ or } P(n)^2|n\}.$$

As in the proof of Theorem 4.1, $\#\mathcal{E}_1(x) \ll x/\log x$. We now define the sets

$$\mathcal{E}_2(x) = \mathcal{N}(x)\backslash\mathcal{E}_1(x)$$

and

$$\mathcal{M}(x) = \{3 \le m \le x/y : P(m) \le x/m\}.$$

Therefore, every $n \in \mathcal{E}_2(x)$ can be written as $n = \ell m$, where $\ell = P(n) > P(m)$, and $m \in \mathcal{M}(x)$.

Fix $m \in \mathcal{M}(x)$. Then the equation $\varphi(n) = (\ell-1)\varphi(m) = p-1$ holds with some prime p. In particular, $\varphi(m)\ell - (\varphi(m)-1) = p$. Since $\varphi(m) - 1 > 0$ and $\gcd(\varphi(m), \varphi(m)-1) = 1$, by the Brun method (see Theorem 2.3 in [19] and (10)), the number of primes $\ell \le x/m$ for which the above equation holds with some other prime p is

$$O\left(\frac{x}{\varphi(\varphi(m))\log(x/\varphi(m))^2}\right) = O\left(\frac{x}{\varphi(\varphi(m))\log^2(x/m)}\right).$$

Summing up the above inequality over all the possible values of m, we get

$$\#\mathcal{E}_2(x) \ll x \sum_{m \in \mathcal{M}(x)} \frac{1}{\varphi(\varphi(m))\log^2(x/m)}. \tag{12}$$

We now recall the estimate

$$\sum_{\substack{m \le t \\ p \mid \varphi(m)}} 1 \ll \frac{t \log_2 t}{p}$$

(see Theorem 3.5 in [12], for example). Let $z = \log_2^5 x$ and for $m < x$ define

$$h(m) = \sum_{\substack{p \mid \varphi(m) \\ p > z}} \frac{1}{p-1}.$$

Clearly, by changing the order of summation, we have

$$\sum_{m<t} h(m) = \sum_{m<t} \sum_{\substack{p \mid \varphi(m) \\ p>z}} \frac{1}{p-1} \ll \sum_{z<p<t} \frac{1}{p} \sum_{\substack{m<t \\ p \mid \varphi(m)}} 1 \ll t \log_2 t \sum_{p>z} \frac{1}{p^2} \ll \frac{t \log_2 t}{z \log z},$$

which shows that if we set $\mathcal{H}(t) = \{m < t : h(m) > 1\}$, then

$$\#\mathcal{H}(t) \le \sum_{m \in \mathcal{H}(t)} h(m) \le \sum_{m<t} h(m) \ll \frac{t \log_2 t}{z \log z}. \tag{13}$$

For $m \in \mathcal{H}(x/y)$, we use the fact that

$$\frac{1}{\varphi(\varphi(m))} = \frac{1}{m} \cdot \frac{m}{\varphi(m)} \cdot \frac{\varphi(m)}{\varphi(\varphi(m))} \ll \frac{(\log_2 x)^2}{m},$$

together with the fact that

$$\frac{1}{\log^2(x/m)} \le \frac{1}{\log^2 y} \ll \frac{\log_2^2 x}{\log^2 x}.$$

Hence, by inequality (13) and partial summation, we get that

$$\begin{aligned}
\sum_{m\in\mathcal{H}(x/y)} \frac{1}{\varphi(\varphi(m))\log^2(x/m)} &\ll \frac{\log_2^4 x}{\log^2 x} \sum_{m\in\mathcal{H}(x/y)} \frac{1}{m} \\
&= \frac{\log_2^4 x}{\log^2 x}\left(\int_1^{x/y} \frac{1}{t} d(\#\mathcal{H}(t)) + O(1)\right) \\
&\ll \frac{\log_2^4 x}{\log^2 x}\left(\int_1^{x} \frac{\#\mathcal{H}(t)}{t^2} dt + 1\right) \\
&\ll \frac{\log_2^4 x}{\log^2 x}\left(\frac{1}{z\log z}\int_1^{x} \frac{\log_2 t}{t} dt + 1\right) \\
&\ll \frac{\log_2^4 x}{\log^2 x}\left(1 + \frac{\log x \log_2 x}{z\log z}\right) \ll \frac{1}{\log x \log_3 x}.
\end{aligned}$$

We now estimate the contribution to the sum in (12) from $m \notin \mathcal{H}(x/y)$. By the Mertens formula, we deduce that if $m \notin \mathcal{H}(x/y)$, then

$$\begin{aligned}
\frac{1}{\varphi(\varphi(m))} &= \frac{1}{\varphi(m)}\frac{\varphi(m)}{\varphi(\varphi(m))} = \frac{1}{\varphi(m)} \prod_{p\mid\varphi(m)} \left(1 + \frac{1}{p-1}\right) \\
&\le \frac{1}{\varphi(m)} \prod_{p<z} \left(1 + \frac{1}{p-1}\right) \prod_{\substack{p>z \\ p\mid\varphi(m)}} \left(1 + \frac{1}{p-1}\right) \\
&\ll \frac{\exp(h(m))\log z}{\varphi(m)} \ll \frac{\log z}{\varphi(m)} \ll \frac{\log_3 x}{\varphi(m)}.
\end{aligned}$$

Therefore, it is now suffices to show that

$$\sum_{m\in\mathcal{M}(x)} \frac{1}{\varphi(m)\log^2(x/m)} \ll \frac{1}{\log x}. \tag{14}$$

From the Landau bound of the sum of reciprocals of the Euler function (see [27]), we derive that

$$\sum_{m\le x^{1/2}} \frac{1}{\varphi(m)\log^2(x/m)} \ll \frac{1}{\log^2 x} \sum_{m\le x^{1/2}} \frac{1}{\varphi(m)} \ll \frac{1}{\log x}.$$

Let $w = \lfloor \log_2 x \rfloor + 1$. For an integer k in the interval $2 \le k \le w$, we define the set

$$\mathcal{F}_k(x) = \{m \in \mathcal{M}(x) : x^{1-1/k} < m \le x^{1-1/(k+1)}\}$$

Clearly, each $m \in \mathcal{F}_k(x)$ is $x^{1/k}$-smooth and also $1/\log(x/m) \ll k/\log x$. Thus,

$$\sum_{m \in \mathcal{F}_k(x)} \frac{1}{\varphi(m)\log^2(x/m)} \ll \frac{k^2}{\log^2 x} \sum_{\substack{x^{1-1/k} < m \le x^{1-1/(k+1)} \\ P(m) < x^{1/k}}} \frac{1}{\varphi(m)}.$$

From Lemma 1 of [30], one derives, via partial summation (see also the proof of Theorem 2 of [30]), that

$$\sum_{\substack{x^{1-1/k} < m \le x^{1-1/(k+1)} \\ P(m) < x^{1/k}}} \frac{1}{\varphi(m)} \le k^{-k+o(k)} \log x.$$

Thus,

$$\sum_{m \in \mathcal{F}_k(x)} \frac{1}{\varphi(m)\log^2(x/m)} \ll \frac{k^{-k+o(k)}}{\log x},$$

and summing up over k we get (14), thus completing the proof. □

Remark 4.4. *Heuristically, for each m (say, up to $x^{1/10}$) the number of primes $x^{1/2} \le \ell \le x/\varphi(m)$ for which $p = (\ell-1)\varphi(m)+1$ is prime is likely to be of order $x/\left(\varphi(\varphi(m))\log^2 x\right)$. In particular, those primes ℓ are at least as large as $x^{1/2}$ once x is large enough. Summing over $m \le x^{1/10}$, we conclude that apparently*

$$\#\mathcal{N}(x) \gg \frac{x}{\log^2 x} \sum_{m < x^{1/10}} \frac{1}{\varphi(\varphi(m))} \tag{15}$$

(since $\ell > x^{1/2}$, each such $n = m\ell \le x$ is counted only once). By Lemma 2 of [24], we know that as t tends to infinity, the set $\mathcal{G}(t)$ of positive integers $m \le t$ such that $\varphi(m)$ is divisible by all primes $p < \log_2 t/(\log_3 t)^2$ is of cardinality $\#\mathcal{G}(t) = (1+o(1))t$. By the Mertens formula, we see that the inequality

$$\frac{1}{\varphi(\varphi(m))} = \frac{1}{\varphi(m)} \frac{\varphi(m)}{\varphi(\varphi(m))} \ge \frac{1}{\varphi(m)} \prod_{p < \log_2 t/(\log_3 t)^2} \left(1 + \frac{1}{p-1}\right) \gg \frac{\log_3 t}{m}$$

holds for all $m \in \mathcal{G}(t)$. *Putting* $z = \exp(\log^{1/2} x)$, *by partial summation, we deduce*

$$\begin{aligned}\sum_{m<x^{1/10}} \frac{1}{\varphi(\varphi(m))} &\gg \log_3 x \sum_{m\in\mathcal{G}(x^{1/10})} \frac{1}{m} \\ &= \log_3 x \left(\int_1^{x^{1/10}} \frac{1}{t} d(\#\mathcal{G}(t)) + O(1)\right) \\ &= \log_3 x \left(\int_z^{x^{1/10}} \frac{\#\mathcal{G}(t)}{t^2} dt + O(1)\right) \\ &\gg \log_3 x \log x,\end{aligned}$$

which together with (15) *suggests that the bound of Theorem 4.3 is of the correct order of magnitude. Again, a rigorous proof depends on a quantitative form of Conjecture 3.1.*

5 Euler Function and Polynomials

Theorem 5.1. *Let* $f(X) \in \mathbb{Z}[X]$ *be a polynomial with integer coefficients of degree* $d > 1$. *Then the bound*

$$\#\mathcal{N}_f(x) \ll_f x \exp\left(-(\kappa_d + o(1)) \log^{1/2} x\right)$$

holds for sufficiently large values of x, *where* $\kappa_d = \sqrt{(2 - 2/d)\log 2}$.

Proof. We let x be a sufficiently large positive real number. Let y be a real number to be chosen later.

We define the set

$$\mathcal{E}_1(x) = \{n \le x : \tau(n) \ge 2^{y/2}\}.$$

By the well known upper bound (see Theorem 5.4 of Chapter 1 of [31]):

$$\sum_{n\le x} \tau(n)^2 \ll x \log^3 x$$

we derive that

$$\#\mathcal{E}_1(x) \ll x 2^{-y} \log^3 x. \tag{16}$$

We now define the set

$$\mathcal{E}_2(x) = \{n \le x : \tau(\varphi(n)) \ge 2^y\}.$$

By a result of [25] which asserts that the estimate

$$\sum_{n<x} \tau(\varphi(n)) \ll x \exp\left(O\left(\sqrt{\frac{\log x}{\log_2 x}}\right)\right)$$

holds, we derive that

$$\#\mathcal{E}_2(x) \ll x2^{-y} \exp\left(O\left(\sqrt{\frac{\log x}{\log_2 x}}\right)\right). \tag{17}$$

We denote $\widetilde{\mathcal{N}}_f(x) = \mathcal{N}_f(x) \setminus (\mathcal{E}_1(x) \cup \mathcal{E}_2(x))$.

We now consider the set $\mathcal{M}(x)$ of positive integers m such that $|f(m)| = \varphi(n)$ for some $n \in \widetilde{\mathcal{N}}_f(x)$.

It is clear that for every $n \in \widetilde{\mathcal{N}}_f(x)$ we have

$$2^{\omega(n)} \le \tau(n) < 2^{y/2} \qquad \text{and} \qquad 2^{\omega(\varphi(n))} \le \tau(\varphi(n)) < 2^y. \tag{18}$$

Consider the prime number factorization of $n \in \widetilde{\mathcal{N}}_f(x)$ given by $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. If $|f(m)| = \varphi(n)$, then

$$|f(m)| = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1).$$

It is easy to verify that for any integer a there are at most two solutions of the equation $p^\alpha(p-1) = a$ in prime p and positive integer α. By (18), we have $k < y/2$. Therefore each representation $|f(m)| = a_1 a_2 \dots a_k$ of $|f(m)|$ as a product of k positive integers leads to at most $2^k < 2^{y/2}$ possible values of n with $|f(m)| = \varphi(n)$. As usual, we denote by $\tau_k(s)$ the number of representations of a positive integer s as a product of s integers, $s = a_1 a_2 \dots a_k$. Therefore

$$\#\widetilde{\mathcal{N}}_f(x) \le \#\mathcal{M}(x) 2^{y/2} \max\left\{\tau_k(|f(m)|) : m \in \mathcal{M}(x),\ k < y/2\right\}.$$

Since $|f(m)| \ge 0.5|m|^d$ holds for all but finitely many values of m, it follows that $\#\mathcal{M}(x) \ll_f x^{1/d}$.

Let $s = q_1^{\beta_1} \dots q_r^{\beta_r}$ be the prime number factorization of $s > 1$. Then,

$$\tau_k(s) = \prod_{j=1}^{r} \binom{\beta_j + k - 1}{k-1} \le \prod_{j=1}^{r} (\beta_j + 1)^{k-1} = \tau(s)^{k-1}.$$

Thus, if $m \in \mathcal{M}(x)$, then, from (18), we derive

$$\tau_k(|f(m)| \le \tau(|f(m)|)^{k-1} \le \tau(|f(m)|)^{y/2} \le 2^{y^2/2}.$$

Hence,

$$\#\widetilde{\mathcal{N}}_f(x) \ll_f x^{1/d} 2^{y^2/2+y/2}. \tag{19}$$

Thus, combining (16), (17) and (19), we derive

$$\#\mathcal{N}_f(x) \ll_f x2^{-y} \log^3 x + x2^{-y} \exp\left(O\left(\sqrt{\frac{\log x}{\log_2 x}}\right)\right) + x^{1/d} 2^{y^2/2+y/2}.$$

Choosing

$$y = \sqrt{\left(2 - \frac{2}{d}\right)\frac{\log x}{\log 2}} - 2,$$

we obtain

$$2^{y^2/2+y/2} \le 2^{(y+2)^2/2-y} = x^{1-1/d} 2^{-y},$$

which completes the proof. □

Remark 5.2. *We note that if $d = 1$ and $f(X) = c(aX + b)$, where $abc \neq 0$, a and b are coprime, and $|a| \ge 2$, then the inequality*

$$\#\mathcal{N}_f(x) \ll_f \frac{x}{\log^{\beta_a} x} \tag{20}$$

holds for sufficiently large values of x, with some positive constant β_a depending only on a. Indeed, taking p to be any prime factor of a, it follows that if $p^{\alpha_p} \| f(m)$, then $\alpha_p \ll 1$. In particular, if $n \le x$ is such that $\varphi(n) = f(m)$ holds for some integer m, then n has $O(1)$ prime factors q which are congruent to 1 modulo p, and the Wirsing theorem (see [33]) now easily implies that the inequality (20) *holds for sufficiently large x with $\beta_a = 1/(p-1)$.*

Remark 5.3. *It is natural to expect that the factorization structure of the polynomial f should affect $\#\mathcal{N}_f(x)$ is a rather dramatic way. For example, it is reasonable to expect that $\#\mathcal{N}_f(x)$ is much smaller for $f(X) = X^2 + 1$ than for $f(X) = X^2$.*

References

[1] W. R. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers', *Annals Math.*, **140** (1994), 703-722.

[2] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.*, **83** (1998), 331–361.

[3] W. Banks, J. B. Friedlander, C. Pomerance and I. E. Shparlinski, 'Multiplicative structure of values of the Euler Function', *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, vol.41, Amer. Math. Soc., 2004, 29–48.

[4] W. Banks, F. Luca and I. E. Shparlinski, 'Arithmetic properties of $\varphi(n)/\lambda(n)$ and the structure of the multiplicative group modulo n', *Preprint*, 2003.

[5] W. Banks and I. E. Shparlinski, 'Congruences and exponential sums with the Euler function', *Proc. Conference in Number Theory in Honour of Prof. H.C. Williams*, Banff, Alberta, 2003 (to appear).

[6] N. L. Bassily, I. Kátai and M. Wijsmuller, 'On the prime power divisors of the iterates of the Euler-φ function', *Publ. Math. Debrecen*, **55** (1999), 17–32.

[7] E. R. Canfield, P. Erdős and C. Pomerance, 'On a problem of Oppenheim concerning "Factorisatio Numerorum"', *J. Number Theory*, **17** (1983), 1–28.

[8] J. M. De Koninck, F. Luca and A. Sankaranarayanan, 'Positive integers n whose Euler function is a power of the kernel function', *Rocky Mountain J. Math.*, to appear.

[9] T. Dence and C. Pomerance, 'Euler's function in residue classes', *The Ramanujan J.*, **2** (1998), 7–20.

[10] L. E. Dickson, 'A new extension of Dirichlet's theorem on prime numbers', *Mesenger of Math.*, **33** (1904), 155–161.

[11] P. Erdős, 'On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function', *Quart. J. Math.*, **6** (1935), 205–213.

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

[13] P. Erdős and C. Pomerance, 'On the normal number of prime factors of $\varphi(n)$', *Rocky Mountain J. Math.*, **15** (1985), 343–352.

[14] P. Erdős, C. Pomerance and E. Schmutz, 'Carmichael's lambda function', *Acta Arith.*, **58** (1991), 363–385.

[15] K. Ford, 'The distribution of totients', *The Ramanujan J.*, **2** (1998), 67–151.

[16] K. Ford, 'The number of solutions of $\varphi(x) = m$', *Annals of Math.*, **150** (1999), 283–311.

[17] K. Ford, S. Konyagin and C. Pomerance, 'Residue classes free of values of Euler's function', *Proc. Number Theory in Progress*, Walter de Gruyter, Berlin, 1999, 805–812.

[18] J. B. Friedlander, 'Shifted primes without large prime factors', *Number Theory and Applications*, Kluwer, NATO ASI, (1989), pp. 393–401.

[19] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[20] G.H. Hardy and J.E. Littlewood, 'Some problems on partitio numerorum III. On the expression of a number as a sum of primes', *Acta Math.*, **44** (1923), 1–70.

[21] G. H. Hardy and E. M. Wright, *An Introduction to the theory of numbers*, Fifth Edition, The Clarendon Press, Oxford University Press, New York, 1979.

[22] D.R. Heath-Brown, 'Artin's conjecture for primitive roots', *Quart. J. Math.*, **37**, (1986), 27–38.

[23] A. Hildebrand and G. Tenenbaum, 'Integers without large prime factors', *J. de Théorie des Nombres de Bordeaux*, **5** (1993), 411–484.

[24] 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.

[25] F. Luca and C. Pomerance, 'On the average number of divisors of the Euler function', Preprint, 2003.

[26] H. Maier and C. Pomerance, 'On the number of distinct values of Euler's φ-function', *Acta Arith.*, **49** (1988), 263–275.

[27] H. Montgomery, 'Primes in arithmetic progressions', *Mich. Math. J.*, **17** (1970), 33–39.

[28] C. Pomerance, 'Popular values of Euler's function', *Mathematika*, **27** (1980), 84–89.

[29] C. Pomerance, 'Two methods in elementary analytic number theory', *Number theory and application*, R. A. Mollin, ed., Kluwer Acad. Publ., Dordrecht, 1989, 135–161.

[30] C. Pomerance and I. E. Shparlinski, 'Smooth orders and cryptographic applications', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2369** (2002), 338–348.

[31] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957.

[32] A. Schinzel and W. Sierpiński, 'Sur certaines hypothèses concernant les nombres premiers', *Acta Arith.*, **4** (1958), 185–208; Erratum, *Acta Arith.*, **5** (1959), 259.

[33] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 1995.

[34] S. Wagon, 'Carmichael's empirical theorem', *Math. Intelligencer*, **8** (1986), 61–63.