Fields Institute Communications
Volume **00**, 0000

Multiplicative Structure of Values of the Euler Function

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

John B. Friedlander
Department of Mathematics, University of Toronto
Toronto, Ontario M5S 3G3, Canada
frdlndr@math.toronto.edu

Carl Pomerance
Department of Fundamental Mathematics, Bell Laboratories
Murray Hill, NJ 07974-0636, USA
carlp@research.bell-labs.com

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

Dedicated to Hugh Williams on the occasion of his sixtieth birthday.

Abstract. We establish upper bounds for the number of smooth values of the Euler function. In particular, although the Euler function has a certain "smoothing" effect on its integer arguments, our results show that, in fact, most values produced by the Euler function are not smooth. We apply our results to study the distribution of "strong primes", which are commonly encountered in cryptography.

We also consider the problem of obtaining upper and lower bounds for the number of positive integers $n \le x$ for which the value of the Euler function $\varphi(n)$ is a perfect square and also for the number of $n \le x$ such that $\varphi(n)$ is squarefull. We give similar bounds for the Carmichael function $\lambda(n)$.

1 Introduction

Let $\varphi(n)$ be the *Euler function*, defined as usual by

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{p^\nu \,\|\, n} p^{\nu-1}(p-1), \qquad n \ge 1.$$

2000 *Mathematics Subject Classification.* Primary 11N60, 11N64; Secondary 11N25.

Let $P(n)$ denote the largest prime factor of the integer $n > 1$, and let $P(1) = 1$. In this paper, we consider the problem of estimating the number $\Phi(x, y)$ of integers $n \le x$ for which the value $\varphi(n)$ is y-smooth. Recall that an integer k is said to be *y-smooth* if $P(k) \le y$. We also consider the related problem of bounding the number $S_\varphi(x)$ of integers $n \le x$ such that $\varphi(n)$ is a perfect square. Our bounds for $\Phi(x, y)$ and $S_\varphi(x)$ are closely linked with the set $\mathcal{P}_y$ of prime numbers p such that $p - 1$ is y-smooth.

We first show that the Rankin method yields a nontrivial bound for $\Phi(x, y)$ for a very wide range in the xy-plane. In particular, we show that $\Phi(x, y) = o(x)$ if $u = (\log x)/(\log y) \to \infty$. We remark that, despite a large variety of results on the arithmetical properties of $\varphi(n)$ (for instance, see [8, 11, 12, 13, 22]), and a large variety of results on smooth numbers (for instance, see the surveys [16, 19]), it seems the function $\Phi(x, y)$ has not been previously studied in the literature.

We also show that our upper bound for $\Phi(x, y)$ can be applied to the study of *strong primes*, which are commonly encountered in cryptographic applications (for example, in the selection of safe RSA moduli); see [24]. Recall that a prime p is said to be *strong* if both $p-1$ and $p+1$ have a large prime divisor, and if $p-1$ has a prime divisor r such that $r-1$ has a large prime divisor. A significant part in the development of these ideas has been played by Hugh Williams; see for example [30].

Using similar methods we also improve an upper bound from [27] on the number of odd integers $n \le x$ for which the multiplicative order $l(n)$ of 2 modulo n is y-smooth.

A well-known problem in prime number theory concerns the question of the distribution of prime numbers among the values of quadratic and higher degree polynomials (in one variable and with integer coefficients). Even the existence of infinitely many such primes has not yet been decided in any particular instance, apart from those polynomials for which this existence can be ruled out for trivial reasons. Doubtless, the most famous single case is the problem of proving that there are infinitely many primes of the form $m^2 + 1$.

There have been a number of partial steps in the direction of this result, for the most part as a consequence of sieve methods. One knows, thanks to Brun, that the number of integers $m^2 + 1 \le x$ that are prime is $O(x^{1/2}/\log x)$, which provides an upper bound of the same order of magnitude as would be expected on heuristic grounds. Brun's method also allows one to show that there are at least $cx^{1/2}/\log x$ such integers having no more than k prime factors, for some fixed positive constants c and k. Following a number of weaker statements of this type, Iwaniec [21] established this result with $k = 2$.

For the special polynomial $m^2 + 1$ another way to phrase the same question is to ask whether there are infinitely many primes p such that $\varphi(p) = p - 1$ is a perfect square. Considering the problem from this point of view it is natural to ask: Is it even true that there are infinitely many *integers* n such that $\varphi(n)$ is a perfect square? Of course, a positive answer is immediate if one looks at odd powers of 2: $\varphi\left(2^{2k+1}\right) = 2^{2k}$. More generally, if n is a product of odd powers of primes of the form $p = m^2 + 1$, then $\varphi(n)$ is a perfect square. However, it is less clear how quickly the function $S_\varphi(x)$ grows as $x \to \infty$. Moreover, these examples still leave open the perhaps more basic question of whether there are infinitely many *squarefree* n for which $\varphi(n)$ is a perfect square. We show below that this is indeed the case. Concerning the growth rate of $S_\varphi(x)$ our results show that the number of integers $n \le x$ for which $\varphi(n)$ is square is asymptotically much greater than the total number of perfect squares less than x; it appears that many square numbers are "popular" values for the Euler function. Of course, we do not claim that our results will help to deal with the original problem of finding primes of the form $p = m^2 + 1$.

Our methods for bounding $S_\varphi(x)$ are sufficiently flexible that we can also establish bounds for some closely related functions, for example replacing $\varphi(n)$ by arithmetical functions such as the Carmichael function $\lambda(n)$ or the sum-of-divisors function $\sigma(n)$. We introduce the following general notation: Given an integer-valued function $\xi(n)$ defined on the natural numbers, denote by

- $S_\xi(x)$ the number of integers $n \le x$ for which $\xi(n)$ is a perfect square;
- $F_\xi(x)$ the number of integers $n \le x$ for which $\xi(n)$ is *squarefull*, that is, if p is any prime divisor of $\xi(n)$ then $p^2 \mid f(n)$;
- $M_\xi(x)$ the maximum number of times any single square m^2 occurs as $\xi(n)$ as n runs over the integers $n \le x$;
- $V_\xi(x)$ the number of distinct squares m^2 occurring as $\xi(n)$ for some integer $n \le x$.

Accordingly, we denote by $S^*_\xi(x)$, $M^*_\xi(x)$, $V^*_\xi(x)$ and $F^*_\xi(x)$ the same quantities but restricted to *squarefree* positive integers $n \le x$. Note that one always has the trivial relation

$$\max\{M_\xi(x), V_\xi(x)\} \le S_\xi(x) \le F_\xi(x),$$

and the analogous relation holds for $S^*_\xi(x)$, $M^*_\xi(x)$, $V^*_\xi(x)$ and $F^*_\xi(x)$.

In this paper, we give lower bounds for $S_\varphi(x)$, $M_\varphi(x)$ and $V_\varphi(x)$, as well as an upper bound for $F_\varphi(x)$. Assuming a weak (and widely believed) form of the Elliott-Halberstam conjecture, our unconditional lower bounds for $S_\varphi(x)$ and $M_\varphi(x)$ can be greatly improved, and both bounds then take the form $x^{1+o(1)}$.

By a somewhat different proof, we obtain analogous results for $S^*_\varphi(x)$ and $M^*_\varphi(x)$. However, we have been unable to say anything interesting about $V^*_\varphi(x)$.

As is frequently the case with the arithmetical functions $\varphi(n)$ and $\sigma(n)$, similar methods can be applied to the study of both. Thus, although we have not done so explicitly here, one can easily obtain analogues of our lower bound for $S^*_\varphi(x)$ and our upper bound for $F_\varphi(x)$ for the functions $S^*_\sigma(x)$ and $F_\sigma(x)$, respectively.

For the Carmichael function such an extension requires a slightly different version of the argument. Recall that the *Carmichael function* $\lambda(n)$, is defined for $n \ge 1$ as the largest order occurring amongst the elements in $(\mathbb{Z}/n\mathbb{Z})^\times$. More explicitly, for a prime power p^ν, we have

$$\lambda(p^\nu) = \begin{cases} p^{\nu-1}(p-1) & \text{if } p \ge 3 \text{ or } \nu \le 2, \\ 2^{\nu-2} & \text{if } p = 2 \text{ and } \nu \ge 3, \end{cases}$$

and for arbitrary $n \ge 2$,

$$\lambda(n) = \operatorname{lcm}\left(\lambda\left(p_1^{\nu_1}\right), \ldots, \lambda\left(p_k^{\nu_k}\right)\right),$$

where $n = p_1^{\nu_1} \ldots p_k^{\nu_k}$ is the prime factorization of n; one also has $\lambda(1) = 1$.

We remark that $S_\lambda(x) \le F_\lambda(x) \le F_\varphi(x)$ since $\lambda(n) \mid \varphi(n)$, hence our upper bound for $F_\varphi(x)$ also applies to $F_\lambda(x)$. In fact, we do not currently know any better bound for $F_\lambda(x)$. Our lower bound for $S_\varphi(x)$ does not immediately imply anything about $S_\lambda(x)$, but we show that a small modification of the technique can be applied to $S_\lambda(x)$ as well, providing the same nontrivial lower bound for this function.

We also pose several open questions and discuss some heuristic estimates. In particular, under a certain very plausible conjecture about the proportion of smooth values occurring among shifts of prime numbers, we show that the proportion of smooth values of the Euler function is close to our upper bound for $\Phi(x, y)$. Such heuristics imply that the proportion of integers n such that $\varphi(n)$ is smooth is exponentially higher than the proportion of smooth integers as $u = (\log x)/(\log y) \to \infty$.

Acknowledgements. The authors would like to thank Andrew Granville for pointing out the relevance of [14] to our work. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628 and by Macquarie University (Sydney), J. F. was supported in part by NSERC grant A5123 and by a Killam Research Fellowship, and I. S. was supported in part by ARC grant DP0211459.

2 Smooth Values of Shifted Primes

We denote as usual by $\psi(x, y)$ the number of positive integers $n \le x$ which are y-smooth, that is

$$\psi(x, y) = \#\{1 \le n \le x \,|\, P(n) \le y\}.$$

Thanks to the work of Dickman [9], de Bruijn [5], and others, it is known that in a very wide range of the xy-plane, $\psi(x, y) \sim \rho(u)x$, where $u = (\log x)/(\log y)$ and $\rho(u)$ is the *Dickman–de Bruijn* function. The latter is defined by

$$\rho(u) \ = \ 1, \qquad 0 \le u \le 1,$$

and

$$\rho(u) \ = \ 1 - \int_1^u \frac{\rho(v-1)}{v}\, dv, \qquad u > 1.$$

Moreover, $\rho(u) = u^{-u+o(u)}$ as $u \to \infty$.

Let $\pi(x)$ denote as usual the number of primes $p \le x$, and let $\pi(x, y)$ denote the number of primes p such that $p \le x$ and $p - 1$ is y-smooth. Since the numbers $p - 1$ with p prime are likely to behave as “random” integers, it seems reasonable to expect that behaviour of $\pi(x, y)$ can be deduced from that of $\psi(x, y)$. That is, it seems very plausible to conjecture that the asymptotic relation

$$\pi(x, y)/\pi(x) \sim \psi(x, y)/x \tag{2.1}$$

holds in a very wide range, conceivably as wide as $x \ge y$ and $y \to \infty$; see [1, 2, 15, 16, 23, 25, 27]. This would of course then imply $\pi(x, y) \sim \rho(u)\pi(x)$ also holds in a somewhat narrower range.

It has been remarked in Section 5.c of [16] that, for any fixed $u > 1$, the relation (2.1) follows under the assumption of a weak and widely believed form of the Elliott–Halberstam conjecture [18]. However, presently there is no feasible approach to an unconditional proof of (2.1). On the other hand, upper and lower bounds for $\pi(x, y)$ have been proved unconditionally in a number of papers; see [1, 2, 3, 15, 27] and the references contained therein. In particular, it has been shown in [2] that

$$\pi(x, y) \gg \frac{x}{\log^2 x} \qquad \text{for } u \le 3.3772. \tag{2.2}$$

For many applications such bounds are as useful as the asymptotic formula (2.1).

As for upper bounds, by Theorem 1 of [27], for $\exp\left(\sqrt{\log x \log\log x}\right) \le y \le x$, we have

$$\pi(x, y) \ll u\rho(u)\pi(x), \tag{2.3}$$

where $u = (\log x)/(\log y)$. In the shorter range $\exp\bigl((\log x)^{2/3+\varepsilon}\bigr) \le y \le x$, the slightly stronger estimate

$$\pi(x,y) \ll \rho(u)\pi(x)$$

follows from Theorem 4 of [14] in much the same way as the lower bound in Corollary 3 of [14]; converting the lower bound to an upper bound (and working with $n-1$ instead of $n+1$) requires only trivial modifications. In view of the conjectured formula (2.1) we expect that this last bound reflects the truth.

Let $L(x,y)$ count the number of odd primes $p \le x$ such that $l(p)$ is y-smooth, where $l(n)$ denotes the multiplicative order of 2 modulo n. Theorem 3 of [27] provides the following bound (with an additional term $\log 2u$ in the denominator, which we ignore):

Lemma 2.1 *For* $\exp\bigl(\sqrt{\log x \log\log x}\,\bigr) \le y \le x$, *we have*

$$L(x,y) \ll u\rho(u/2)\pi(x),$$

where $u = (\log x)/(\log y)$.

Let $f(X) \in \mathbb{Z}[X]$ be a polynomial with integer coefficients. Let us denote by $\psi_f(x,y)$ the number of positive integers $n \le x$ for which $f(n)$ is both positive and y-smooth. We also denote by $\pi_f(x,y)$ the number of primes $p \le x$ for which $f(p)$ is both positive and y-smooth. Thus we have $\pi(x,y) = \pi_{f_0}(x,y)$ for $f_0(X) = X - 1$.

We need the following bounds of [20].

Lemma 2.2 *For any fixed, non-constant polynomial* $f(X) \in \mathbb{Z}[X]$ *and* $\log x \le y \le x$, *we have*

$$\psi_f(x,y) \le x\exp(-(1+o(1))u\log u),$$

when $u = (\log x)/(\log y) \to \infty$.

Lemma 2.3 *For any fixed, non-constant polynomial* $f(X) \in \mathbb{Z}[X]$ *and* $\log x \le y \le x$, *we have*

$$\pi_f(x,y) \le \pi(x)\exp(-(1+o(1))u\log u),$$

when $u = (\log x)/(\log y) \to \infty$.

We remark that the bounds of Lemma 2.2 and 2.3 are not likely to be tight. For example, for an irreducible polynomial f of degree d it is natural to expect $\rho(du) = \exp(-(1+o(1))du\log u)$ instead of $\exp(-(1+o(1))u\log u)$ in these inequalities. In fact some of the results of [20] have been slightly sharpened in [29] but they do not improve our estimates.

We also need the Brun-Titchmarsh theorem, for example see Theorem 3.7 in Chapter 3 of [18]. Let $\pi(x;k,a)$ denote the number of primes $p \le x$ such that $p \equiv a \pmod{k}$.

Lemma 2.4 *For integers* $k \ge 1$ *and* a *and for all* $x > k$, *the bound*

$$\pi(x;k,a) \ll \frac{x}{\varphi(k)\bigl(2+\log(x/k)\bigr)}$$

holds, where the implied constant is absolute.

Finally, for an integer $m \ge 1$ and any integer-valued function $\xi(n)$, let $T_\xi(m,x)$ denote the number of positive $n \le x$ such that $\xi(n) \equiv 0 \pmod{m}$. Let $\Omega(m)$ denote as usual the total number of prime divisors of m counted with their multiplicities.

It has been shown in [4] that there is a constant C_D depending only on D such that, for every integer m for which $\Omega(m) \le D$, we have

$$T_\varphi(m,x) \le C_D \frac{x(\log\log x)^D}{m}. \tag{2.4}$$

3 Smooth Values of the Euler Function

We are now ready to present our bound for $\Phi(x,y)$; we use Rankin's method in a way similar to its application in [26].

Theorem 3.1 *For any fixed $\varepsilon > 0$ and $(\log\log x)^{1+\varepsilon} \le y \le x$, we have*

$$\Phi(x,y) \le x\exp(-(1+o(1))\,u\log\log u)$$

when $u = (\log x)/(\log y) \to \infty$.

Proof Let $\mathcal{P}_y$ be the set of primes p such that $P(p-1) \le y$, and let $\mathcal{S}_y$ be the set of integers $s \ge 2$ with $P(s) \le y$. For any $c > 0$, we have

$$\begin{aligned}\Phi(x,y) &\le x^c \sum_{\substack{n\le x\\ P(\varphi(n))\le y}} n^{-c} \le x^c \sum_{\substack{n\le x\\ p\,\mid\, n \,\Rightarrow\, p\in\mathcal{P}_y}} n^{-c} \le x^c \sum_{\substack{n=1\\ p\,\mid\, n \,\Rightarrow\, p\in\mathcal{P}_y}}^{\infty} n^{-c}\\ &= x^c \prod_{p\in\mathcal{P}_y} \left(1-p^{-c}\right)^{-1} \le x^c \prod_{s\in\mathcal{S}_y} \left(1-s^{-c}\right)^{-1}.\end{aligned}$$

We now choose

$$c = 1 - \frac{\log\log u}{\log y} = 1 - \frac{u\log\log u}{\log x}.$$

Under the conditions of the theorem we have

$$c = 1 - \frac{\log\log u}{\log y} \ge 1 - \frac{\log\log\log x}{\log y} \ge 1 - \frac{1}{1+\varepsilon} = \frac{\varepsilon}{1+\varepsilon};$$

hence

$$\log\Bigl(\prod_{s\in\mathcal{S}_y}\left(1-s^{-c}\right)^{-1}\Bigr) = \sum_{s\in\mathcal{S}_y}\sum_{k=1}^{\infty}\frac{1}{ks^{kc}} \ll \sum_{s\in\mathcal{S}_y} s^{-c}.$$

Furthermore, we similarly have

$$\sum_{s\in\mathcal{S}_y} s^{-c} = \prod_{p\le y}\left(1-p^{-c}\right)^{-1} \le \exp\Bigl(O\bigl(\sum_{p\le y} p^{-c}\bigr)\Bigr).$$

Letting $r = \lfloor \log y \rfloor$, we have the estimate

$$\begin{aligned}\sum_{p\le y} p^{-c} &= \sum_{k=1}^{r}\sum_{e^k\le p<e^{k+1}} p^{-c} \le \sum_{k=1}^{r} e^{-ck}\pi\left(e^{k+1}\right) \ll \sum_{k=1}^{r} k^{-1}e^{(1-c)k}\\ &\ll \frac{e^{(1-c)r}}{(1-c)r} \ll \frac{y^{(1-c)}}{(1-c)\log y} = \frac{\log u}{\log\log u}.\end{aligned}$$

Thus,

$$\sum_{s\in\mathcal{S}_y} s^{-c} \le u^{O(1/\log\log u)}.$$

Therefore, remarking that $x^c = x\exp\left(-u\log\log u\right)$ we derive the bound

$$\Phi(x,y) \le x\exp\left(-u\log\log u + u^{O(1/\log\log u)}\right),$$

which completes the proof. □

4 Strong Primes and Smooth Values of the Euler Function over Sparse Sequences

We now consider smooth values of the Euler function taken at polynomial values or shifed primes (or combinations of both). Namely, for a given polynomial $f(X) \in \mathbb{Z}[X]$ we denote by $\Phi_f(x, y)$ the number of integers $n \le x$ for which $f(n)$ is positive and $\varphi(f(n))$ is y-smooth.

Theorem 4.1 *For any fixed, non-constant polynomial $f \in \mathbb{Z}[X]$ and $\log x \le y \le x$, we have*

$$\Phi_f(x, y) \le \exp\left(-(\tfrac{1}{2} + o(1))u^{1/2} \log u\right) x,$$

when $u = (\log x)/(\log y) \to \infty$.

Proof Suppose the degree of f is d. Without loss of generality, we may assume that the greatest common divisor of the coefficients of f is 1. As before, let $\mathcal{P}_y$ be the set of primes p such that $p - 1$ is y-smooth. Let $w = u^{1/2}$ and $z = x^{1/w}$. Then $z = y^{u/w} = y^w$. If $n \le x$ and $\varphi(f(n))$ is y-smooth, then either $f(n)$ is z-smooth or it has a prime divisor $p \ge z$ with $p \in \mathcal{P}_y$. Therefore, we have

$$\begin{aligned} \Phi_f(x, y) &\le \psi_f(x, z) + \sum_{\substack{z < p \le x \\ p \in \mathcal{P}_y}} \sum_{\substack{n \le x \\ f(n) \equiv 0 \pmod p}} 1 \\ &\le \psi_f(x, z) + d \sum_{\substack{z < p \le x \\ p \in \mathcal{P}_y}} \left(\frac{x}{p} + 1\right) \le \psi_f(x, z) + 2dx \sum_{\substack{z < p \le x \\ p \in \mathcal{P}_y}} \frac{1}{p}. \end{aligned}$$

We obviously have $z = \exp(\sqrt{\log x \log y}) \ge \log x$, thus by Lemma 2.2 we see that

$$\psi_f(x, z) \le x \exp\left(-(1 - \varepsilon) w \log w\right)$$

for any fixed $\varepsilon > 0$ and u sufficiently large.

By partial summation we have

$$\sum_{\substack{z < p \le x \\ p \in \mathcal{P}_y}} \frac{1}{p} = \frac{\pi(x, y)}{x} - \frac{\pi(z, y)}{z} + \int_z^x \frac{\pi(t, y)}{t^2}\, dt.$$

Using Lemma 2.3, an elementary calculation shows that

$$\sum_{\substack{z < p \le x \\ p \in \mathcal{P}_y}} \frac{1}{p} \le \exp(-(1 - \varepsilon) w \log w)$$

for any fixed $\varepsilon > 0$ and all sufficiently large values of u. Since $w \log w = \frac{1}{2} u^{1/2} \log u$, the proof is complete. □

Accordingly, we denote by $\Pi_f(x, y)$ the number of primes $p \le x$ for which $f(p)$ is positive and $\varphi(f(p))$ is y-smooth.

Theorem 4.2 *For any fixed, non-constant polynomial $f \in \mathbb{Z}[X]$ and $\log x \le y \le x$, we have*

$$\Pi_f(x, y) \le \frac{\pi(x)}{\exp((\frac{1}{2} + o(1))u^{1/2} \log u)} + \frac{\pi(x) \log\log x}{\exp((1 + o(1))u \log u)}$$

when $u = (\log x)/(\log y) \to \infty$.

Proof As before, we denote by $\mathcal{P}_y$ the set of primes p such that $p-1$ is y-smooth. Let $w = u^{1/2}$ and $z = x^{1/w}$. Then $z = y^{u/w} = y^w$. If a prime $p \le x$ is such that $\varphi(f(p))$ is y-smooth, then either $f(p)$ is z-smooth or $f(p)$ has a prime divisor $r \ge z$ with $r \in \mathcal{P}_y$.

Therefore, by Lemma 2.4 we have

$$\Pi_f(x,y) \;\le\; \pi_f(x,z) + \sum_{\substack{z<r\le x\\ r\in\mathcal{P}_y}} \sum_{\substack{p\le x\\ f(p)\equiv 0 \pmod r}} 1 \;\ll\; \pi_f(x,z) + x \sum_{\substack{z<r\le x\\ r\in\mathcal{P}_y}} \frac{1}{r\log(e^2x/r)}.$$

By partial summation and Lemma 2.3 we see that

$$\begin{aligned}
\sum_{\substack{z<r\le x/z\\ r\in\mathcal{P}_y}} \frac{1}{r\log(e^2x/r)} &\le \exp(-(1+o(1))w\log w) \sum_{\substack{z<r\le x/z\\ r \text{ prime}}} \frac{1}{r\log(e^2x/r)},\\
\sum_{\substack{x/z<r\le x\\ r\in\mathcal{P}_y}} \frac{1}{r\log(e^2x/r)} &\le \exp(-(1+o(1))u\log u) \sum_{\substack{x/z<r\le x\\ r \text{ prime}}} \frac{1}{r\log(e^2x/r)}.
\end{aligned}$$

An elementary calculation shows that

$$\begin{aligned}
\sum_{\substack{z<r\le x/z\\ r \text{ prime}}} \frac{1}{r\log(e^2x/r)} &= \frac{(2+o(1))\log w}{\log x}\\
\sum_{\substack{x/z<r\le x\\ r \text{ prime}}} \frac{1}{r\log(e^2x/r)} &= \frac{(1+o(1))\log\log x}{\log x},
\end{aligned}$$

so that, using Lemma 2.3 also for the term $\pi_f(x,z)$, the theorem follows. □

Let $\Pi(x,y)$ be the number of primes $p \le x$ such that $\varphi(p-1)$ is y-smooth. Thus $\Pi(x,y) = \Pi_{f_0}(x,y)$ for $f_0(X) = X-1$. Therefore Theorem 4.2 applies to $\Pi(x,y)$ as well. Below, we obtain another bound which is stronger for small values of u. In particular it implies that $\Pi(x,y) = o(\pi(x))$ if $u \to \infty$ which means that almost all primes are “strong”.

Recall that a prime p is said to be *y-strong* if neither $p-1$ nor $p+1$ is y-smooth and if $p-1$ has a prime divisor q such that $q-1$ is not y-smooth. Theorem 3.1 implies that the number of primes $p \le x$ which are not y-strong is at most $\pi(x)\exp\left(-(1+o(1))u\log\log u\right)$ provided that

$$(\log\log x)^{1+\varepsilon} \le y \le \exp\left(\frac{\log x(\log\log\log\log x)^{1-\varepsilon}}{\log\log x}\right)$$

since in this range $\log x = \exp\left(o\left(u\log\log u\right)\right)$. To see this, note that if a prime p is not y-strong, then either $p+1$ is y-smooth, or $p-1$ has a prime divisor $r \ge y$ such that $r^2 \,|\, p-1$, or $\varphi(p-1)$ is y-smooth. For primes of the first type we can use the analogue of bounds on $\pi(x,y)$ mentioned in Section 2, the number of primes of the second type is $O(x/y)$, and for the primes of the third type Theorem 3.1 applies.

For smaller values of u the exceptional set given by Theorem 3.1 is not as small as $\pi(x)\exp\left(-(1+o(1))u\log\log u\right)$ and Theorem 4.2 provides a better bound, but it still does not imply that $\Pi(x,y) = o(\pi(x))$ as soon as $u \to \infty$. This however follows from our next result.

Theorem 4.3 *For* $\exp\left(\sqrt{\log x \log\log x}\,\right) \le y \le x$ *we have*

$$\Pi(x,y) \ll u^{-1}\pi(x).$$

Proof As before, denote by $\mathcal{P}_y$ the set of primes p such that $p-1$ is y-smooth. Using the bound (2.3), via partial summation we derive that

$$\begin{aligned}\sum_{\substack{x\ge r>y\\ r\in P_y}} \frac{1}{r} &= \frac{1}{x}\left(\pi(x,y)-\pi(y)\right) + \int_y^x \frac{1}{t^2}\left(\pi(t,y)-\pi(y)\right)\,dt\\ &\ll \int_y^x \frac{1}{t\log y}\rho\left(\frac{\log t}{\log y}\right)\,dt = \int_1^u \rho(s)\,ds \ll 1.\end{aligned}$$

Therefore,

$$\sum_{\substack{x^{1/5}\ge r>y\\ r\notin P_y,\ r \text{ prime}}} \frac{1}{r} = \log\log(x^{1/5}) - \log\log y + O(1) = \log u + O(1)$$

and so

$$\prod_{\substack{x^{1/5}\ge r>y\\ r\notin P_y,\ r \text{ prime}}} \left(1-\frac{1}{r-1}\right) \ll u^{-1}.$$

We apply the upper bound sieve (for example, Theorem 4.1 of [18] or Theorem 1, page 91 of [17]) to remove the primes $p \le x$ with $p \equiv 1 \pmod r$ for some prime $r \in (y, x^{1/5}]$ with $r \notin \mathcal{P}_y$. Using the last-mentioned bound to estimate the main term and the Bombieri–Vinogradov theorem to bound the remainder term, we complete the proof of the theorem. □

5 Smooth Values of the Multiplicative Order

Let $N(x,y)$ denote the number of odd integers $n \le x$ such that $l(n)$ is y-smooth, where, as before, $l(n)$ denotes the multiplicative order of 2 modulo n. Theorem 4 of [27] asserts that for $\exp\left(\sqrt{\log x \log\log x}\,\right) \le y \le x$, the bound

$$N(x,y) \ll x/u$$

holds, where $u = (\log x)/(\log y)$. Here we obtain a significantly sharper estimate.

Theorem 5.1 *For* $\exp\left(\sqrt{\log x \log\log x}\,\right) \le y \le x$ *we have*

$$N(x,y) \le x\exp(-(\tfrac{1}{2}+o(1))\,u\log\log u)$$

when $u = (\log x)/(\log y) \to \infty$*.*

Proof Let $\mathcal{L}_y$ be the set of odd primes p such that $l(p)$ is y-smooth. Since $l(p) \,\big|\, l(n)$ for any prime $p \,\big|\, n$ we have for any $c > 0$:

$$N(x,y) \le x^c \sum_{\substack{n\le x\\ P(l(n))\le y}} n^{-c} \le x^c \sum_{\substack{n\le x\\ p\,|\,n \Rightarrow p\in\mathcal{L}_y}} n^{-c} \le x^c \prod_{\substack{p\le x\\ p\in\mathcal{L}_y}} \left(1-p^{-c}\right)^{-1}.$$

We choose

$$c = 1 - \frac{\log\log u}{2\log y} = 1 - \frac{u\log\log u}{2\log x}.$$

Under the conditions of the theorem, we have

$$u = \frac{\log x}{\log y} \le \sqrt{\frac{\log x}{\log\log x}}, \qquad u \log\log u \le \sqrt{\log x \, \log\log x},$$

and therefore

$$1 \ge c \ge 1 - \frac{1}{2}\sqrt{\frac{\log\log x}{\log x}} \ge \frac{1}{2}.$$

We shall need the estimate

$$\log\Bigg(\prod_{\substack{p\le x\\ p\in\mathcal{L}_y}} \left(1-p^{-c}\right)^{-1}\Bigg) = \sum_{\substack{p\le x\\ p\in\mathcal{L}_y}} \sum_{k=1}^{\infty} \frac{1}{kp^{kc}} \ll \sum_{\substack{p\le x\\ p\in\mathcal{L}_y}} p^{-c}.$$

By Abel's summation formula,

$$\begin{aligned}\sum_{\substack{p\le x\\ p\in\mathcal{L}_y}} p^{-c} &= \sum_{p\le y} p^{-c} + \sum_{\substack{y<p\le x\\ p\in\mathcal{L}_y}} p^{-c}\\ &= \frac{L(x,y)}{x^c} + c\int_2^y \frac{\pi(t)}{t^{c+1}}\,dt + c\int_y^x \frac{L(t,y)}{t^{c+1}}\,dt\end{aligned}$$

where we recall that $L(x,y)$ is defined as the number of odd primes $p \le x$ such that $l(p)$ is y-smooth. In the above we shall employ the bound

$$\int_2^y \frac{\pi(t)}{t^{c+1}}\,dt \ll \int_2^y \frac{1}{t^c \log t}\,dt \ll \frac{y^{1-c}}{1-c} \ll (\log u)^{1/2}.$$

Also, by Lemma 2.1,

$$\frac{L(x,y)}{x^c} \ll \frac{u\rho(u/2)\pi(x)}{x^c} \ll \frac{u\rho(u/2)x^{1-c}}{\log x}.$$

The estimate

$$\rho(v) = \exp\left(-v\log(v\log v) + v + o(v)\right), \qquad v \to \infty, \tag{5.1}$$

follows, for example, from Theorem 8 in Chapter III.5 of [28]; see also Section 3.i of [16]. Since

$$x^{1-c} = \exp\left(\tfrac{1}{2}u\log\log u\right),$$

it follows that

$$L(x,y) = o(x^c).$$

Finally, we have by Lemma 2.1,

$$\begin{aligned}\int_y^x \frac{L(t,y)}{t^{c+1}}\,dt &\ll \int_y^x \frac{\pi(t)\log t}{t^{c+1}\log y}\,\rho\left(\frac{\log t}{2\log y}\right)dt\\ &\ll \int_y^x t^{1-c}\,\rho\left(\frac{\log t}{2\log y}\right)\frac{dt}{2t\log y}\\ &= \int_{1/2}^{u/2} y^{2v(1-c)}\rho(v)\,dv\\ &= \int_{1/2}^{u/2} \exp(v\log\log u)\,\rho(v)\,dv.\end{aligned}$$

Now put $w = (\log u)/(\log\log u)$. We split the last integral into three pieces and estimate each piece separately. For v in the range $1/2 \le v \le w/3$ we find

$$\exp(v\log\log u)\,\rho(v) \le \exp\left(\tfrac{1}{3}\log u\right) = u^{1/3};$$

thus

$$\int_{1/2}^{w/3} \exp(v\log\log u)\,\rho(v)\,dv \le u^{1/3}w = \frac{u^{1/3}\log u}{\log\log u}.$$

For v in the range $w/3 \le v \le 3w$ we have

$$v\log v \ge \frac{w\log w}{3} = \frac{\log u}{3\log\log u}\left(\log\log u - \log\log\log u\right) \ge \frac{\log u}{4},$$

provided that u is sufficiently large. Hence, using (5.1), it follows that

$$\exp(v\log\log u)\,\rho(v) = \exp\left(O(w)\right).$$

Thus,

$$\int_{w/3}^{3w} \exp(v\log\log u)\,\rho(v)\,dv = w\exp\left(O(w)\right) = u^{O(1/\log\log u)}.$$

For v in the range $3w \le v \le u/2$, there holds

$$v\log v \ge 3w\log w = \frac{3\log u}{\log\log u}\left(\log\log u - \log\log\log u\right) \ge 2.9\log u$$

if u is sufficiently large. Hence, $\log(v\log v) > \log\log u + 1.064$, so that using (5.1), it follows that

$$\exp(v\log\log u)\,\rho(v) \le \exp\left(-0.06v\right)$$

for u sufficiently large. Consequently,

$$\int_{3w}^{u/2} \exp(v\log\log u)\,\rho(v)\,dv = O(1).$$

Therefore, remarking that $x^c = x\exp\left(-\tfrac{1}{2}u\log\log u\right)$, we derive that

$$N(x,y) \le x\exp\left(-\tfrac{1}{2}u\log\log u + u^{O(1/\log\log u)}\right),$$

which completes the proof. □

We remark that, as in [27], Theorem 5.1 has only been formulated for the multiplicative order $l(n)$ of 2, but the result clearly holds for the order of any fixed base $g \ge 2$.

6 Construction of Square Values of the Euler and Carmichael Functions

In this section we obtain lower bounds for $S_\varphi(x)$ and $S_\lambda(x)$ and for some related functions.

Theorem 6.1 *Let $v > 1$ be any fixed real number. Suppose there exist positive constants A and C such that for all sufficiently large z and $y = z^{1/v}$, one has*

$$\pi(z,y) \ge C\,\frac{z}{\log^A z}. \tag{6.1}$$

Then the following bound holds: as $x \to \infty$,

$$S_\varphi(x) \ge x^{1-1/v+o(1)}.$$

Proof Let us define y by the equation

$$y \log(8y^v) = \log x$$

and put $z = y^v$; then $(8z)^y = x$. We define the set

$$\mathcal{P}_{z,y} = \{y < p \le z \mid p \text{ is prime and } p - 1 \text{ is } y\text{-smooth}\};$$

then if x is sufficiently large,

$$\#\mathcal{P}_{z,y} = \pi(z,y) - \pi(y) \ge C\, \frac{z}{\log^A z} - \frac{2y}{\log y} = z^{1+o(1)}.$$

We also put

$$Q_y = \prod_{p \le y} p.$$

Let $k = \lfloor y \rfloor$, and for each subset $\mathcal{R} \subseteq \mathcal{P}_{z,y}$ of cardinality $\#\mathcal{R} = k$, consider the integer

$$m_{\mathcal{R}} = Q_y \prod_{p \in \mathcal{R}} p.$$

It is clear that for any $d \,|\, Q_y$ we have $\varphi\,(dm_{\mathcal{R}}) = d\varphi\,(m_{\mathcal{R}})$. It is also clear that $\varphi\,(m_{\mathcal{R}})$ is y-smooth. Therefore there is a unique divisor $d_{\mathcal{R}}$ of Q_y such that $\varphi(d_{\mathcal{R}} m_{\mathcal{R}})$ is a square; put $n_{\mathcal{R}} = d_{\mathcal{R}} m_{\mathcal{R}}$. Because of our choice of parameters we have

$$n_{\mathcal{R}} \le Q_y^2 z^k \le z^y \exp((2 + o(1))y) \le (8z)^y = x$$

provided that x is large enough. Since the integers $n_{\mathcal{R}}$ are pairwise distinct for different sets $\mathcal{R}$, and since $k = y(1 + o(1))$ and $z^y = x^{1+o(1)}$, we derive that

$$S_\varphi(x) \ge \binom{\#\mathcal{P}_{z,y}}{k} \ge \left(\frac{\#\mathcal{P}_{z,y}}{k}\right)^k = \left(z^{1-1/v+o(1)}\right)^k = x^{1-1/v+o(1)}.$$

This completes the proof. □

The use of (2.2) in Theorem 6.1 yields the unconditional bound

$$S_\varphi(x) \gg x^{0.7038}. \tag{6.2}$$

As we have already mentioned, one expects that the condition (6.1) assumed in Theorem 6.1 should hold for any fixed $v > 1$ with appropriate positive constants $A = A(v)$ and $C = C(v)$ (presumably, with $A(v) = 1$ and $C(v) = v^{-v+o(v)}$ as $v \to \infty$). If true, one immediately obtains a lower bound of the form

$$S_\varphi(x) \ge x^{1+o(1)}. \tag{6.3}$$

Depending on the assumed range of admissible values of v, one can obtain various explicit expressions for the term $o(1)$ occurring in the exponent.

Although Theorem 6.1 gives no indication as to how many integers m^2 occur as values of $\varphi(n)$ with $n \le x$ nor as to how often an individual integer m^2 can be repeated, small modifications of the above proof do provide such results. Of course, our upper bound for $F_\varphi(x)$ in the next section serves as an upper bound for $M_\varphi(x)$ and $V_\varphi(x)$ as well. Lower bounds are provided by the following:

Theorem 6.2 *Under the same assumptions as in Theorem 6.1, we have the bounds*

$$M_\varphi(x) \ge x^{1-1/v+o(1)} \qquad \textit{and} \qquad V_\varphi(x) \ge x^{1/3-1/3v+o(1)}.$$

Proof To prove the lower bound for $M_\varphi(x)$ we simply note that the perfect squares m^2 constructed in the proof of Theorem 6.1 which occur as values of $\varphi(n)$ with $n \le x$, satisfy the bound $m^2 \le x$, and every m^2 is y-smooth. Since, by our choice of parameters, we have $y = o(\log x)$, it follows that the number of such squares is at most $\psi(x, y) = x^{o(1)}$; see for example (1.18) in Section 1.a of [16]. Hence it follows that at least one of these square values must be taken by $\varphi(n)$ for the requisite number of n.

To establish the lower bound for $V_\varphi(x)$ we simply replace the integers $n_\mathcal{R} = d_\mathcal{R} m_\mathcal{R}$ in the proof of Theorem 6.1 by the integers $k_\mathcal{R} = d_\mathcal{R} m_\mathcal{R}^3$. The values of $\varphi(k_\mathcal{R})$ are again perfect squares, and since $\varphi(k_\mathcal{R}) = m_\mathcal{R}^2 r$ where r is y-smooth, these values are pairwise distinct for different sets $\mathcal{R}$. Adjusting the choice of the parameter y in the proof of Theorem 6.1 in an obvious way we obtain the bound claimed for $V_\varphi(x)$. □

The application of (2.2) gives the same bound (6.2) for $M_\varphi(x)$ as for $S_\varphi(x)$ and also gives the bound $V_\varphi(x) \gg x^{0.2346}$; under the unproved assumption that (6.1) holds for arbitrary $v > 1$ these exponents can be increased to $1+o(1)$ and $1/3+o(1)$, respectively.

If one considers the functions corresponding to $M_\varphi(x)$ and $V_\varphi(x)$ but with respect to all values of $\varphi(n)$ (as opposed to just those which are squares), these problems have had a long history. In particular, our proofs above have been inspired by the lower bounds given by Erdős [10].

We next show how the arguments of the proof of Theorem 6.1 can be used to estimate $S_\lambda(x)$.

Theorem 6.3 *Under the same assumptions as in Theorem 6.1, we have the same lower bounds respectively for $S_\lambda(x)$, $M_\lambda(x)$, $V_\lambda(x)$ as given for $S_\varphi(x)$, $M_\varphi(x)$, $V_\varphi(x)$ in the previous two theorems.*

Proof Because of the similarities to the previous arguments we only sketch this. To obtain the bound for $S_\lambda(x)$ we proceed as in the proof of Theorem 6.1, but change "8" in the definition of y to 21, noting that $21 > e^3$. Further, we choose $\widetilde{\mathcal{P}}_{z,y}$ to be the same as $\mathcal{P}_{z,y}$ but deleting those primes for which $p-1$ is divisible by any prime power which exceeds y. The number of primes being deleted is $O(z/\sqrt{y})$ so that

$$\#\widetilde{\mathcal{P}}_{z,y} \ge \#\mathcal{P}_{z,y} + O(z/\sqrt{y}) = z^{1+o(1)}.$$

We define $m_\mathcal{R}$ as before and say

$$\lambda(m_\mathcal{R}) = \prod_{p \le y} p^{\alpha_p}.$$

By restricting ourselves to those subsets $\mathcal{R} \subseteq \widetilde{\mathcal{P}}_{z,y}$ we are able to conclude that each factor p^{α_p} is at most y. Let

$$d_\mathcal{R} = 2\lambda(m_\mathcal{R})^2 = 2^{2\alpha_2+1} \prod_{3 \le p \le y} p^{2\alpha_p}$$

and let $n_\mathcal{R} = d_\mathcal{R} m_\mathcal{R}$. Then $\lambda(n_\mathcal{R}) = d_\mathcal{R}/2$, a square. Further,

$$n_\mathcal{R} \le 2y^{2\pi(y)} Q_y z^k \le e^{(3+o(1))y} z^y \le (21z)^y = x.$$

From this point on, the lower bound for $S_\lambda(x)$ follows as in the proof of Theorem 6.1. The bounds for $M_\lambda(x)$ and $V_\lambda(x)$ follow as in the proof of Theorem 6.2. □

We now use a different approach to obtain a lower bound for $S^*_\varphi(x)$. In fact, we obtain a lower bound on the number $S^*_{\varphi,\sigma}(x)$ of squarefree positive integers $n \le x$ for which $\varphi(n)$ and $\sigma(n)$ are simultaneously perfect squares.

Theorem 6.4 *Under the same hypothesis as Theorem 6.1 we have*

$$S^*_\varphi(x) \ge x^{1-1/v+o(1)}.$$

Further, if $v > 1$ is fixed and there are positive constants A, C such that for all sufficiently large values of z we have

$$\pi_\pm(z, z^{1/v}) \ge C\frac{z}{\log^A z},$$

where $\pi_\pm(z,y)$ counts the number of primes $p \le x$ for which both $p-1$ and $p+1$ are y-smooth, then

$$S^*_{\varphi,\sigma}(x) \ge x^{1-1/v+o(1)}.$$

Proof Let $y = \log x/\log\log x$, and let $z = y^v$. Let $\mathcal{P}$ denote the set of primes $p \le z$ with $P(p-1) \le y$. Take $k = \lfloor \log x/\log z \rfloor$, and let N denote the number of subsets $\mathcal{R} \subset \mathcal{P}$ with $\#\mathcal{R} \le k$ and $\varphi\left(\prod_{p\in\mathcal{R}} p\right)$ a square. Thus $S^*_\varphi(x) \ge N$. Let q_i denote the i-th prime, and take $m = \pi(y)$, so that for each $p \in \mathcal{P}$ we have

$$p - 1 = \prod_{i=1}^m q_i^{\alpha_i}$$

for some nonnegative integers $\alpha_1, \ldots, \alpha_m$. Let $\mathbf{v}_p = (\alpha_1, \ldots, \alpha_m) \bmod 2$, where each α_i is now reduced modulo 2. So, N is the number of subsets $\mathcal{R} \subset \mathcal{P}$ with $\#\mathcal{R} \le k$ and $\sum_{p\in\mathcal{R}} \mathbf{v}_p = \mathbf{0}$ in $\mathbb{F}_2^m$. Since any sequence of $m+1$ vectors in $\mathbb{F}_2^m$ has a nonempty subsequence which sums to $\mathbf{0}$, it follows from Proposition 1.2 in [1] that

$$N \ge \frac{\binom{\pi(z,y)}{k}}{\binom{k}{m+1}} \ge \left(\frac{\pi(z,y)}{2k}\right)^k = \left(\frac{z^{1+o(1)}}{2y/v}\right)^k = \left(z^{1-1/v+o(1)}\right)^k = x^{1-1/v+o(1)},$$

since $k \sim y/v = z^{1/v+o(1)}$. This concludes the proof of the first part of the theorem.

For the second part of the theorem we change the definition of $\mathcal{P}$ to the set of primes $p \le z$ with $p^2 - 1$ being y-smooth. Further, if $p \in \mathcal{P}$ we now let $\mathbf{v}_p$ be $(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) \bmod 2$ where $p + 1 = \prod_i q_i^{\beta_i}$. The argument proceeds as before, but the role played by m in the above display is now played by $2m$. This completes the proof of the theorem. □

As before, using (2.2) we have (6.2) for $S^*_\varphi(x)$. Note that by considering $\pi_{-1}(z,y)$, which counts the number of primes $p \le z$ with $p+1$ being y-smooth, instead of $\pi(z,y)$ in the first part of Theorem 6.4, we get the same result for $S^*_\sigma(x)$. (The inequality (2.2) holds too for $\pi_{-1}(x,y)$.) It is interesting that the method of Theorem 6.1 does not seem to allow a generalization to σ. On the other hand, the method of Theorem 6.4 does not seem to give anything for $V_\varphi(x)$ nor for $S_\lambda(x)$. However, we do achieve the same inequality for $M^*_\varphi(x)$ (and for $M^*_\sigma(x)$) as in Theorem 6.2.

Using sieve methods one can show that there is some $v_0 > 1$ such that

$$\pi_\pm(z, z^{1/v_0}) \gg z/\log z, \tag{6.4}$$

and by the incorporation of additional ingredients it has been shown in [7] that every $v_0 < 4/3$ is admissible (in fact it is a very special case of a more general result of [7]). Thus, from Theorem 6.4 it follows that $S^*_{\varphi,\sigma}(x) \ge x^{1/4+o(1)}$. We conjecture that the hypothesis of the second part of Theorem 6.4 holds for each fixed $v > 1$, and so $S^*_{\varphi,\sigma}(x) = x^{1+o(1)}$.

7 Majorizing the Number of Squarefull Values of the Euler and Carmichael Functions

The following theorem provides a nontrivial upper bound for $F_\varphi(x)$.

Theorem 7.1 *We have the bound*

$$F_\varphi(x) \le x \exp\left(-(1+o(1))(\log x)^{1/2}(\log\log\log x)^{1/2}\right).$$

Proof Obviously, if $\varphi(n)$ is squarefull and not y-smooth, then $p^2 \mid \varphi(n)$ for some prime $p > y$. Therefore, for any $y \le x$, we have

$$F_\varphi(x) \le \Phi(x,y) + \sum_{p>y} T_\varphi(p^2, x).$$

We choose

$$u = \left(\frac{\log x}{\log\log\log x}\right)^{1/2} \qquad \text{and} \qquad y = x^{1/u}.$$

Then, the bound of Theorem 3.1 applies, which, together with (2.4), implies

$$\begin{aligned} F_\varphi(x) &\le x\exp(-(1+o(1))\,u\log\log u) + O\Big(x(\log\log x)^2\sum_{p>y}\frac{1}{p^2}\Big) \\ &\le x\exp(-(1+o(1))\,u\log\log u) + O\left(xy^{-1}(\log\log x)^2\right), \end{aligned}$$

and the result follows. □

As we have already observed, $F_\lambda(x) \le F_\varphi(x)$, hence Theorem 7.1 yields also the bound

$$F_\lambda(x) \le x \exp\left(-(1+o(1))(\log x)^{1/2}(\log\log\log x)^{1/2}\right).$$

We remark that the proof of Theorem 7.1 actually works for the larger count $P_\varphi(x)$ of integers $n \le x$ with $P(\varphi(n))^2|\varphi(n)$. Thus, probably the bound is not tight. Nevertheless, under assumption of the conditional bound (6.3), any potential improvement will still give an estimate for $F_\varphi(x)$ of the form $x^{1+o(1)}$.

8 Heuristic Lower Bound and Open Questions

Recall that $\psi(x,y)$ denotes the number of positive integers $n \le x$ which are y-smooth. The following estimate is a substantially relaxed and simplified version of Corollary 1.3 of [19]; see also [6]. For $\log^2 x \le y \le x$ we have

$$\psi(x,y) \ll \rho(u)x, \tag{8.1}$$

where, as always, $u = (\log x)/(\log y)$ and we recall that $\rho(u) = u^{-u+o(u)}$.

While the upper bound of Theorem 3.1 is considerably weaker than the analogous bound provided by (8.1) we expect that this reflects the true state of affairs. Certainly the Euler function has a “smoothing” effect on its integer arguments. Notice, for example, that $\varphi(n)$ is always at least as smooth as n and is smoother than n whenever n is squarefree so that we obtain the weak inequality $\Phi(x,y) \ge \psi(x,y)$. Moreover, it has been shown in [12] that normally $\varphi(n)$ has a substantially greater number of prime divisors than a “typical” integer of the same size so that it is perfectly reasonable to expect that $\Phi(x,y)$ is considerably larger than is $\psi(x,y)$. For example, it seems likely that the statement

$$\frac{\log\left(\psi(x,y)/x\right)}{\log\left(\Phi(x,y)/x\right)} \to \infty \tag{8.2}$$

must hold for a very wide region in the xy-plane; in fact we believe even more, namely that the bound of Theorem 3.1 is tight. We give some evidence for this below.

We are able to show that, under the conjecture that

$$\pi(z,y) \ge v^{-v+o(v)} \frac{z}{\log z} \tag{8.3}$$

for $y \ge \log z$ and as $v = (\log z)/(\log y) \to \infty$, which is somewhat weaker than the widely accepted conjecture (2.1) in the common range where both are asserted, we have for $2 \le y \le x^{1/\log\log x}$ that

$$\Phi(x,y) \ge x \exp\left(-(1+o(1))u \log\log\log x\right) \tag{8.4}$$

holds, where $u = (\log x)/(\log y)$ as usual. Note that (8.4) is trivially true in the range $y \le \log\log x$.

To derive (8.4) we define

$$w = \left\lfloor \frac{u}{\log\log x} \right\rfloor, \qquad\qquad v = u/w,$$

and put $z = x^{1/w} = y^v$. If n is any product of w distinct primes $p_1, \ldots, p_w \le z$ such that $p_j - 1$ is y-smooth for $j = 1, \ldots, w$, then $n \le x$ and $\varphi(n)$ is y-smooth; thus,

$$\Phi(x,y) \ge \binom{\pi(z,y)}{w} \ge \left(\frac{\pi(z,y)}{w}\right)^w.$$

Now, using the assumption (8.3), we see

$$\begin{aligned}\Phi(x,y) \quad &\ge \quad \left(v^{-v+o(v)} \frac{z}{w \log z}\right)^w \\ &= \quad v^{-u+o(u)} x (\log x)^{-w} = x \left(v^{1+o(1)} (\log x)^{1/v}\right)^{-u}.\end{aligned}$$

After simple calculations we obtain (8.4).

Note that the conditional result (8.4) implies that when $u \ge e^{(\log\log x)^{1+o(1)}}$ we have

$$\Phi(x,y) \ge x \exp\left(-(1+o(1))u \log\log u\right). \tag{8.5}$$

Also, comparing this with the bound

$$\psi(x,y) = x \exp\left(-(1+o(1))u \log u\right)$$

obtained in [6], we see that (8.2) holds in this case, assuming the conjecture (8.3). In fact, (8.4) implies (8.2) in the range $(\log x)^{1+\epsilon} \le y \le x^{1/(\log\log x)^{1-\epsilon}}$ for any fixed $\epsilon > 0$.

We also present an alternative heuristic argument, based on one of the methods in [26], which leads us to believe that in fact the lower bound (8.5) holds as well for larger values of y, namely in the range $\exp(\sqrt{\log x}) \le y \le x^{o(1)}$. Let

$$w = \lfloor u/\log u \rfloor, \qquad z = x^{1/w}, \qquad v = (\log z)/(\log y) = u/w \sim \log u.$$

Take the set $\mathcal{R}_{z,y}$ of primes p in the interval $(z^{1-1/u}, z)$ with $P(p-1) \le y$. From the lower bound on the range for y stated above, we have $z^{1-1/u} < z/e$, so that heuristically

$$\sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p} \ge v^{-v+o(v)} \left(\log\log z - \log\log z^{1-1/u} \right) \ge v^{-v+o(v)}.$$

In the stated range for y and for sufficiently large x we have

$$z^{-1+1/u} < y^{-1} \le e^{-u} < \frac{1}{2w(w-1)}.$$

Thus, for sufficiently large x,

$$\sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p^2} \le z^{-1+1/u} \sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p} \le \frac{1}{2w(w-1)} \left(\sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p} \right)^2.$$

Next, define the set $\mathcal{M}$ to be the set of squarefree integers m comprised precisely of w primes from $\mathcal{R}_{z,y}$. By the above inequality we conclude that

$$\begin{aligned}
\sum_{m \in \mathcal{M}} \frac{1}{m} &\ge \frac{1}{w!} \left(\sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p} \right)^w - \frac{1}{(w-2)!} \sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p^2} \left(\sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p} \right)^{w-2} \\
&\ge \frac{1}{2w!} \left(\sum_{p \in \mathcal{R}_{z,y}} \frac{1}{p} \right)^w \\
&\ge \exp\left(-(1+o(1))(wv\log v + w\log w)\right) = \exp\left(-(1+o(1))u\log\log u\right).
\end{aligned}$$

Finally, to complete the argument note that for any such m, if we have $mk \le x$ then $P(\varphi(mk)) \le y$, since the multiplier k satisfies $k \le y$. Indeed,

$$x = z^w > m > z^{(1-1/u)w} = x^{1-1/u} = x/y,$$

and hence

$$\Phi(x,y) \ge x \sum_{m \in \mathcal{M}} \frac{1}{m} \ge x \exp(-(1+o(1))u\log\log u).$$

We owe to an anonymous referee the suggestion that use of the stronger conjecture (2.1) for $\pi(x,y)$ leads to an asymptotic formula for $\Phi(x,y)$ for $x = y^u$. Specifically, one shows that

$$\Phi(x,y) = (1+o(1))\tau(u)x,$$

say for any fixed u, where the function τ is defined by the initial conditions $\tau(u) = 1$ for $u \le 1$, $\tau(u) = 1 - \frac{1}{2}(\log u)^2$ for $1 \le u \le 2$ together with the formula

$$u\tau(u) = \int_0^u \rho(t)\tau(u-t)dt,$$

which holds for all $u > 1$. An analysis of this integral equation leads to the estimate

$$\tau(u) = \exp(-(1+o(1))u\log\log u),$$

conditionally confirming the expected result.

We have established in Section 4 a number of upper bounds for $\Pi(x,y)$, however we wonder whether the bound

$$\Pi(x,y) \le \pi(x)\exp\left(-(1+o(1))u\log\log u\right)$$

also holds for values of y much closer to x. Certainly, studying $\Pi(x, y)$ for large values of y is a very interesting problem, especially because of its links to strong primes.

It is clear that the methods of this paper can be applied with little change to yield similar results for the number of values of $\varphi(n)$, $\sigma(n)$ or $\lambda(n)$ which are cubes or any fixed k-th power. One can also apply these techniques to study k-full values of these arithmetical functions. This naturally gives rise to the corresponding question about polynomial values occurring among the values of the Euler and Carmichael functions. For example, is it true that for any polynomial f, with integer coefficients, satisfying some congruence conditions, $\varphi(n) = f(m)$ for infinitely many integer pairs n, m? If so, can one establish reasonable bounds for the functions corresponding to those studied in this paper? If not, for which polynomials f is it true? For linear polynomials f this problem has been studied in several works; see [13] and references therein.

Some of our techniques also apply to $S_l(x)$, $M_l(x)$, $V_l(x)$ and $F_l(x)$ except that we restrict these of course to odd integers n. For example, the bound (2.4) together with Theorem 5.1 and the inequality $T_l(m, x) \le T_\varphi(m, x)$ can be used to obtain an analogue of Theorem 7.1 for $F_l(x)$.

As mentioned in the introduction, it is not known if there are infinitely many primes p with $p - 1$ a square. We can ask the slightly easier question: are there infinitely many primes p with $p-1$ squarefull? Of course, the answer must be "yes" but perhaps it is too much to hope that the extra freedom may allow a proof.

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] A. Balog, '$p+a$ without large prime factors', *Sem. Theorie des Nombres, Bordeaux*, 1983–84, 5 pp. (1984) Talence.

[4] 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.

[5] N. G. de Bruijn, 'On the number of positive integers $\le x$ and free of prime factors $> y$', *Nederl. Acad. Wetensch. Proc. Ser. A.*, **54** (1951), 50–60.

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

[7] C. Dartyge, G. Martin and G. Tenenbaum, 'Polynomial values free of large prime factors', *Periodica Math. Hungar.*, **43** (2001), 111–119.

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

[9] K. Dickman, 'On the frequency of numbers containing prime factors of a certain relative magnitude,' *Ark. Mat. Astr. Fys.*, **22** (1930), 1–14.

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

[11] 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.

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

[13] 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.

[14] É. Fouvry and G. Tenenbaum, 'Répartition statistique des entiers sans grand facteur premier dans les progressions arithmétiques', *Proc. London Math. Soc.*, **72** (1996), 481–514.

[15] J. B. Friedlander, 'Shifted primes without large prime factors' *Number Theory and Applications*, Kluwer A. P., Dordrecht, 1989, 393–401.

[16] A. Granville, 'Smooth numbers: Computational number theory and beyond', *Proc. MSRI Conf. Algorithmic Number Theory: Lattices, Number Fields, Curves, and Cryptography, Berkeley 2000*, Cambridge Univ. Press, (to appear).

[17] G. Greaves, *Sieves in Number Theory*, Springer–Verlag, Berlin, 2001.

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

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

[20] N. A. Hmyrova, 'On polynomials with small prime divisors, II', *Izv. Akad. Nauk SSSR Ser. Mat.*, **30** (1966), 1367–1372 (in Russian).

[21] H. Iwaniec, 'Almost-primes represented by quadratic polynomials', *Invent. Math.*, **47** (1978), 171–188.

[22] 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.

[23] G. Martin, 'An asymptotic formula for the number of smooth values of a polynomial', *J. Number Theory*, **93** (2002), 108–182.

[24] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1996.

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

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

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

[28] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, University Press, Cambridge, UK, 1995.

[29] N. M. Timofeev, 'Polynomials with small prime divisors', *Taškent. Gos. Univ., Naučn. Trudy No. 548, Voprosy Mat.*, Taškent, 1977, 87–91 (Russian).

[30] H.C. Williams, 'A $p+1$ method of factoring', *Math. Comp.*, **39** (1982), 225–234.