

## PRODUCTS OF SHIFTED PRIMES SIMULTANEOUSLY TAKING PERFECT POWER VALUES

TRISTAN FREIBERG

(Received 2 March 2011; accepted 1 February 2012)

Communicated by I. E. Shparlinski

Dedicated to the memory of Alf van der Poorten

### Abstract

Let  $r$  be an integer greater than 1, and let  $A$  be a finite, nonempty set of nonzero integers. We obtain a lower bound for the number of positive squarefree integers  $n$ , up to  $x$ , for which the products  $\prod_{p|n}(p+a)$  (over primes  $p$ ) are perfect  $r$ th powers for all the integers  $a$  in  $A$ . Also, in the cases where  $A = \{-1\}$  and  $A = \{+1\}$ , we will obtain a lower bound for the number of such  $n$  with exactly  $r$  distinct prime factors.

2010 *Mathematics subject classification*: primary 11N25; secondary 11A25.

*Keywords and phrases*: shifted primes, Euler's totient function, perfect powers.

### 1. Introduction

If we pick a large integer close to  $x$  at random, the probability that it is a perfect  $r$ th power is around  $x^{1/r}/x$ . We might expect the shifted primes  $p+a$  to behave more or less like random integers in terms of their multiplicative properties. Thus, if we take a large squarefree integer  $n$  close to  $x$ , we might naively expect that  $\sigma(n) = \prod_{p|n}(p+1) \approx n$  is an  $r$ th power with probability close to  $x^{1/r}/x$ . However, as we will see, the probability is much higher than this, indeed more than  $x^{0.7038}/x$ , for any given  $r$ . We will even show that the likelihood of  $\phi(n)$  and  $\sigma(n)$  *simultaneously* being (different)  $r$ th powers is more than  $x^{0.2499}/x$ . (As usual,  $\phi$  denotes Euler's totient function and  $\sigma$  denotes the sum-of-divisors function.) It would seem that  $r$ th powers are 'popular' values for products of shifted primes in general.

Counting those  $n$  with exactly  $r$  prime factors, we will show that the number of such  $n$  up to  $x$  for which  $\phi(n)$  is a perfect  $r$ th power is at least of the order of  $x^{1/r}/(\log x)^{r+2}$ , and likewise for  $\sigma(n)$ . Thus the number of positive integers  $n$  such that  $n \leq x$  and  $n = pq$ , where  $p$  and  $q$  are distinct primes, and  $(p-1)(q-1)$  is a square, is at least of

Supported by the Göran Gustafsson Foundation (KVA).

© 2012 Australian Mathematical Publishing Association Inc. 1446-7887/2012 \$16.00

the order of  $x^{1/2}/(\log x)^4$ . This may be seen as an ‘approximation’ to the well-known conjecture that there are infinitely many primes  $p$  for which  $p - 1$  is a square. It is easily seen that, for any given  $r \geq 2$ , there is at most one prime  $p$  such that  $p + 1$  is a perfect  $r$ th power, namely  $3 + 1 = 2^2$ ,  $7 + 1 = 2^3$ , and so on.

**NOTATION** The expressions  $F = O(G)$ ,  $F \ll G$ , and  $G \gg F$  all mean that  $|F| \leq cG$ , where  $c$  is a positive constant. Further,  $F \asymp G$  means that  $F \ll G \ll F$ . Where the constant  $c$  is not absolute but depends on one or more parameters, this dependence may be indicated, as in, for example,  $F \asymp_\epsilon G$ , where the implied constants depend on  $\epsilon$ . If  $f(x)$  and  $g(x)$  are functions and  $g(x)$  is nonzero for all sufficiently large  $x$ , we write  $f(x) \sim g(x)$  to mean that  $\lim_{x \rightarrow \infty} f(x)/g(x) = 1$ , and  $f(x) = o(g(x))$  to mean that  $\lim_{x \rightarrow \infty} f(x)/g(x) = 0$ . Other notation will be introduced as needed.

Given an integer  $r \geq 2$  and a finite, nonempty set  $A$  of nonzero integers, let

$$\mathcal{B}(x; A, r) = \left\{ n \in S \cap [1, x] : \prod_{p|n} (p + a) \in \mathbb{Z}^r \ \forall a \in A \right\},$$

where  $S$  denotes the set of squarefree integers and  $\mathbb{Z}^r$  denotes the set of perfect  $r$ th powers. Banks *et al.* [4] proved, among other results, that

$$|\mathcal{B}(x; \{-1\}, 2)| \geq x^{0.7039-o(1)} \quad \text{and} \quad |\mathcal{B}(x; \{+1\}, 2)| \geq x^{0.7039-o(1)},$$

and that

$$|\mathcal{B}(x; \{-1, +1\}, 2)| \geq x^{1/4-o(1)}.$$

The first theorem generalizes both of these results.

**THEOREM 1.1.** *Fix an integer  $r \geq 2$ , and a finite, nonempty set  $A$  of nonzero integers. As  $x$  tends to infinity,*

$$|\mathcal{B}(x; A, r)| \geq x^{1/2|A|-o(1)}.$$

Moreover, if  $|A| = 1$ , then as  $x$  tends to infinity,

$$|\mathcal{B}(x; A, r)| \geq x^{0.7039-o(1)}.$$

In the cases where  $A = \{-1\}$  or  $A = \{+1\}$ ,  $\mathcal{B}(x; A, r)$  is the set of positive squarefree integers  $n$  up to  $x$  for which  $\phi(n)$  or  $\sigma(n)$  respectively is an  $r$ th power. There is no condition on the number of prime factors of  $n$ , but the next theorem concerns the sets

$$\begin{aligned} \mathcal{B}^*(x; -1, r) &= \mathcal{B}(x; \{-1\}, r) \cap \{n : \omega(n) = r\}, \\ \mathcal{B}^*(x; +1, r) &= \mathcal{B}(x; \{+1\}, r) \cap \{n : \omega(n) = r\}, \end{aligned}$$

where  $\omega(n)$  is the number of distinct prime factors of  $n$ .

**THEOREM 1.2.** *Fix an integer  $r \geq 2$ . For all sufficiently large  $x$ ,*

$$|\mathcal{B}^*(x; -1, r)| \gg \frac{rx^{1/r}}{(\log x)^{r+2}} \quad \text{and} \quad |\mathcal{B}^*(x; +1, r)| \gg \frac{rx^{1/r}}{(\log x)^{r+2}}. \tag{1.1}$$

*The implied constants are absolute.*

The proof of Theorem 1.1, in Section 3, is an extension of the proof by Banks *et al.* [4] of the aforementioned special cases of Theorem 1.1. It employs some of the ideas of Erdős [9, 10] upon which Alford *et al.* [1] based their proof that there are infinitely many Carmichael numbers. (A Carmichael number is a composite number  $n$  for which  $a^n \equiv a \pmod n$  for all integers  $a$ .) Theorem 1.2 can be proved along the same lines. Indeed, in [5] it is shown that for all sufficiently large  $x$ , the lower bound  $|\mathcal{B}^*(x; -1, r)| \geq 4x^{1/r}/(9e(\log x)^{2r})$  holds for  $2 \leq r \leq (\log x/(12 \log \log x))^{1/2}$ . However, our proof of Theorem 1.2, in Section 4, introduces a new method, which, as we will explain, is an application of the ideas of Goldston *et al.* [11].

## 2. Preliminaries

Theorem 1.1 is a consequence of the first four results of this section, and we use the fifth in the proof of Theorem 1.2.

An integer  $n$  is called  $y$ -smooth if  $p \leq y$  for every prime  $p$  dividing  $n$ . Given a polynomial  $F(X) \in \mathbb{Z}[X]$  and numbers  $x \geq y \geq 2$ , let

$$\pi_F(x, y) = |\{p \leq x : F(p) \text{ is } y\text{-smooth}\}|.$$

In the case where  $F = X - 1$ , Erdős [9] proved that there exists a number  $\eta \in (0, 1)$  such that  $\pi_F(x, x^\eta) \gg_\eta \pi(x)$  (where  $\pi(x)$  is the number of primes up to  $x$ ), for all large  $x$  depending on the choice of  $\eta$ . Several authors have improved upon this, the next two results being the best so far obtained.

**THEOREM 2.1.** *Fix a nonzero integer  $a$  and let  $F(X) = X + a$ . There exists an absolute constant  $c$  such that*

$$\pi_F(x, y) > \frac{x}{(\log x)^c}$$

for all sufficiently large  $x$ , provided that  $y \geq x^{0.2961}$ .

**PROOF.** See [2, Theorem 1]. □

**THEOREM 2.2.** *Let  $F \in \mathbb{Z}[X]$ . Let  $g$  be the largest of the degrees of the irreducible factors of  $F$  in  $\mathbb{Z}[X]$ , and let  $k$  be the number of distinct irreducible factors of  $F$  in  $\mathbb{Z}[X]$  of degree  $g$ . Suppose that  $F(0) \neq 0$  if  $g = k = 1$ , and let  $\epsilon$  be any positive real number. Then*

$$\pi_F(x, y) \asymp \frac{x}{\log x}$$

for all sufficiently large  $x$ , provided that  $y \geq x^{g+\epsilon-1/2k}$ .

**PROOF.** See [6, Theorem 1.2]. □

For a finite additive abelian group  $G$ , denote by  $n(G)$  the length of the longest sequence of (not necessarily distinct) elements of  $G$ , no nonempty subsequence of which sums to 0, the additive identity of  $G$ . For instance, if  $G = (\mathbb{Z}/2\mathbb{Z})^m$ , then  $n(G) \leq m$ , for any sequence of  $m + 1$  elements of  $G$  contains a nonempty subsequence

whose elements sum to  $(0, \dots, 0) \pmod 2$ , as can be seen by considering that such a sequence contains  $2^{m+1} - 1 > 2^m = |G|$  nonempty subsequences. For any group  $G$  of order  $m$ , then any sequence of  $m$  elements contains a nonempty subsequence whose sum is 0, hence  $n(G) \leq m - 1$ . The next theorem, due to van Emde Boas and Kruyswijk [8], gives a nontrivial upper bound for  $n(G)$ .

**THEOREM 2.3.** *If  $G$  is a finite abelian group and  $m$  is the maximal order of an element in  $G$ , then  $n(G) < m(1 + \log(|G|/m))$ .*

**PROOF.** See [8]. A proof is also given in [1, Theorem 1.1]. □

The following proposition shows that under certain conditions there are many sequences in  $G$  whose elements sum to 0.

**PROPOSITION 2.4.** *Let  $G$  be a finite abelian group and let  $r$  and  $k$  be integers such that  $r > k > n = n(G)$ . Then any subsequence of  $r$  elements of  $G$  contains at least  $\binom{r}{k} / \binom{r}{n}$  distinct subsequences of length at most  $k$  and at least  $k - n$ , whose sum is the identity.*

**PROOF.** See [1, Proposition 1.2]. □

We will use the well-known Siegel–Walfisz theorem in the proof of Theorem 1.2.

**THEOREM 2.5 (Siegel–Walfisz).** *For any positive number  $B$ , there is a constant  $C_B$  that depends only on  $B$ , such that*

$$\sum_{\substack{p \leq N \\ p \equiv a \pmod k}} \log p = \frac{N}{\phi(k)} + O(N \exp(-C_B(\log N)^{1/2}))$$

whenever  $k \leq (\log N)^B$  and  $a$  is coprime with  $k$ .

**PROOF.** See [7, Ch. 22]. □

### 3. Proof of Theorem 1.1

The following proof hinges on Theorem 2.3 and Proposition 2.4, which are key ingredients in the celebrated proof of Alford *et al.* [1] that there are infinitely many Carmichael numbers. In fact it is shown in [1, Theorem 1] that  $C(x)$ , the number of Carmichael numbers up to  $x$ , satisfies  $C(x) \geq x^{\beta-\epsilon}$  for any positive  $\epsilon$  and all sufficiently large  $x$  (depending on the choice of  $\epsilon$ ), where

$$\beta = \frac{5}{12} \left( 1 - \frac{1}{2\sqrt{e}} \right) = 0.290\,36\dots$$

Using a variant of the construction in [1], Harman [12] proved that  $\beta = 0.332\,240\,8$  is admissible, and, by combining the ideas of [1, 4, 12], Banks [3] established the following result.

**THEOREM 3.1** [3, Theorem 1]. *For every fixed  $C < 1$ , there is a number  $x_0(C)$  such that for all  $x \geq x_0(C)$  the inequality*

$$|\{n \leq x : n \text{ is Carmichael and } \phi(n) \text{ is an } r\text{th power}\}| \geq x^{\beta-\epsilon}$$

*holds, where  $\beta = 0.332\,240\,8$  and  $\epsilon$  is arbitrarily small but positive, for all positive integers  $r \leq \exp((\log \log x)^C)$ .*

(Harman [13] subsequently proved that  $\beta = 0.7039 \times 0.4736 > 1/3$  is admissible here.) The method of the proof may yield further interesting results.

Theorems 2.1 and 2.2 are also crucial, and it will be manifest that extending the admissible range for  $y$  in those theorems will lead to better estimates for  $|\mathcal{B}(x; A, r)|$ . Explicitly, if  $F(X) = \prod_{a \in A} (X + a)$  and

$$\pi_F(x, x^\eta) \asymp_{F,\eta} \frac{x}{\log x},$$

then the following proof yields  $|\mathcal{B}(x; A, r)| \geq x^{1-\eta-o(1)}$ .

**PROOF OF THEOREM 1.1.** Fix an integer  $r \geq 2$  and a set  $A = \{a_1, \dots, a_s\}$  of nonzero integers. Let  $x$  be a large number, and let

$$y = \frac{\log x}{\log \log x}. \tag{3.1}$$

Let  $t = \pi(y)$ , and let  $G = (\mathbb{Z}/r\mathbb{Z})^{st}$ , so that by Theorem 2.3,

$$n(G) < r(1 + \log|G|/r) = r(1 + (st - 1) \log r). \tag{3.2}$$

Fix any number  $\epsilon \in (0, 1/3s)$ , and let

$$u = \begin{cases} 0.2961^{-1} & \text{if } s = 1, \\ \left(1 + \epsilon - \frac{1}{2s}\right)^{-1} & \text{if } s \geq 2. \end{cases}$$

Let

$$F(X) = (X + a_1)(X + a_2) \cdots (X + a_s),$$

and let

$$\begin{aligned} S_F(y^u, y) &= \{p \leq y^u : F(p) \text{ is } y\text{-smooth}\} \\ &= \{p \leq y^u : p + a_1, \dots, p + a_s \text{ are } y\text{-smooth}\}. \end{aligned}$$

We may suppose that  $x$ , and hence  $y$ , is large enough so that, by Theorems 2.1 and 2.2,

$$|S_F(y^u, y)| = \pi_F(y^u, y) \gg \frac{y^u}{(\log y^u)^c} \tag{3.3}$$

for some constant  $c$ . (We may suppose that  $c = 1$  if  $s \geq 2$ .) Finally, let

$$k = \left\lfloor \frac{\log x}{\log y^u} \right\rfloor, \tag{3.4}$$

where  $[\alpha]$  denotes the integer part of a real number  $\alpha$ .

By (3.1), (3.3) and (3.4),

$$\frac{\pi_F(y^u, y)}{k} \gg \frac{(\log x)^{u-1}}{(\log \log x)^{u-1+c}},$$

and by (3.1), (3.2) and (3.4),

$$\frac{k}{n(G)} \gg_{r,s} \frac{\log x / \log y^u}{t} \gg \log \log x, \tag{3.5}$$

because  $t = \pi(y) \sim y / \log y$  as  $y$  tends to infinity, by the prime number theorem. Hence, since  $u > 1$ , we may assume  $x$  is large enough that

$$n(G) < k < \pi_F(y^u, y). \tag{3.6}$$

For primes  $p \in S_F(y^u, y)$  and integers  $a \in A$ , we may write

$$p + a = 2^{\beta_1^{(a)}} 3^{\beta_2^{(a)}} \cdots p_t^{\beta_t^{(a)}},$$

where  $\beta_i^{(a)}$  are nonnegative integers when  $1 \leq i \leq t$ . We define

$$\mathbf{v}_p = (\beta_1^{(a_1)}, \dots, \beta_t^{(a_1)}, \beta_1^{(a_2)}, \dots, \beta_t^{(a_2)}, \dots, \beta_1^{(a_s)}, \dots, \beta_t^{(a_s)})$$

as the ‘exponent vector’ for  $p$ . For a subset  $R$  of  $S_F(y^u, y)$ ,  $\prod_{p \in R} (p + a)$  is an  $r$ th power for every  $a \in A$  if and only if

$$\sum_{p \in R} \mathbf{v}_p \equiv \mathbf{0} \pmod r,$$

where  $\mathbf{0} \pmod r$  is the zero element of  $G$ . If, moreover,  $R$  is of size at most  $k$ , then by (3.4),

$$\prod_{p \in R} p \leq y^{uk} \leq x.$$

Thus

$$|\mathcal{B}(x; A, r)| \geq \left| \left\{ R \subseteq S_F(y^u, y) : |R| \leq k \text{ and } \sum_{p \in R} \mathbf{v}_p \equiv \mathbf{0} \pmod r \right\} \right|, \tag{3.7}$$

as distinct subsets  $R \subseteq S_F(y^u, y)$  give rise to distinct integers  $n$ , by the uniqueness of factorization.

Because of (3.6), we may deduce from Proposition 2.4 that the right-hand side of (3.7) is at least

$$\binom{\pi_F(y^u, y)}{k} \bigg/ \binom{\pi_F(y^u, y)}{n(G)} \geq \left( \frac{\pi_F(y^u, y)}{k} \right)^k \pi_F(y^u, y)^{-n(G)} = x^{f(x)},$$

where

$$f(x) = (k - n(G)) \frac{\log \pi_F(y^u, y)}{\log x} - \frac{k \log k}{\log x}.$$

Letting  $x$  tend to infinity and using (3.1), (3.3)–(3.5), we can now see that  $f(x) = 1 - 1/u - o(1)$ . Therefore, as  $x$  tends to infinity,

$$|\mathcal{B}(x; A, r)| \geq x^{1-1/u-o(1)},$$

and Theorem 1.1 follows by our choice of  $u$ , and letting  $\epsilon$  tend to 0 if  $s \geq 2$ . □

### 4. Proof of Theorem 1.2

We use a different approach to prove Theorem 1.2. The proof is ‘inspired’ by the breakthrough results of Goldston *et al.* [11] on short intervals containing primes. Basically, their proof begins with the observation that if  $W(n)$  is a nonnegative weight and

$$\sum_{N < n \leq 2N} \left( \sum_{1 \leq h \leq H} \vartheta(n+h) - \log(2N+H) \right) W(n) \tag{4.1}$$

is positive, then for some  $n \in (N, 2N]$ , the interval  $(n, n+H]$  contains at least two primes. Here and later,

$$\vartheta(n) = \begin{cases} \log n & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Goldston *et al.* were able to obtain a nonnegative weight  $W(n)$  for which the sum (4.1), with  $H = \epsilon \log N$ , is positive for all sufficiently large  $N$ . In our problem, we will be led to consider

$$\sum_{1 \leq n \leq N} \left( \sum_{1 \leq a \leq H} \vartheta(a^r n + 1) - (r-1) \log(H^r N + 1) \right)$$

(see (4.3)). A lower bound for this expression corresponds to a lower bound for the number of positive integers  $n \leq N$  for which  $\{a^r n + 1 : a \leq H\}$  contains at least  $r$  primes. As we do not require  $H$  to be ‘short’ compared to  $N$ , we may take  $H = r \log N$ ; then the weight  $W(n) = 1$  works, and the problem is much easier.

**PROOF OF THEOREM 1.2.** Throughout the proof,  $r$  is a fixed integer greater than 1, and  $n, a, a_1, a_2, \dots$  are positive integers. Observe that if, for some  $n$ , the numbers  $\ell_i$ , given by

$$\ell_i = a_i^r n + 1,$$

are distinct primes (where  $i = 1, \dots, r$ ), then

$$\phi(\ell_1 \cdots \ell_r) = (a_1 \cdots a_r n)^r.$$

If the primes  $\ell_i$  are of the form  $a_i^r n - 1$  then  $\sigma(\ell_1 \cdots \ell_r) = (a_1 \cdots a_r n)^r$ . We will prove that (1.1) holds for  $|\mathcal{B}(x; -1, r)|$ , provided that  $x$  is sufficiently large, and the same

proof applies to  $|\mathcal{B}(x; +1, r)|$  if we consider primes of the form  $a_i^r n - 1$  rather than  $a_i^r n + 1$ .

Let  $N$  be a parameter tending monotonically to infinity and set  $H = r \log N$ . Let  $\mathcal{A}(N)$  be the set of positive integers  $n \leq N$  for which

$$C_n := \{a^r n + 1 : a \leq H\} \cap \mathcal{P}$$

(where  $\mathcal{P}$  is the set of all primes) contains at least  $r$  primes. We will show that

$$|\mathcal{A}(N)| \gg \frac{N}{\log N}, \tag{4.2}$$

but first we will describe how this implies a lower bound for  $|\mathcal{B}(x; -1, r)|$ .

Every  $n \in \mathcal{A}(N)$  gives rise, via  $C_n$ , to some  $\ell_1 \cdots \ell_r \in \mathcal{B}((H^r N + 1)^r; -1, r)$ , though different  $n$  may give rise to the same  $r$ -tuple of primes. On the other hand, given  $n \in \mathcal{A}(N)$  and a prime  $p = a^r n + 1 \in C_n$ , each  $m \in \mathcal{A}(N)$  for which  $p \in C_m$  corresponds to a solution to  $a^r n = b^r m$ ,  $b \leq H$ . Therefore there can be at most  $H$  different integers  $n \in \mathcal{A}(N)$  giving rise to the same element of  $\mathcal{B}((H^r N + 1)^r; -1, r)$ . Consequently,

$$|\mathcal{B}((H^r N + 1)^r; -1, r)| \geq \frac{|\mathcal{A}(N)|}{H} \gg \frac{N}{r(\log N)^2}$$

by (4.2), and (1.1) follows.

We will now establish (4.2). We will show that for all large  $N$ ,

$$S(N) = \sum_{1 \leq n \leq N} \left( \sum_{1 \leq a \leq H} \vartheta(a^r n + 1) - (r - 1) \log(H^r N + 1) \right) \gg rN \log N. \tag{4.3}$$

Consequently  $\mathcal{A}(N)$  is nonempty for large  $N$ . Indeed, if (4.3) holds then

$$\begin{aligned} rN \log N \ll S(N) &\leq \sum_{n \in \mathcal{A}(N)} \left( \sum_{1 \leq a \leq H} \vartheta(a^r n + 1) - (r - 1) \log(H^r N + 1) \right) \\ &\leq |\mathcal{A}(N)| H \log(H^r N + 1), \end{aligned}$$

and (4.2) follows because  $\log(H^r N + 1) \sim \log N$ .

For the evaluation of  $S(N)$ , first note that

$$\sum_{1 \leq n \leq N} \sum_{1 \leq a \leq H} \vartheta(a^r n + 1) = \sum_{1 \leq a \leq H} \sum_{\substack{p \leq a^r N + 1 \\ p \equiv 1 \pmod{a^r}}} \log p.$$

Since  $a^r \ll_r (\log N)^r$  for  $a \leq H$ , we may apply Theorem 2.5 to the last sum. We have

$$\sum_{\substack{p \leq a^r N + 1 \\ p \equiv 1 \pmod{a^r}}} \log p = \frac{a^r N}{\phi(a^r)} + O\left(\frac{a^r N}{\phi(a^r)(\log N)^2}\right) \sim \frac{a}{\phi(a)} N.$$



Therefore, from the well-known estimate

$$\sum_{1 \leq a \leq H} \frac{a}{\phi(a)} \sim cH \quad \text{where } c = \prod_p \left(1 + \frac{1}{p(p-1)}\right) = 1.943\,596\dots,$$

we deduce that

$$\sum_{1 \leq n \leq N} \sum_{1 \leq a \leq H} \vartheta(a^r n + 1) \sim N \sum_{1 \leq a \leq H} \frac{a}{\phi(a)} \sim cNH.$$

Also,

$$\sum_{1 \leq n \leq N} (r-1) \log(H^r N + 1) \sim N(r-1) \log N,$$

so combining all of this yields

$$S(N) \sim N(cH - (r-1) \log N) \gg rN \log N,$$

and (4.3) follows.

### Acknowledgements

I would like to thank Andrew Granville for introducing me to the problems considered in this paper, and for his help in its preparation. I thank William Banks for bringing [5] to my attention, and Christian Elsholtz for some helpful comments. Finally, I am grateful to the anonymous referee for providing comments and corrections.

### References

- [1] W. R. Alford, A. Granville and C. Pomerance, 'There are infinitely many Carmichael numbers', *Ann. of Math. (2)* **139** (1994), 703–722.
- [2] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.* **83** (1998), 331–361.
- [3] W. D. Banks, 'Carmichael numbers with a square totient', *Canad. Math. Bull.* **52** (2009), 3–8.
- [4] W. D. Banks, J. B. Friedlander, C. Pomerance and I. E. Shparlinski, 'Multiplicative structure of values of the Euler function', in: *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, vol. 41 (eds. A. van der Poorten and A. Stein) (American Mathematical Society, Providence, RI, 2004), pp. 29–47.
- [5] W. D. Banks and F. Luca, 'Power totients with almost primes', *Integers* **11** (2011), 307–313.
- [6] C. Dartyge, G. Martin and G. Tenenbaum, 'Polynomial values free of large prime factors', *Period. Math. Hungar.* **43** (2001), 111–119.
- [7] H. Davenport, *Multiplicative Number Theory*, 3rd edn (Springer, New York, 2000), revised and with a preface by H. L. Montgomery.
- [8] P. van Emde Boas and D. Kruyswijk, *A Combinatorial Problem on Finite Abelian Groups III*, Afd. zuivere Wisk., 1969-008 (Math. Centrum, Amsterdam, 1969).
- [9] P. Erdős, 'On the normal number of prime factors of  $p-1$  and some other related problems concerning Euler's  $\phi$ -function', *Q. J. Math. (Oxford Ser.)* **6** (1935), 205–213.
- [10] P. Erdős, 'On pseudoprimes and Carmichael numbers', *Publ. Math. Debrecen* **4** (1956), 201–206.

- [11] D. A. Goldston, J. Pintz and C. Y. Yıldırım, 'Primes in tuples I', *Ann. of Math. (2)* **170** (2009), 819–862.
- [12] G. Harman, 'On the number of Carmichael numbers up to  $x$ ', *Bull. Lond. Math. Soc.* **37** (2005), 641–650.
- [13] G. Harman, 'Watt's mean value theorem and Carmichael numbers', *Int. J. Number Theory* **4** (2008), 241–248.

TRISTAN FREIBERG, Department of Mathematics,  
KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden  
e-mail: [tristanf@kth.se](mailto:tristanf@kth.se)