Ramanujan Journal manuscript No.
(will be inserted by the editor)

Sets of monotonicity for Euler's totient function

Paul Pollack · Carl Pomerance · Enrique Treviño

Abstract We study subsets of $[1, x]$ on which the Euler φ-function is monotone (nondecreasing or nonincreasing). For example, we show that for any $\epsilon > 0$, every such subset has size smaller than ϵx, once $x > x_0(\epsilon)$. This confirms a conjecture of the second author.

Keywords Euler function · monotone subsequence · locally repeated values

Mathematics Subject Classification (2000) Primary: 11A25 · Secondary: 11N25, 11N36

1 Introduction

Let φ denote Euler's totient function, so that $\varphi(n) := \#(\mathbf{Z}/n\mathbf{Z})^\times$. It is easy to prove that $\varphi(n) \to \infty$ as $n \to \infty$, but it does not tend to infinity monotonically; e.g., $\varphi(9) = 6$ while $\varphi(10) = 4$. Thus, it is natural to wonder how far φ is from being monotone. This question was posed more precisely by the second author at the 2009 West Coast Number Theory Conference [15]: Let $M^\uparrow(x)$ denote the maximum size of a subset of $[1, x]$ on which φ is nondecreasing. Define $M^\downarrow(x)$ similarly, with "nonincreasing" replacing "nondecreasing". Can one understand the rate of growth of the functions $M^\uparrow(x)$ and $M^\downarrow(x)$?

The second author conjectured (ibid.) that both $M^\uparrow(x)/x \to 0$ and $M^\downarrow(x)/x \to 0$. We begin this paper by proving strong forms of both conjectures. We start with the nonincreasing case:

Theorem 1.1 *As $x \to \infty$, we have*

$$M^\downarrow(x) \le \frac{x}{\exp\left(\left(\frac{1}{2} + o(1)\right)\sqrt{\log x \log\log x}\right)}.$$

Paul Pollack
University of British Columbia, Department of Mathematics, 1984 Mathematics Road, Vancouver, British Columbia V6T 1Z2, Canada
E-mail: pollack@math.ubc.ca

Carl Pomerance
Dartmouth College, Department of Mathematics, 6188 Kemeny Hall, Hanover, New Hampshire 03755, USA
E-mail: carl.pomerance@dartmouth.edu

Enrique Treviño
Swarthmore College, Department of Mathematics and Statistics, 500 College Avenue, Swarthmore, Pennsylvania 19081, USA
E-mail: etrevin1@swarthmore.edu

It is clear that a result like Theorem 1.1 cannot hold for $M^{\uparrow}(x)$, since φ is increasing on the primes. In fact, we show that the primes give something close to best possible, namely we have $M^{\uparrow}(x) = x/(\log x)^{1+o(1)}$ as $x \to \infty$. More precisely, we prove the following result:

Theorem 1.2 *Let $\mathscr{W}(x) := \{\varphi(n) : n \le x\}$ denote the image of φ on $[1, x]$, and let $W(x) := \#\mathscr{W}(x)$. Then*

$$\limsup_{x\to\infty} M^{\uparrow}(x)/W(x) < 1.$$

Erdős [4] showed that $W(x) = x/(\log x)^{1+o(1)}$, as $x \to \infty$. Subsequent to this, many authors worked on fleshing out the "$o(1)$"-term in his result, culminating in Ford's determination of the precise order of magnitude of $W(x)$ ([8], announced in [9]).

We start the proof of Theorem 1.2 by showing that if $\mathscr{S} \subset [1, x]$ is a set on which φ is nondecreasing, then it is very rare for φ to agree on neighboring elements of $\mathscr{S}$. Here a key role is played by upper estimates for the number of solutions n to an equation of the form $\varphi(n) = \varphi(n + k)$. This equation has been treated in [6, Theorem 2] and [10], but only for fixed k. We require results which are uniform in k, which we state and prove in §3.

Our results in §3 already suffice to show that $\limsup M^{\uparrow}(x)/W(x) \le 1$. To obtain the small improvement indicated in Theorem 1.2, we show that a positive proportion of the elements of $\mathscr{W}(x)$ are missing from the set $\varphi(\mathscr{S})$. As an example of how this goes, suppose we have a pair of elements $d_1 < d_2$ of $\mathscr{W}(x)$ for which each preimage of d_1 exceeds each preimage of d_2. If φ is nondecreasing on $\mathscr{S}$, then $\varphi(\mathscr{S})$ must be missing at least one of d_1 and d_2. In §4, we show how to construct a large number of such pairs $\{d_1, d_2\}$.

The construction alluded to in the last paragraph exploits an observation of Erdős: Call a number in the image of the Euler function a *totient*. Suppose that d is a totient with preimages $n_1, \ldots, n_k$. We say that the number n is *convenient for* d if $d\varphi(n)$ is a totient with preimages $n_1 n, \ldots, n_k n$ and no others. Erdős [5, pf. of Theorem 4] proved that for each fixed totient d, almost all primes p are convenient for d. We require a variant of this result, which we prove using methods of Ford (op. cit.) and which appears as Lemma 4.1 below.

One may also ask about lower bounds on $M^{\uparrow}(x)$ and $M^{\downarrow}(x)$. As noted above, if $\mathscr{S}$ consists of all the primes in $[1, x]$, then φ is nondecreasing on $\mathscr{S}$, and so $M^{\uparrow}(x) \ge \pi(x)$. The second author [15] has asked the following:

Question *Does $M^{\uparrow}(x) - \pi(x) \to \infty$ as $x \to \infty$?*

We have not been able to resolve this. Computations suggest (see §9) that this difference does not tend to infinity, in fact it seems $M^{\uparrow}(x) = \pi(x) + 64$ for x large enough. Perhaps the following closely related question is not unattackable:

Question *If $\mathscr{S}$ is a subset of $[1, x]$ on which φ is nondecreasing, must we have $\sum_{n\in\mathscr{S}} \frac{1}{n} \le \log\log x + O(1)$?*

The behavior of $M^{\downarrow}(x)$ is more mysterious. Let $M^0(x)$ denote the maximal size of a subset of $[1, x]$ on which φ is constant. Clearly, $M^{\downarrow}(x) \ge M^0(x)$. Erdős [4] showed that there is a constant $\alpha > 0$ so that $M^0(x) \ge x^{\alpha}$ for all large x. The current record here is $\alpha = 0.7038$, due to Baker and Harman [2], but heuristic arguments (see [17] or [18, §4]) suggest that (as $x \to \infty$)

$$M^0(x) = x/L(x)^{1+o(1)}, \quad \text{where} \quad L(x) = \exp(\log x \log_3 x/\log_2 x). \tag{1.1}$$

Perhaps it is true that $M^{\downarrow}(x) \ll M^0(x)$. This would improve Theorem 1.1, since (from either [17] or [18]) the upper bound on $M^0(x)$ implicit in (1.1) is known to hold unconditionally. In the opposite direction, we prove:

Theorem 1.3 *$M^{\downarrow}(x) - M^0(x) > x^{0.18}$ for large x.*

We do not know how to improve the upper bounds of Theorems 1.1 and 1.2, even if we ask that φ be *strictly monotone* on $\mathscr{S}$. Turning instead to lower bounds, the primes once again furnish a fairly large subset of $[1, x]$ on which φ is strictly increasing. For the strictly decreasing case, we prove the following:

Theorem 1.4 *For all large x, there is a subset $\mathscr{S}$ of $[1, x]$ of size at least $x^{0.19}$ for which the restriction of φ to $\mathscr{S}$ is strictly decreasing.*

It would be interesting to know the extent to which Theorem 1.4 can be improved. If the largest prime gap up to x is $x^{o(1)}$ (with $x \to \infty$), as is widely expected, then the proof of Theorem 1.4 allows us to replace the exponent 0.19 with $\frac{1}{3} - \epsilon$.

Our final theorem illustrates that very satisfactory estimates can be obtained for the largest set of *consecutive integers* in $[1, x]$ on which φ is monotone.

Theorem 1.5 *The maximum size of a set of consecutive integers contained in $[1, x]$ on which φ is nonincreasing is*

$$\frac{\log_3 x}{\log_6 x} + (\alpha - \gamma + o(1))\frac{\log_3 x}{(\log_6 x)^2} \qquad (x \to \infty).$$

The same estimate holds with "nondecreasing" replacing "nonincreasing". Here $\gamma = 0.57721566490\ldots$ is the Euler–Mascheroni constant, and α is defined by the relation

$$\exp(\alpha) = \prod_{p \text{ prime}} (1 - 1/p)^{-1/p}, \quad \textit{so that} \quad \alpha = 0.58005849381\ldots.$$

The form of Theorem 1.5, while perhaps surprising, is not entirely unexpected. Erdős [5, Theorem 1] showed that the same result holds for the maximum size of a set $\mathscr{S} \subset [1, x]$ of consecutive integers for which $\max_{m \in \mathscr{S}} \varphi(m) \sim \min_{m \in \mathscr{S}} \varphi(m)$. Our proof follows Erdős's, with some modifications (compare also [16]).

Certain other natural ways of measuring the non-monotonic behavior of φ reduce to ones we have considered here. For example, take the problem of partitioning $[1, x]$ into sets on which φ is strictly increasing. It seems reasonable to ask for an estimate of the smallest number of sets one needs in such a partition. In fact, the minimum number of required sets is precisely $M^{\downarrow}(x)$, by a combinatorial theorem of Dilworth. Analogous comments apply with "strictly increasing" replaced by "strictly decreasing", "nonincreasing", or "nondecreasing".

Notation

Most of our notation is standard. A possible exception is our notation for $\prod_{p \mid n} p$ (the *algebraic radical* of n), written as either $\gamma(n)$ or $\mathrm{rad}(n)$. We write $\omega(n) := \sum_{p \mid n} 1$ for the number of distinct prime factors of n. If $d \mid n$ and $\gcd(d, n/d) = 1$, we say that d is a *unitary divisor* of n, and we write $d \parallel n$. We remind the reader that $\log_k$ denotes the kth iterate of the natural logarithm. The Landau–Bachmann o and O-symbols, as well as Vinogradov's $\ll$ notation, are employed with their usual meanings. Implied constants are absolute unless otherwise specified.

2 Sets on which φ is nonincreasing: Proof of Theorem 1.1

Lemma 2.1 *Let $\mathscr{S}$ be a subset of $[1,x]$ on which φ is nonincreasing. For $x \geq 1$, the number of prime powers $n \in \mathscr{S}$ is at most $\log x/\log 2$. If $x \geq 1$ and $k > 1$, the number of $n \in \mathscr{S}$ with $\omega(n) = k$ is at most*

$$42(k-1)!x^{1-\frac{1}{k}}. \tag{2.1}$$

Proof For each r, there is at most one prime power of the form $n = p^r$ in $\mathscr{S}$, since the function $p \mapsto \varphi(p^r)$ is an increasing function of p. Also, it is clear that there are no such n once $r > \log x/\log 2$. This proves the first claim.

We prove the second assertion of the lemma by induction on k. Take first the case $k = 2$. Let $\mathscr{T}$ be the set of $n \in \mathscr{S}$ with $\omega(n) = 2$, and partition $\mathscr{T}$ into sets $\mathscr{T}_{p^r}$, according to the smallest prime power p^r for which $p^r \parallel n$. Then φ is nonincreasing on the set $\mathscr{T}'_{p^r} := \{n/p^r : n \in \mathscr{T}_{p^r}\} \subset [1, x/p^r]$, and every $m \in \mathscr{T}'_{p^r}$ is a prime power. So by the first part of the lemma,

$$\#\mathscr{T} \leq \frac{1}{\log 2} \sum_{p^r \leq x^{1/2}} \log \frac{x}{p^r} \leq 2 \log x \sum_{p^r \leq x^{1/2}} 1.$$

Also,

$$\sum_{p^r \leq x^{1/2}} 1 = \pi(x^{1/2}) + \sum_{r \geq 2} \sum_{p \leq x^{\frac{1}{2r}}} 1 \leq \pi(x^{1/2}) + x^{1/4} \frac{\log (x^{1/2})}{\log 2} \leq \pi(x^{1/2}) + x^{1/4} \log x.$$

Recalling the elementary estimate $\pi(X) \leq 6X/\log X$ for $X > 1$ (cf. [1, Theorem 4.6]), we find that

$$\#\mathscr{T} \leq 24x^{1/2} + 2x^{1/4}(\log x)^2 < 42x^{1/2}$$

for all $x \geq 1$. This agrees with the claim of the lemma.

Suppose the case k has been proved (for all $\mathscr{S}$ and all x). Take $\mathscr{T}$ as the set of $n \in \mathscr{S}$ with $\omega(n) = k+1$. Partitioning $\mathscr{T}$ into sets $\mathscr{T}_{p^r}$ as in the last paragraph, we obtain from the induction hypothesis that

$$\#\mathscr{T} \leq 42(k-1)!x^{1-\frac{1}{k}} \sum_{p^r \leq x^{\frac{1}{k+1}}} \frac{1}{(p^r)^{1-1/k}}. \tag{2.2}$$

Estimating crudely,

$$\sum_{p^r \leq x^{\frac{1}{k+1}}} \frac{1}{(p^r)^{1-1/k}} \leq \sum_{n \leq x^{1/(k+1)}} \frac{1}{n^{1-1/k}} \leq 1 + \int_1^{x^{\frac{1}{k+1}}} \frac{dt}{t^{1-1/k}} < k \cdot x^{\frac{1}{k(k+1)}}. \tag{2.3}$$

Substituting (2.3) back into (2.2) establishes the $k+1$ case. □

Proof (Proof of Theorem 1.1) Let $\mathscr{S}$ be a subset of $[1,x]$ on which φ is nonincreasing. Let $K := \lfloor \sqrt{\log x/\log\log x} \rfloor$, and split the $n \in \mathscr{S}$ according to whether or not $\omega(n) \leq K$. Since the expression (2.1) is increasing as a function of k, Lemma 2.1 gives that the number of n of the first type is at most

$$42K!x^{1-\frac{1}{K}} + (1 + \log x/\log 2).$$

Using the trivial estimate $K! < K^K$, we find after a short computation that this is at most

$$\frac{x}{\exp\left(\left(\frac{1}{2} + o(1)\right)\sqrt{\log x \log\log x}\right)}, \tag{2.4}$$

as $x \to \infty$. The number of n of the second type does not exceed the total number of $n \le x$ with $\omega(n) > K$. By a classical inequality of Hardy and Ramanujan [12, Lemma B], this is

$$\ll \sum_{k>K} \frac{x}{\log x} \frac{(\log\log x + O(1))^{k-1}}{(k-1)!}.$$

The sum appearing here is dominated by its first term, corresponding to $k-1 = K$; using the estimate $K! \ge (K/e)^K$, another short computation shows that this sum is also bounded by (2.4). □

3 Towards Theorem 1.2: Counting solutions to $\varphi(n) = \varphi(n+k)$

Let $P(x;k)$ denote the number of $n \le x$ for which $\varphi(n) = \varphi(n+k)$. To prove Theorem 1.2 we require a reasonable estimate for $P(x;k)$ valid uniformly for $k \le \log x$. We begin by quoting three results from [10].

Theorem A (see [10, Theorem 1]) *Suppose that j and $j+k$ have the same prime factors (so that k is even), and let $g = \gcd(j, j+k)$. Suppose that for the positive integer r, both*

$$\frac{j}{g}r + 1 \quad \textit{and} \quad \frac{j+k}{g}r + 1 \tag{3.1}$$

are primes not dividing j. Then with

$$n = j\left(\frac{j+k}{g}r + 1\right),$$

we have $\varphi(n) = \varphi(n+k)$.

Let $P_0(x;k)$ be the number of solutions $n \le x$ to $\varphi(n) = \varphi(n+k)$ which are of the form given in Theorem A, and let $P_1(x;k)$ be the number of remaining solutions.

Theorem B (cf. [10, Corollary 1]) *Assume the prime k-tuples conjecture in the quantitative form of Bateman–Horn. Suppose k is even, and put*

$$c(k) = \sum_{j\colon \gamma(j)=\gamma(j+k)} \frac{\gcd(j, j+k)}{j(j+k)} \prod_{\substack{p \mid jk(j+k)/\gcd(j,j+k)^3 \\ p>2}} \frac{p-1}{p-2}. \tag{3.2}$$

Then $0 < c(k) < \infty$, and as $x \to \infty$,

$$P_0(x;k) \sim 2C_2 c(k) \frac{x}{(\log x)^2},$$

where $C_2 := 2\prod_{p>2}(1-(p-1)^{-2})$ is the twin prime constant.

Theorem C (see [10, Theorem 2]) *Fix a natural number k. For $x > x_0(k)$, we have $P_1(x;k) < x/\exp((\log x)^{1/3})$.*

We require a uniform version of Theorem C and an unconditional upper-bound analogue of Theorem B.

Theorem 3.1 *For $x > x_0$, we have $P_1(x;k) < x/\exp((\log x)^{1/3})$, uniformly for natural numbers $k \le \exp((\log x)^{1/3})$.*

Proof (Proof (sketch)) We imitate the proof of [10, Theorem 2]. Let $n \le x$ be a solution to $\varphi(n) = \varphi(n+k)$ not accounted for by Theorem A. Write $n = mp$ and $n+k = m'p'$, where p is the largest prime factor of n and p' the largest prime factor of $n+k$. As in [10], if $\varphi(m)/m = \varphi(m')/m'$, then n has the shape indicated in Theorem A. So we can assume that $\varphi(m)/m \ne \varphi(m')/m'$. For fixed k, Theorem C then follows from the argument described in [6] for the case $k = 1$. Suppose now that k is not fixed but satisfies the bound indicated in our theorem. The argument of [6] goes through with obvious minor changes until [6, eq. (4.4)]. At that point, it is important to know that given m and a certain prime q', the congruence $mp + k \equiv 0 \pmod{q'}$ forces p to lie in a uniquely determined residue class modulo q'. This holds as long as $q' \nmid m$. If $q' \mid m$ and $q' \mid mp+k$, then $q' \mid k$. But we also have that $q' \equiv 1 \pmod r$, where $r \ge l^4$ and $l = \exp((\log x)^{1/3})$. Hence $q' > l^4 > k$, and so $q' \nmid k$. $\square$

Obtaining a uniform upper bound on $P_0(x;k)$ requires more preparation.

Lemma 3.2 *Let k be a natural number. The number of natural numbers j for which j and $j+k$ have the same set of prime factors is at most*

$$3 \cdot 7^{3+2\omega(k)}.$$

Consequently, for each $\epsilon > 0$, there are fewer than k^ϵ such numbers j once $k > k_0(\epsilon)$.

Proof If j and $j+k$ have the same set of prime divisors, then this common set is a subset of the primes dividing k. Hence, the equation $(j+k)/k + (-j/k) = 1$ is an instance of the S-unit equation $x + y = 1$ over $\mathbf{Q}$, where S consists of the infinite place together with the primes dividing k. By a theorem of Evertse [7, Theorem 1], the number of solutions here is at most $3 \cdot 7^{1+2\#S} = 3 \cdot 7^{3+2\omega(k)}$. The final claim in the lemma follows from the well-known upper bound $\omega(k) \ll \frac{\log k}{\log\log 3k}$ (cf. [13, p. 471]). $\square$

The following result is our analogue of Theorem B.

Theorem 3.3 *Let $\varepsilon(x)$ be a positive-valued function of x for which $\varepsilon(x) \to 0$ while $x^{\varepsilon(x)} \to \infty$. Let k be an even natural number satisfying $2 \le k \le x^{\varepsilon(x)}$. Then as $x \to \infty$,*

$$P_0(x;k) \le (16C_2 + o(1))c(k)\frac{x}{(\log x)^2},$$

uniformly in k. Moreover, $(2k)^{-1} \le c(k) \le \left(3 \cdot 7^{3+2\omega(k)} \prod_{\substack{p\mid k\\ p>2}} \frac{p-1}{p-2}\right) \cdot k^{-1}$.

Remark Since $\prod_{p\mid k, p>2} \frac{p-1}{p-2} \ll k/\varphi(k) \ll \log\log k$ and $\omega(k) \ll \log k/\log\log(3k)$, it follows that $c(k) \ll k^{-1}\exp(O(\log k/\log\log(3k)))$. All that will be used in the proof of Theorem 1.2 is that $c(k)$ is absolutely bounded.

Proof Fix a j for which $\gamma(j) = \gamma(j+k)$. Put $g = \gcd(j, j+k)$. Assume first that $j(j+k)/g \le x^{\sqrt{\varepsilon(x)}}$. If $n \le x$ has the form given in Theorem A corresponding to this value of j, then

$$\frac{j(j+k)}{g} r \le x, \tag{3.3}$$

and both expressions in (3.1) are prime. By Selberg's upper bound sieve (see [11, Theorem 5.7]), the number of such n is at most

$$(16C_2 + o(1)) \left(\frac{g}{j(j+k)} \prod_{\substack{p\mid jk(j+k)/g^3\\ p>2}} \frac{p-1}{p-2} \right) \frac{x}{(\log x)^2},$$

as $x \to \infty$. Summing, we find that the contribution from these "small" j satisfies the bound asserted in the theorem.

Thus, it is enough to show that the j with $j(j+k)/g > x^{\sqrt{\varepsilon(x)}}$ make a negligible contribution and to prove the estimate for $c(k)$. We start with the latter. The term $j = k$ makes a contribution of $(2k)^{-1}$ to (3.2), and so the lower bound claimed for $c(k)$ is trivial. The upper bound is immediate from Lemma 3.2, since each term in (3.2) is bounded by $k^{-1} \prod_{p|k, p>2} \frac{p-1}{p-2}$.

For j with $j(j+k)/g > x^{\sqrt{\varepsilon(x)}}$, inequality (3.3) itself (without any sieving) gives that the number of $n \le x$ corresponding to j is at most $x^{1-\sqrt{\varepsilon(x)}}$. By Lemma 3.2 (with $\epsilon = 1$), the total number of j is at most $x^{\varepsilon(x)}$, and so the contribution from all such j is at most $x^{1-\sqrt{\varepsilon(x)}+\varepsilon(x)} \le x^{1-\frac{1}{2}\sqrt{\varepsilon(x)}}$ for large enough x. This contribution can be absorbed into the $o(1)$-term in the theorem. Indeed, for large x,

$$\frac{x^{1-\frac{1}{2}\sqrt{\varepsilon(x)}}}{c(k)x(\log x)^{-2}} \le (2k)(\log x)^2 x^{-\frac{1}{2}\sqrt{\varepsilon(x)}} \le (\log x)^2 x^{-\frac{1}{3}\sqrt{\varepsilon(x)}} < \frac{1}{\log x},$$

uniformly for $k \le x^{\varepsilon(x)}$. To see the final inequality in this chain, observe that $\varepsilon(x) > 1/\log x$ for large x, so that $x^{-\frac{1}{3}\sqrt{\varepsilon(x)}} < \mathrm{e}^{-\frac{1}{3}\sqrt{\log x}} < (\log x)^{-3}$ for large x. □

Remark Assuming a plausible uniform version of the prime k-tuples conjecture (such as implied by [14, Hypothesis UH]), a slight modification of the proof of Theorem 3.3 shows that the asymptotic formula asserted in Theorem B holds uniformly for even integers $k \le x^{\varepsilon(x)}$.

4 Towards Theorem 1.2, II: New totients from old

Before continuing, we state precisely Ford's result [8, §§4, 5][1] on the order of magnitude of $W(x)$. Let $\mathscr{V} = \{\varphi(n) : n \in \mathbf{N}\}$ be the set of all totients, and let $V(x) := \#\mathscr{V} \cap [1, x]$. Ford showed that for large x,

$$V(x) \asymp W(x) \asymp Z(x),$$

where

$$Z(x) := \frac{x}{\log x} \exp(C(\log_3 x - \log_4 x)^2 + C' \log_3 x - (C' + 1/2 - 2C) \log_4 x).$$

Here $C = 0.817814\ldots$ and $C' = 2.17696874\ldots$ are constants defined as follows. Let

$$F(x) := \sum_{n=1}^{\infty} a_n x^n, \quad \text{where} \quad a_n = (n+1)\log(n+1) - n\log n - 1. \tag{4.1}$$

Since each $a_n > 0$ and $a_n \sim \log n$ (as $n \to \infty$), it follows that F is defined and strictly increasing on $[0, 1)$, with $F(0) = 0$ and $F(x) \to \infty$ as $x \uparrow 1$. Thus, there is a unique number $\rho = 0.542598\ldots$ with $F(\rho) = 1$. We have

$$C := \frac{1}{2|\log \rho|} \quad \text{and} \quad C' := 2C(1 + \log F'(\rho) - \log(2C)) - 3/2. \tag{4.2}$$

The proof of Ford's theorem is quite technically involved but the general strategy is not hard to understand. The upper-bound aspect is proved by showing that the preimages of a typical totient have a very tightly constrained multiplicative structure. To establish the lower bound, one

[1] All references to [8] are to the corrected arXiv version of that paper.

first constructs a set of candidate preimages with a similarly restricted multiplicative structure. The candidate set has size $\asymp Z(x)$, and one shows that φ is close to injective on these candidates. The following lemma is closely related to these lower-bound arguments.

Lemma 4.1 *Fix natural numbers $d_1, d_2 \in \mathscr{V}$, and fix $D \geq \max\{d_1, d_2\}$. For large x, there are $\gg_D Z(x)$ numbers n which satisfy all of the following:*

(i) $\varphi(n) \leq x/D$,

(ii) n is convenient for both d_1 and d_2,

(iii) $n/\varphi(n) \leq K$, where K is an absolute constant.

Proof This follows from a simple adaptation of the lower-bound argument of Ford [8, §5], which we briefly review here. Put $M = M_2 + \lfloor(\log D)^{1/9}\rfloor$, where M_2 is a sufficently large absolute constant. With C as defined in (4.2), put

$$L_0 := \lfloor 2C(\log_3 x - \log_4 x)\rfloor \quad \text{and} \quad L := L_0(x) - M.$$

Put

$$\xi_i := 1 - \omega_i, \quad \text{where} \quad \omega_i := \frac{1}{10(L_0 - i)^3} \quad (0 \leq i \leq L-1).$$

Our "candidate set" in this proof is the set $\mathscr{B}$ of integers $n = p_0 p_1 \cdots p_L > x^{9/10}$ with $p_0 > p_1 > \cdots > p_L$ and

$$\begin{aligned} \varphi(n) &\leq x/D, \\ \log_2 p_i &\geq (1+\omega_i)\log_2 p_{i+1} \qquad (0 \leq i \leq L-1), \\ p_L &\geq \max\{D+2, 17\}, \end{aligned}$$

and for which the numbers $x_i := \frac{\log_2 p_i}{\log_2 (x/D)}$ (for $1 \leq i \leq L$) satisfy the system of inequalities

$$\begin{aligned} a_1x_1 + a_2x_2 + \cdots + a_Lx_L &\leq \xi_0, \\ a_1x_2 + a_2x_3 + \cdots + a_{L-1}x_L &\leq \xi_1 x_1, \\ &\vdots \\ a_1x_{L-1} + a_2x_L &\leq \xi_{L-2}x_{L-2}, \\ 0 \leq x_L &\leq \xi_{L-1}x_{L-1}, \end{aligned} \tag{4.3}$$

with the a_i defined in (4.1). The argument for [8, eq. (5.17)] gives that $\#\mathscr{B} \gg_D Z(x)$. The proof on [8, pp. 25–29] (changing some occurrences of d to D) shows that if M_2 is sufficiently large, then at most $\frac{1}{4}\#\mathscr{B}$ values of $n \in \mathscr{B}$ fail to be convenient for d_1. The same holds for d_2. Hence, there are $\gg \#\mathscr{B} \gg Z(x)$ values of $n \in \mathscr{B}$ which satisfy conditions (i) and (ii) of the lemma.

To complete the proof, it is enough to show that $n/\varphi(n)$ is bounded for $n \in \mathscr{B}$. In the notation of [8, §3], the conditions on n imply that $(x_1, \ldots, x_L) \in \mathscr{S}_L(\boldsymbol{\xi}) \subset \mathscr{S}_L(\mathbf{1})$. So with $x_0 = 1$, [8, Lemma 3.8] gives that

$$x_j \leq 4.771\rho^{j-i}x_i \qquad (0 \leq i < j \leq L), \tag{4.4}$$

where $\rho = 0.542598\ldots$ is defined as in the introduction. Since $p_L > 17$, we have

$$x_L = \frac{\log_2 p_L}{\log_2 (x/D)} > \frac{1}{\log_2 (x/D)}.$$

Now taking $j = L$ in (4.4) gives that for $1 \leq i \leq L$,

$$\log_2 p_i = x_i \log_2(x/D) \geq \frac{1}{5}(\rho^{-1})^{L-i} \geq 0.2(1.8)^{L-i},$$

so that $\sum_{i=0}^{L} \frac{1}{p_i}$ is absolutely bounded. Since $\frac{n}{\varphi(n)} \ll \exp\left(\sum_{p|n} \frac{1}{p}\right)$, we have (iii). $\square$

5 Proof of Theorem 1.2

Lemma 5.1 *let $\mathscr{S}$ be a subset of $[1,x]$ on which φ is nondecreasing. For large x, the set $\varphi(\mathscr{S})$ is missing $\gg W(x)$ elements of $\mathscr{W}(x)$, uniformly in the choice of $\mathscr{S}$.*

Proof Fix totients d_1 and d_2 with $d_1 < d_2$ but where the smallest preimage n_1 of d_1 is greater than the largest preimage n_2 of d_2. For example, we can take

$$d_1 = 2^{18} \cdot 257, \quad \text{with smallest preimage } n_1 = 135268352,$$

and

$$d_2 = d_1 + 28, \quad \text{with largest preimage } n_2 = 134742074.$$

We apply Lemma 4.1 with our values of d_1 and d_2 and with $D = Kn_1n_2$; we obtain a set $\mathscr{A}$ of $\gg_D V(x)$ integers n with properties (i)-(iii) of Lemma 4.1. Let

$$\mathscr{V}_1 = \{d_1\varphi(n) : n \in \mathscr{A}\} \quad \text{and} \quad \mathscr{V}_2 = \{d_2\varphi(n) : n \in \mathscr{A}\}.$$

As n ranges over $\mathscr{A}$, the numbers $d_1\varphi(n)$ are all distinct, since $d_1\varphi(n)$ has smallest preimage $n_1 n$. Moreover, for $n \in \mathscr{A}$,

$$n_1 n = n_1 \frac{n}{\varphi(n)} \varphi(n) \le Kn_1\varphi(n) \le Kn_1 \frac{x}{Kn_1n_2} \le x,$$

so that $\mathscr{V}_1$ is a subset of $\mathscr{W}(x)$. Similarly, $\#\mathscr{V}_2 = \#\mathscr{A}$ and $\mathscr{V}_2$ is a subset of $\mathscr{W}(x)$.

Let $\mathscr{A}_1$ be the set of $n \in \mathscr{A}$ for which $d_1\varphi(n) \notin \varphi(\mathscr{S})$, and let $\mathscr{A}_2$ be the set of $n \in \mathscr{A}$ for which $d_2\varphi(n) \notin \varphi(\mathscr{S})$. Suppose $n \in \mathscr{A}$ but that both $d_1\varphi(n), d_2\varphi(n) \in \varphi(\mathscr{S})$. Since $d_1\varphi(n) < d_2\varphi(n)$ and $\varphi|_{\mathscr{S}}$ is nondecreasing, it follows that $\mathscr{S}$ contains two integers m_1 and m_2 with $m_1 < m_2$ and $\varphi(m_1) = d_1\varphi(n)$, $\varphi(m_2) = d_2\varphi(n)$. This contradicts that $m_1 \ge n_1 n > n_2 n \ge m_2$. So every $n \in \mathscr{A}$ belongs to either $\mathscr{A}_1$ or $\mathscr{A}_2$, and so $\varphi(\mathscr{S})$ is missing at least $\frac{1}{2}\#\mathscr{A} \gg_D Z(x) \gg W(x)$ elements of $\mathscr{W}(x)$. ◻

Proof (Completion of the proof of Theorem 1.2) Let $\mathscr{S}$ be a subset of $[1,x]$ on which φ is nondecreasing, and list the elements of $\mathscr{S}$ as $n_1 < n_2 < \cdots < n_m$, in increasing order. The number of values of i for which $n_{i+1} - n_i > \log x$ is clearly at most $x/\log x = o(W(x))$. Partition the indices $1 \le i < m$ for which $n_{i+1} - n_i \le \log x$ into two classes, according to whether $\varphi(n_i) = \varphi(n_{i+1})$ or not. If i belongs to the first class, then $\varphi(n_i) = \varphi(n_i + k)$ for some $k \le \log x$. By Theorems 3.1 and 3.3, the number of $n \le x$ with $\varphi(n) = \varphi(n+k)$ is $\ll x/(\log x)^2$, uniformly for $k \le \log x$. So summing over $k \le \log x$, we find that the number of i in the first class is $\ll x/\log x = o(W(x))$. Since φ is nondecreasing on $\mathscr{S}$, distinct values of i in the second class correspond to distinct integers $\varphi(n_i)$. So by Lemma 5.1, the number of such i is bounded by $(1-c)W(x)$, for some $c > 0$ and all large x. Thus, $\limsup M^{\uparrow}(x)/W(x) \le 1 - c < 1$. ◻

6 Strictly decreasing sequences: Proof of Theorem 1.4

The proof of Theorem 1.4 makes use of the following theorem of Baker, Harman, and Pintz [3, Theorem 1] concerning small gaps between primes:

Theorem D *If x is sufficiently large, then there is a prime in the interval $[x - x^{0.525}, x]$.*

Proof (Proof of Theorem 1.4) Using Bertrand's postulate, let p_0 be a prime number with $x^{1/10} < p_0 \le 2x^{1/10}$. Let q_0 be the largest prime for which $p_0 q_0 \le x$. By Theorem D, we have

$$\frac{x}{p_0} - x^{1/2} \le q_0 \le \frac{x}{p_0} \tag{6.1}$$

for large x. We now carry out $k := \lfloor x^{0.19} \rfloor$ steps of the following algorithm: Assume that $p_0, \dots, p_i$, $q_0, \dots, q_i$ have already been chosen. Let p_{i+1} be the first prime exceeding p_i, and let q_{i+1} be a prime chosen so that

$$p_{i+1}q_{i+1} < p_i q_i \quad \text{while} \quad \varphi(p_{i+1}q_{i+1}) > \varphi(p_i q_i). \tag{6.2}$$

To see that this makes sense, we must show that there is a prime q_{i+1} obeying (6.2), i.e., that there is a prime q_{i+1} satisfying

$$q_{i+1} < \frac{p_i}{p_{i+1}} q_i \quad \text{and} \quad q_{i+1} - 1 > \frac{p_i - 1}{p_{i+1} - 1}(q_i - 1). \tag{6.3}$$

Now (6.3) places q_{i+1} in an interval with right-endpoint $\frac{p_i}{p_{i+1}} q_i$ with length

$$\left(\frac{p_i}{p_{i+1}} - \frac{p_i - 1}{p_{i+1} - 1}\right) q_i + \frac{p_i - 1}{p_{i+1} - 1} - 1 > \frac{q_i}{p_{i+1}^2} - 1.$$

By Theorem D, a suitable choice of q_{i+1} exists if $q_i / p_{i+1}^2 > q_i^{0.53}$ (say), so if $p_{i+1} < q_i^{0.235}$. From the choice of k and the prime number theorem, we have $p_0, p_1 \dots, p_{i+1} \le x^{0.1901}$ (say); also, since $\varphi(p_i q_i) \ge \varphi(p_0 q_0) \gg x$,

$$q_i - 1 \ge \frac{\varphi(p_0 q_0)}{p_i - 1} \gg x/p_i \gg x^{0.8099}.$$

Hence,

$$q_i^{0.235} > x^{0.1903} > p_{i+1}.$$

This shows that the construction goes through for k steps. We take $n_i := p_i q_i$ for $i = 0, 1, \dots, k$. Then $\{n_k < n_{k-1} < \cdots < n_0\}$ is a subset of $[1, x]$ on which φ is strictly decreasing with size $k + 1 > x^{0.19}$. □

7 A nontrivial lower bound on $M^{\downarrow}(x)$: Proof of Theorem 1.3

Lemma 7.1 *Given $x \ge 1$, let d be the largest integer for which the equation $\varphi(n) = d$ has $M^0(x)$ solutions $n \le x$. For each fixed $\epsilon > 0$, we have $d > x^{1-\epsilon}$ once $x > x_0(\epsilon)$.*

Proof Suppose for the sake of contradiction that $d \le x^{1-\epsilon}$. If x is large, we can choose a prime $p \le x^{\epsilon/2}$ for which $p - 1$ does not divide d. Indeed, the number of divisors of d is $x^{o(1)}$, by the maximal order of the divisor function (see, e.g., [13, Theorem 317]), while the number of $p \le x^{\epsilon/2}$ is $\gg_\epsilon x^{\epsilon/2}/\log x$. Since $p - 1 \nmid d$, each solution n to $\varphi(n) = d$ is coprime to p. Thus, $\varphi(np) = (p-1)d$. So the number $d' := (p-1)d$ has at least $M^0(x)$ preimages under φ. Since $d' < pd \le x^{1-\epsilon/2}$, each preimage of d' is $< 2x^{1-\epsilon/2} \log\log x < x$, assuming x is large. (We use here the minimal order of the Euler function; see [13, Theorem 328].) Hence, d' has at least $M^0(x)$ preimages in $[1, x]$, contradicting the maximality of d.

Proof (Proof of Theorem 1.3) Given x, choose d as in Lemma 7.1. Then $d > x^{0.95}$ once x is large. Let $\mathscr{P}$ be the set of primes p for which $p-1$ divides d. Every solution n to $\varphi(n) = d$ is supported on the primes in $\mathscr{P}$. Also, $\#\mathscr{P} = x^{o(1)}$, by the maximal order of the divisor function. It follows that there are only $x^{o(1)}$ solutions n to $\varphi(n) = d$ with fewer than 100 prime factors (counted with multiplicity).

Let N be the least solution to $\varphi(N) = d$ with at least 100 prime factors. Clearly, $N > d > x^{0.95}$. The proof of Theorem 1.4 (with $x = N$) gives us a sequence

$$p_k q_k < \cdots < p_1 q_1 < p_0 q_0 \le N$$

along which φ is strictly decreasing, with $k > N^{0.19}$. Moreover, by (6.1), we have

$$p_0 q_0 \ge N - 2N^{0.6};$$

since $q_0 \le N/p_0 \le N^{0.9}$, this yields

$$\begin{aligned}\varphi(p_0 q_0) &= p_0 q_0 - p_0 - q_0 + 1 \\ &> p_0 q_0 - 2q_0 \ge N - 2N^{0.6} - 2N^{0.9}.\end{aligned}$$

Now N has at least one prime factor $r \le N^{1/100}$, and so

$$\varphi(N) \le N(1 - 1/r) \le N - N^{0.99} < \varphi(p_0 q_0),$$

assuming that x is large. It follows that φ is nonincreasing on the set $\mathscr{S} := \{p_k q_k < \cdots < p_0 q_0\} \cup \{n : N \le n \le x, \varphi(n) = d\}$, and that

$$\#\mathscr{S} > N^{0.19} + (M^0(x) - x^{o(1)}) \ge (x^{0.95})^{0.19} + (M^0(x) - x^{o(1)}) > x^{0.18} + M^0(x)$$

for large values of x. □

8 Consecutive integers: Proof of Theorem 1.5

Proof (Proof of the lower bound) Let $\delta > 0$. For large x, we describe how to construct a set $\{n+1, \ldots, n+k\}$ of consecutive integers contained in $[1, x]$ with

$$k := \left\lfloor \frac{\log_3 x}{\log_6 x} + (\alpha - \gamma - \delta) \frac{\log_3 x}{(\log_6 x)^2} \right\rfloor$$

on which φ is nonincreasing. The nondecreasing case is similar (but slightly simpler) and we omit it. Rather than insist that φ be nonincreasing, it suffices to require that

$$\frac{\varphi(n+1)}{n+1} > \frac{\varphi(n+2)}{n+2} > \cdots > \frac{\varphi(n+k)}{n+k}. \tag{8.1}$$

Indeed, if $m \in \{n+1, \ldots, n+(k-1)\}$, and $\varphi(m)/m > \varphi(m+1)/(m+1)$, then

$$\varphi(m+1) < \varphi(m) + \varphi(m)/m \le \varphi(m) + 1,$$

so that $\varphi(m+1) \le \varphi(m)$.

To understand the ratios appearing in (8.1), it is convenient to introduce a partition of the primes into three classes: the *small primes* in $[2, k]$, the *medium-sized primes* in $(k, \frac{1}{2}\log x]$, and the large primes $> \frac{1}{2}\log x$. We make two observations. First, a medium-sized or large prime divides at most one of any k consecutive integers. Second, for each $m \le x$, the contribution to the ratio $\varphi(m)/m = \prod_{p|m}(1-1/p)$ from large primes is quite close to 1. In fact, since m has at most $\frac{\log x}{\log(\frac{1}{2}\log x)}$ prime factors, we have

$$\prod_{\substack{p|m\\ p>\frac{1}{2}\log x}} \left(1-\frac{1}{p}\right)^{-1} \leq \exp\left(\sum_{\substack{p|m\\ p>\frac{1}{2}\log x}} \frac{1}{p-1}\right) < 1+\frac{3}{\log_2 x} \tag{8.2}$$

for large x. Now set A to be the largest initial product of primes $2\cdot 3\cdot 5\cdot 7\cdots$ (*primorial*) for which $A \leq k$, and observe that for each $1 \leq i \leq k$, we have

$$\frac{\varphi(i)}{i} = \prod_{p|i}(1-1/p) \geq \frac{\varphi(A)}{A}.$$

We claim that we can choose disjoint sets of primes $\mathscr{P}_1, \ldots, \mathscr{P}_k$, with each $\mathscr{P}_i \subset ((\log_2 x)^2, \frac{1}{2}\log x]$ (so that in particular, $\mathscr{P}_i$ consists of medium-sized primes), and so that

$$\frac{\varphi(A)}{A}\left(1-\frac{6i}{\log_2 x}\right)\left(1-\frac{1}{(\log_2 x)^2}\right) \leq \frac{\varphi(i)}{i}\prod_{p\in\mathscr{P}_i}\left(1-\frac{1}{p}\right) \leq \frac{\varphi(A)}{A}\left(1-\frac{6i}{\log_2 x}\right) \tag{8.3}$$

for all $1 \leq i \leq k$.

Assuming for the moment that the claim is proved, let us see how to construct our set satisfying (8.1). Let $\mathscr{P}'$ be the set of all medium-sized primes not appearing in any of $\mathscr{P}_1, \ldots, \mathscr{P}_k$, and let $n \in (x/2, x-k]$ be a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv 0 \pmod{\prod_{p\leq k} p}, \\ n+i &\equiv 0 \pmod{\prod_{p\in\mathscr{P}_i} p} \quad \text{for } 1 \leq i < k, \\ n+k &\equiv 0 \pmod{\prod_{p\in\mathscr{P}_k\cup\mathscr{P}'} p}. \end{aligned}$$

The product of the moduli is bounded by $x^{1/2+o(1)}$, by the prime number theorem, and so a solution n in the desired interval exists by the Chinese remainder theorem. For each $1 \leq i \leq k$, write $n+i = a_i b_i c_i$, where a_i, b_i, and c_i are supported on the small, medium-sized, and large primes respectively. Since n is divisible by every small prime, the small prime divisors of a_i coincide with the small prime divisors of i, so that

$$\varphi(a_i)/a_i = \varphi(i)/i. \tag{8.4}$$

The medium-sized prime divisors of $n+i$ always include the primes appearing in $\mathscr{P}_i$ and are exactly these primes except in the case when $i = k$; hence,

$$\frac{\varphi(b_i)}{b_i} \leq \prod_{p\in\mathscr{P}_i}(1-1/p), \tag{8.5}$$

with equality unless $i = k$. (We have used here the first observation of the preceding paragraph.) Piecing together (8.4), (8.5), (8.2), and recalling the definition (8.3) of the sets $\mathscr{P}_i$, we find that for large x,

$$\frac{\varphi(A)}{A}(1-(6i+4)/\log_2 x) \leq \frac{\varphi(n+i)}{n+i} \leq \frac{\varphi(A)}{A}(1-6i/\log_2 x) \tag{8.6}$$

for all $1 \leq i < k$. Moreover, the right-hand inequality holds even when $i = k$. This gives (8.1), as desired.

It remains to prove that we can choose sets $\mathscr{P}_i$ satisfying (8.3). We use the greedy algorithm: Start with $i = 1$, and successively throw primes from $((\log_2 x)^2, \frac{1}{2}\log x]$ into $\mathscr{P}_1$ stopping once (8.3) is satisfied with $i = 1$. Continue the process for all of $i = 2, \ldots, k$. Our only concern is that we never run out of primes; this will be true if

$$\prod_{(\log_2 x)^2 < p \leq \frac{1}{2}\log x} \left(1 - \frac{1}{p}\right) \leq \prod_{1 \leq i \leq k} \left(\frac{\varphi(A)}{A}\frac{i}{\varphi(i)}\left(1 - \frac{6i}{\log_2 x}\right)\left(1 - \frac{1}{(\log_2 x)^2}\right)\right). \tag{8.7}$$

The left-hand product is $\asymp \frac{\log_3 x}{\log_2 x}$ by Mertens's theorem; we will show that the right-hand side has a larger order of magnitude. We have

$$\frac{\varphi(A)}{A} = \frac{\mathrm{e}^{-\gamma}}{\log_2 k}\left(1 + O\left(\frac{1}{\log_2 k}\right)\right), \quad \text{so that} \quad \left(\frac{\varphi(A)}{A}\right)^k = \frac{\mathrm{e}^{-\gamma k}}{(\log_2 k)^k}\exp\left(O\left(\frac{k}{\log_2 k}\right)\right).$$

Also,

$$\begin{aligned}
\prod_{1 \leq i \leq k} \frac{i}{\varphi(i)} &= \prod_{p \leq k} (1 - 1/p)^{-\lfloor k/p \rfloor} \\
&\gg \frac{1}{\log k}\left(\prod_{p \leq k}(1 - 1/p)^{-1/p}\right)^k \\
&= \frac{1}{\log k}(\mathrm{e}^{\alpha}(1 + O(1/k)))^k \gg \frac{\mathrm{e}^{\alpha k}}{\log k}.
\end{aligned} \tag{8.8}$$

The remaining contribution to the right-hand side of (8.7) is

$$\gg (1 - O(k^2/\log_2 x))(1 - O(k/(\log_2 x)^2)) \gg 1.$$

Piecing everything together, we see that the right-hand side of (8.7) has size at least

$$\exp((\alpha - \gamma)k - k\log_3 k + O(k/\log_2 k)).$$

Recalling the definition of k, a short computation shows that this is at least

$$\exp(-\log_3 x + \frac{\delta}{2}\log_3 x/\log_6 x),$$

for large x, which is of greater order of magnitude than $\log_3 x/\log_2 x$. $\square$

Proof (Proof of the upper bound) Fix $\delta > 0$. It will suffice to show that with

$$k := \left\lfloor \frac{\log_3 x}{\log_6 x} + (\alpha - \gamma + \delta)\frac{\log_3 x}{(\log_6 x)^2} \right\rfloor,$$

there are no sets $\{n+1, n+2, \ldots, n+k\} \subset [1, x]$ on which φ is monotone, once x is sufficiently large.

Suppose for the sake of contradiction that we have such a set. Let B be the largest primorial bounded by $\log_3 x/\log_5 x$. Chopping off $O(B)$ terms from the beginning and end of our segment (and so replacing δ by $\delta/2$, say), we can assume that both $n+1$ and $n+k$ are multiples of B. Hence,

$$\max\left\{\frac{\varphi(n+1)}{n+1}, \frac{\varphi(n+k)}{n+k}\right\} \le \frac{\varphi(B)}{B}.$$

If φ is nonincreasing, this implies immediately that

$$\frac{\varphi(B)}{B} \ge \frac{\varphi(n+1)}{n+1} > \frac{\varphi(n+2)}{n+2} > \cdots > \frac{\varphi(n+k)}{n+k}.$$

Suppose instead that φ is nondecreasing. Then $k \le M^{\uparrow}(n+k)$, and so $n > k(\log k)^{1/2}$ by Theorem 1.2 (once x is large). It follows that uniformly for $1 \le i \le k$,

$$\frac{\varphi(n+i)}{n+i} \le \frac{\varphi(n+k)}{n+k}\frac{n+k}{n+i} \le \frac{\varphi(B)}{B}(1+O(1/\sqrt{\log_4 x})).$$

By Mertens's theorem,

$$\frac{\varphi(B)}{B} = \frac{\mathrm{e}^{-\gamma}}{\log_5 x}(1+O(1/\log_5 x)).$$

We conclude that regardless of whether φ is nonincreasing or nondecreasing,

$$\frac{\varphi(n+i)}{n+i} \le \frac{\mathrm{e}^{-\gamma}}{\log_5 x}(1+O(1/\log_5 x)) \qquad \text{(for all } 1 \le i \le k).$$

Hence,

$$\prod_{i=1}^{k}\frac{\varphi(n+i)}{n+i} \le \frac{\mathrm{e}^{-k\gamma}}{(\log_5 x)^k}\exp\left(O\left(\frac{\log_3 x}{\log_5 x \log_6 x}\right)\right). \tag{8.9}$$

We now obtain a contradictory estimate for the left-hand side of (8.9). Write $n+i = a_i b_i c_i$, with the right-hand factors having the same meaning as in the lower-bound portion of the argument. From (8.2),

$$\prod_{1\le i\le k}\frac{\varphi(c_i)}{c_i} \asymp 1. \tag{8.10}$$

We have $\prod_{1\le i\le k}\frac{\varphi(a_i)}{a_i} = \prod_{p\le k}(1-1/p)^{n_p}$, where $n_p = k/p + O(1)$ counts the number of terms of the sequence $n+1,\dots,n+k$ divisible by p. Hence (cf. (8.8)),

$$\prod_{1\le i\le k}\frac{\varphi(a_i)}{a_i} = (\log k)^{O(1)}\mathrm{e}^{-\alpha k}. \tag{8.11}$$

Finally, since a medium-sized prime can divide at most one of $n+1,\dots,n+k$,

$$\prod_{1\le i\le k}\frac{\varphi(b_i)}{b_i} \ge \prod_{k<p\le\frac{1}{2}\log x}(1-1/p) \gg \frac{\log k}{\log_2 x}. \tag{8.12}$$

Collecting and rearranging (8.9)-(8.12), we arrive at the bound

$$\mathrm{e}^{(\gamma-\alpha)k}(\log_5 x)^k \le (\log_2 x)\exp\left(O\left(\frac{\log_3 x}{\log_5 x\log_6 x}\right)\right). \tag{8.13}$$

But the definition of k and a short computation shows that

$$\mathrm{e}^{(\gamma-\alpha)k}(\log_5 x)^k > (\log_2 x)\exp\left(\frac{\delta}{3}\log_3 x/\log_6 x\right)$$

for large x, which contradicts (8.13). $\square$

Remark The construction for the lower bound half of Theorem 1.5 works with "nonincreasing" and "nondecreasing" replaced by "strictly increasing" and "strictly decreasing". For example, in the decreasing case, since the n constructed in the proof satisfy $n > x/2$ and (8.6), a short computation shows that (for large x)

$$\frac{\varphi(n+i)}{\varphi(n+i+1)} > (1-2/x)\frac{\varphi(n+i)/(n+i)}{\varphi(n+i+1)/(n+i+1)} > 1 + \frac{1}{\log_2 x}$$

for all $1 \leq i < k$.

9 Numerics

Let $S(x)$ be the set of numbers on which φ is nondecreasing such that $|S(x)| = M^{\uparrow}(x)$ and such that $S(x)$ is minimal lexicographically. When computing $S(x)$ for small values of x, one is tempted to conjecture that $M^{\uparrow}(x) - \pi(x)$ goes to infinity. This happens because when x is small, $S(x)$ consists mostly of composite numbers. For example, $S(70)$ is

$$\{1,2,3,4,5,8,10,12,14,15,16,20,21,26,28,32,33,35,\ 39,45,52,56,58,62,63,65,67\}.$$

However, $S(10^6)$ consists of mostly prime numbers. Indeed if $s \in S(10^6)$ and $s \geq 31957$, then s is prime. So out of the 78562 numbers in $S(10^6)$, the last 75501 are prime. Combining this with our calculation $M^{\uparrow}(10^7) = 664643 = \pi(10^7) + 64$ leads us to conjecture that $M^{\uparrow}(x) = \pi(x) + 64$ for all $x \geq 31957$.

Before the dominance of the primes above 31957, the primes had also taken command of the list when $11777 \leq x \leq 27678$. Indeed, if x is in that range, then the tail of primes of $S(x)$ consists of all the primes greater than or equal to 11777. However, $S(27679)$ has no tail of primes. This led us to question whether a shadow sequence was hiding behind the primes waiting to pounce at the right time (a huge prime gap, for example). With this in mind, we computed the maximum size $M_2(x)$ of a subset of $\{n \leq x \mid n \text{ is not prime}\}$ on which φ is nondecreasing.

If we had $M^{\uparrow}(x) > \pi(x) + 64$ for x large enough, then either the shadow sequence takes over or for some $p \geq 31957$, we have that the largest subset of $\{p < n \leq x | \varphi(n) \geq p-1\}$ on which φ is monotone has the same cardinality as the largest subset of $\{p < n \leq x | \varphi(n) \geq p-1,\ n \text{ not prime}\}$ on which φ is monotone. The latter seems highly unlikely since, e.g., the first composite n satisfying $\varphi(n) \geq p - 1$ is greater than $p + \sqrt{p} - 1$, while the first prime n satisfying that inequality is expected to be much smaller. The former is analyzed in the following paragraph.

It is not hard to see that $M_2(x) \leq M^{\uparrow}(x) - 2$ for $x \geq 6$. For a shadow sequence to pounce we would need to have $M_2(x) = M^{\uparrow}(x) - 2$ for some $x \geq 31957$. We conjecture that this will not happen. Our main evidence is Table 9.1, on which we consider the difference between $M^{\uparrow}(x)$ and $M_2(x)$ for different values of x. Though the size of the difference varies, it seems to be getting bigger as x gets bigger (even if it does so in an oscillatory manner).

With respect to $M^{\downarrow}(x)$, the size of it is so small with respect to x that computing values of it for small x doesn't reveal much. Indeed, $M^{\downarrow}(10^6) = 995$, a tiny number compared to 10^6. Other information we can mention about $M^{\downarrow}(10^6)$ is that the largest subset contains 791 preimages of 241920. The element in $\{\varphi(n) \mid n \leq 10^6\}$ which has the most preimages is 241920. It has 937 preimages, i.e., $M^0(10^6) = 937$.

One might wonder whether the numbers in the largest subset of $[1, x]$ where φ is nonincreasing follow the pattern in the proofs of Theorems 1.3 and 1.4. Indeed, most of the preimages have only two prime factors coinciding with the pattern of the proofs of those theorems.

Table 9.1 Difference between $M^{\uparrow}(x)$ and $M_2(x)$. The reason 31957 is the threshold is that it is the first prime after a big prime gap. The primes 11777 and 44351 also come after big prime gaps, which is why the difference $M^{\uparrow}(x) - M_2(x)$ decreased at the integers coming before it.

x	$M^{\uparrow}(x)$	$M_2(x)$	$M^{\uparrow}(x) - M_2(x)$
10000	1276	1261	15
11776	1459	1457	2
20000	2312	2297	15
30000	3298	3294	4
31956	3491	3489	2
40000	4267	4244	23
44350	4676	4657	19
50000	5197	5168	29
100000	9656	9595	61
1000000	78562	77681	881

Acknowledgements Much of this work was conducted while P. P. was supported as a Shapiro Visitor at Dartmouth College. P. P. would like to acknowledge helpful conversations with Kevin Ford about the material of [8]. P. P. was supported by NSF award DMS-0802970 while C. P. and E. T. were supported by award DMS-1001180.

References

1. T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976.
2. R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), no. 4, 331–361.
3. R. C. Baker, G. Harman, and J. Pintz, *The difference between consecutive primes. II*, Proc. London Math. Soc. (3) **83** (2001), no. 3, 532–562.
4. 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.
5. P. Erdős, *Some remarks on Euler's φ function*, Acta Arith. **4** (1958), 10–19.
6. P. Erdős, C. Pomerance, and A. Sárközy, *On locally repeated values of certain arithmetic functions. II*, Acta Math. Hungar. **49** (1987), no. 1-2, 251–259.
7. J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), no. 3, 561–584.
8. K. Ford, *The distribution of totients*, Ramanujan J. **2** (1998), 67–151, cited version available online as `arXiv:1104.3264v1`.
9. K. Ford, *The distribution of totients*, Electron. Res. Announc. Amer. Math. Soc. **4** (1998), 27–34 (electronic).
10. S. W. Graham, J. J. Holt, and C. Pomerance, *On the solutions to $\varphi(n) = \varphi(n+k)$*, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 867–882.
11. H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, no. 4, Academic Press, London-New York, 1974.
12. G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. **48** (1917), 76–92.
13. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.
14. G. Martin, *An asymptotic formula for the number of smooth values of a polynomial*, J. Number Theory **93** (2002), no. 2, 108–182.
15. G. Myerson, *Western number theory problems, 17 & 19 Dec. 2009*, available online at `http://www.math.byu.edu/~doud/WNTC/problems2009.pdf`.
16. P. Pollack, *Long gaps between deficient numbers*, Acta Arith. **146** (2011), no. 1, 33–42.
17. C. Pomerance, *Popular values of Euler's function*, Mathematika **27** (1980), no. 1, 84–89.
18. C. Pomerance, *Two methods in elementary analytic number theory*, Number theory and applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 135–161.